ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо застосування цифрового підпису для цілісності даних в організації»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Артем КОВАЛЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
КОВАЛЕНКО Артем
(прізвище, ім'я)

Керівник д. т. н., професор, Кожухівський А.Д.
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Коваленку Артему Олександровичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: Рекомендації щодо застосування цифрового підпису для цілісності даних в організації

керівник кваліфікаційної роботи Кожухівський Андрій, д. т. н., професор
(прізвище, ім’я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.06.2024 р.

3. Вихідні дані до кваліфікаційної роботи
Інформаційній ресурси організації;
рішення щодо впровадження цифрового підпису;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти у сфері електронного підпису.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження основних понять цифрового підпису.
2.Аналіз методів застосування цифрового підпису для забезпечення цілісності даних.
3.Розробка рекомендацій щодо впровадження цифрового підпису в організації.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми забезпечення цілісності даних в організації.	03.03.2025 р.	
2.	Аналіз наукової та технічної літератури з питань цифрового підпису та інформаційної безпеки.		
3.	Аналіз нормативної бази та технологій цифрового підпису, які використовуються в сучасних інформаційних системах.		
4.	Практична оцінка можливостей застосування цифрового підпису для забезпечення цілісності даних в організації.		
5.	Розроблення рекомендацій щодо впровадження цифрового підпису в організації.		
6.	Оформлення результатів дослідження.		
7.	Підготовка доповіді до захисту.	06.06.2025 р.	

Здобувач вищої освіти _____ Артем КОВАЛЕНКО
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Андрій КОЖУХІВСЬКИЙ
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача КОВАЛЕНКА Артема
на тему: «Рекомендації щодо застосування цифрового підпису для цілісності даних в організації»

Актуальність: Забезпечення цілісності даних є критично важливим завданням для будь-якої сучасної організації, зокрема в умовах зростання кіберзагроз та використання інформаційних систем. Цифровий підпис — один з ключових механізмів гарантування автентичності та цілісності інформації, що передається або зберігається. Тема кваліфікаційної роботи є актуальною та відповідає сучасним викликам інформаційної безпеки.

Позитивні сторони:

1. У роботі наведено огляд нормативно-правової бази та технічних аспектів застосування цифрового підпису.
2. Проаналізовано сучасні методи забезпечення цілісності даних та їх реалізацію в різних програмних рішеннях.
3. Надано практичні рекомендації щодо впровадження цифрового підпису в інформаційні системи організації.
4. Матеріал викладено логічно, послідовно, з дотриманням норм наукового стилю. Використані джерела є актуальними, а висновки — обґрунтованими.

Недоліки:

1. Було б доцільно розширити аналіз конкретних прикладів застосування цифрового підпису в українських організаціях.
2. В роботі варто було б окремо розглянути потенційні ризики та обмеження використання цифрового підпису в умовах гібридних загроз.

Вказані зауваження не знижують загального позитивного враження від кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **"добре"**, а здобувач(ка) **КОВАЛЕНКО Артем** – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека**.**

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім'я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач КОВАЛЕНКО Артем до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Рекомендації щодо застосування цифрового підпису для цілісності даних в організації».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***КОВАЛЕНКО Артем*** обрав тему роботи, метою якої було дослідити методи та підходи до забезпечення цілісності даних в організаціях шляхом впровадження цифрового підпису, а також розробити рекомендації щодо його практичного використання. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***КОВАЛЕНКО Артем*** продемонстрував високій рівень теоретичної підготовки, здатність до самостійного аналізу, навички роботи з нормативною базою та актуальними технологіями. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***КОВАЛЕНКА Артема*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Андрій КОЖУХІВСЬКИЙ
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **КОВАЛЕНКО Артем** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 62 сторінки, 17 рисунків, 12 джерел.

Об'єкт дослідження – Цифровий підпис як засіб забезпечення цілісності даних в організації.

Предмет дослідження – Рекомендації щодо застосування цифрового підпису для цілісності даних організації.

Мета роботи – дослідити застосування цифрового підпису як засобу забезпечення цілісності даних в межах організації, окреслити основні принципи його впровадження, а також сформулювати рекомендації щодо його ефективного використання для захисту інформації від втручання та змін.

Методи дослідження – опрацювання наукових джерел з обраної тематики, дослідження технічної документації, міжнародних нормативів та здійснення їх порівняльного аналізу.

Цифровий підпис є важливим інструментом забезпечення цілісності та достовірності даних в організаціях. Використання цифрового підпису дозволяє гарантувати, що інформація не була змінена або підроблена під час передачі або зберігання.

У роботі проаналізовано основні принципи роботи цифрового підпису, типи алгоритмів та засобів, які застосовуються для його створення. Розглянуто нормативно-правові вимоги щодо використання цифрового підпису в Україні.

Розроблено рекомендації для організацій щодо впровадження цифрового підпису, включаючи вибір відповідного програмного забезпечення, інтеграцію з існуючими інформаційними системами та організацію процесу управління ключами.

Застосування цифрового підпису значно підвищує рівень захисту інформації, забезпечує контроль цілісності даних та сприяє дотриманню вимог законодавства.

На основі проведених досліджень запропоновано покрокову методику впровадження цифрового підпису в організації для забезпечення цілісності та безпеки даних.

Галузь використання – інформаційна безпека, захист даних в організаціях.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

PKI – Public Key Infrastructure

HSM – Hardware Security Module

API – Application Programming Interface

RSA – Rivest–Shamir–Adleman

ECDSA – Elliptic Curve Digital Signature Algorithm

BLS – Boneh–Lynn–Shacham

SPHINCS+ – Secure Hash-based Post-Quantum Signature

XMLDSig – XML Digital Signature

EDM – Electronic Document Management

CRM – Customer Relationship Management

NIST – National Institute of Standards and Technology

eIDAS – Electronic Identification, Authentication and Trust Services

PIPEDA – Personal Information Protection and Electronic Documents Act

ESIGN – Electronic Signatures in Global and National Commerce Act

UETA – Uniform Electronic Transactions Act

ВСТУП

У сучасну епоху цифрових технологій інформація виступає одним із найважливіших ресурсів, що забезпечують ефективне функціонування будь-якої організації. Гарантування її безпеки, достовірності та незмінності є основним завданням у сфері захисту інформаційних систем. Із постійним зростанням обсягу електронної інформації, яка передається та зберігається, виникає нагальна потреба у впровадженні надійних методів перевірки автентичності, визначення авторства та захисту даних від стороннього втручання. Одним з найнадійніших засобів для цього є цифровий підпис.

Цифровий підпис представляє собою інструмент сучасної криптографії, який забезпечує ідентифікацію особи, що підписала електронний документ, а також гарантує незмінність вмісту інформації після її підписання. Його використання в організаційній діяльності дозволяє зменшити ризики фальсифікації даних, підвищити довіру до електронних документів та посилити відповідальність за їх обробку.

Тема дослідження є актуальною у зв’язку зі стрімкою цифровізацією процесів управління, зростанням кількості кіберінцидентів, спрямованих на спотворення інформації, а також необхідністю створення ефективних систем електронного документообігу, які відповідали б міжнародним вимогам щодо інформаційної безпеки. У багатьох країнах світу, зокрема й в Україні, цифровий підпис вже отримав широке поширення як у державному управлінні, так і в бізнес-середовищі. Проте результативність його впровадження залежить від комплексу факторів: технологічного забезпечення, нормативного регулювання, внутрішніх процедур організації та рівня підготовки персоналу.

Тому виникає потреба у розробці конкретних і ефективних рекомендацій щодо впровадження цифрового підпису з особливим акцентом на забезпечення цілісності даних. Це дозволить краще усвідомити принципи його дії та визначити комплекс заходів, необхідних для посилення захисту інформаційних активів організації.

Метою цієї роботи є вивчення цифрового підпису як засобу забезпечення цілісності даних, аналіз правових, організаційних і технічних аспектів його застосування, а також формування практичних порад щодо його впровадження в умовах функціонування конкретної організації.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять рекомендовані підходи до впровадження цифрового підпису з метою захисту цілісності даних в організаціях.

Сучасна практика свідчить, що традиційних методів захисту інформації вже недостатньо в умовах зростання кількості кіберзагроз. Цифровий підпис, як елемент інфраструктури відкритих ключів (PKI), дозволяє не лише підтвердити автентичність документа, а й забезпечити прозорість електронного документообігу. Його застосування активно поширюється у державному управлінні, фінансовому секторі та бізнесі. Важливим фактором є не лише наявність технологій, а й відповідне нормативне регулювання, підготовка персоналу та довіра між сторонами. Використання електронного підпису дозволяє знизити витрати, прискорити процеси та підвищити безпеку інформаційної взаємодії. Проте успішне впровадження вимагає комплексного підходу до технічних, правових та організаційних аспектів.

1. ДОСЛІДЖЕННЯ ОСНОВНИХ ПОНЯТЬ ЦИФРОВОГО ПІДПИСУ

1.1. Аналіз поняття та функціонального призначення цифрового підпису

У сучасну епоху інформаційних технологій особливої ваги набуває питання захисту даних та перевірки достовірності інформації. Одним із головних засобів забезпечення інформаційної безпеки виступає цифровий підпис — інструмент, що гарантує достовірність, цілісність та невідмовність електронних документів.

Цифровий підпис — це спеціальний криптографічний інструмент, що дозволяє підтвердити справжність електронного документа або повідомлення. Він є цифровим аналогом звичайного підпису, проте використовується в електронному середовищі. Підпис створюється із застосуванням приватного (закритого) ключа, який належить власнику підпису, а перевірка здійснюється за допомогою публічного (відкритого) ключа.

З технічного боку, цифровий підпис являє собою результат криптографічних операцій над документом, що використовують алгоритми асиметричного шифрування (такі як RSA, ECDSA) та хеш-функції (наприклад, SHA-256).

Цифровий підпис виконує ряд важливих функцій у контексті електронного документообігу та захисту інформації:

Ідентифікація підписувача. Завдяки цифровому підпису можливо точно визначити особу, що підписала документ. Це досягається шляхом використання криптографічної пари ключів, пов’язаних із відповідним сертифікатом підпису.

Цілісність інформації. Завдяки цифровому підпису можна впевнено стверджувати, що документ не зазнав змін після його підписання. Навіть найменша зміна вмісту призводить до недійсності підпису

Невідмовність від авторства. Особа, яка підписала документ, не може заперечити свою участь у його створенні, адже лише вона має доступ до відповідного приватного ключа.

Юридична сила. У законодавстві України та багатьох інших країн цифровий підпис визнається рівнозначним власноручному. Це дає змогу використовувати його у державних послугах, фінансових транзакціях, офіційному електронному листуванні тощо.

Рис. 1.1. Приклад цифрового підпису

Окрім основних функцій, цифровий підпис має важливе значення для розвитку електронного урядування, цифрової комерції та трансформації суспільства в цілому. З його допомогою забезпечується ефективна робота електронних систем документообігу, що дозволяє суттєво скоротити витрати часу і ресурсів як для фізичних осіб, так і для юридичних. У процесі цифровізації державних послуг цифровий підпис забезпечує надійний обмін документами між державними установами, бізнесом та громадянами.

Цей інструмент також активно застосовується в електронному банкінгу, системах онлайн-оплат і фінансових транзакціях. Він забезпечує безпечну передачу конфіденційної інформації, що має особливе значення для банківських структур, страхових компаній та інших фінансових організацій. Документи, підписані в електронній формі, мають ту саму юридичну силу, що й паперові, що дозволяє повністю переходити до електронного документообігу без ризику втрати правової значущості.

З технічної точки зору, створення цифрового підпису включає кілька послідовних кроків. Спершу за допомогою хеш-функції з вмісту документа генерується унікальна хеш-сума. Потім ця хеш-сума шифрується приватним ключем користувача, утворюючи цифровий підпис. Під час перевірки документа хеш-сума повторно обчислюється, а сам підпис розшифровується відкритим ключем. Якщо отримані значення збігаються, це означає, що документ не змінювався, а підпис є дійсним.

Для ефективного функціонування цифрового підпису важливою є система інфраструктури відкритих ключів (PKI — Public Key Infrastructure). Вона забезпечує управління криптографічними ключами, видачу та перевірку сертифікатів, а також підтвердження достовірності учасників. У межах PKI діють сертифікаційні центри, які надають, оновлюють або скасовують сертифікати, що забезпечує довіру між сторонами електронної взаємодії.

В Україні впровадження електронного підпису регламентується низкою законодавчих актів, серед яких основними є Закон України «Про електронні довірчі послуги», Закон «Про електронні документи та електронний документообіг» та інші нормативні документи, прийняті відповідними державними органами. Законодавством передбачено три рівні електронного підпису: простий, удосконалений і кваліфікований. Найвищий рівень юридичної сили має саме кваліфікований електронний підпис (КЕП), який створюється із використанням сертифікованих засобів та підтверджується акредитованим центром сертифікації.

Окрім технічних та правових аспектів, варто враховувати і соціально-економічний ефект від впровадження цифрового підпису. Він сприяє зниженню корупційних ризиків, підвищує прозорість процесів у державному та приватному секторах, забезпечує рівний доступ громадян до електронних послуг. У сферах освіти, медицини, логістики, правосуддя цифровий підпис відкриває широкі можливості для дистанційної комунікації, подачі заяв, реєстрації тощо.

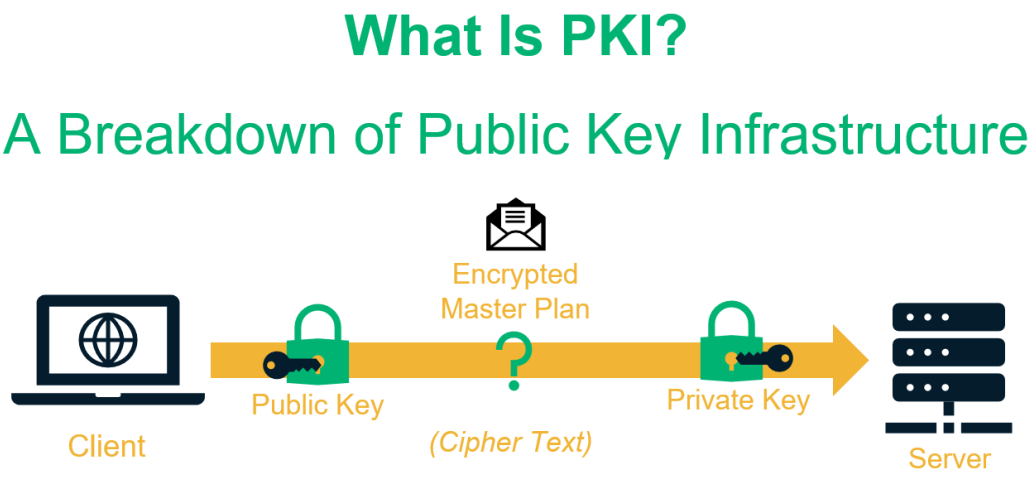

Рис. 1.2. Система інфраструктури відкритих ключів

Цифровий підпис є важливим елементом захищеного та ефективного електронного документообігу. Його впровадження сприяє зміцненню довіри до електронних сервісів, дозволяє зменшити залежність від паперових носіїв та автоматизувати багато процесів у бізнесі, державному секторі та повсякденній діяльності. В умовах активної цифровізації суспільства цифровий підпис стає не лише засобом безпеки, а й основою правового спілкування у цифровому середовищі.

1.2. Аналіз класифікації та характерних ознак основних видів цифрових підписів

В наш час електронний документообіг є невід'ємною складовою щоденної діяльності. Надійне забезпечення справжності та цілісності електронних документів відіграє провідну роль у системі інформаційної безпеки. Одним з основних інструментів, який гарантує автентичність, збереження цілісності та юридичну значущість електронних даних, є цифровий підпис.

Відповідно до положень українського законодавства, зокрема Закону України «Про електронні довірчі послуги», виділяють три ключові типи електронних підписів:

1.Простий електронний підпис (ПЕП)

Під простим електронним підписом маються на увазі електронні дані, що додаються до інших або логічно з ними пов'язані, які використовуються підписувачем з метою підтвердження. Такий підпис може виглядати як логін, пароль, одноразовий код (SMS), або інші засоби, що підтверджують особу.

Основні риси простого електронного підпису (ПЕП) полягають у тому, що він не використовує криптографічні методи захисту, має обмежений правовий статус та застосовується для підписання даних, що не потребують високого рівня захищеності. ПЕП використовують у ситуаціях, коли необхідна певна форма електронного підтвердження, але без високих вимог до безпеки. Він може бути реалізований як:

1. Логін і пароль;

2. Одноразовий код (наприклад, SMS-код);

3. Натискання кнопки «погоджуюсь»;

4 .Сканований підпис.

2.Удосконалений електронний підпис (УЕП)

Цей тип електронного підпису створюється з використанням криптографічних технологій, що забезпечують більш високий рівень безпеки, ніж ПЕП. Він базується на особистому криптографічному ключі, який ідентифікує конкретного користувача.

Характерні особливості такого підпису полягають у тому, що він забезпечує перевірку цілісності документа та достовірності підпису. Його можна використовувати для електронної звітності, укладення договорів та здійснення інших правових дій. При цьому не обов'язково проходити сертифікацію пристроїв, за допомогою яких здійснюється підпис. Ось перелік сфер і прикладів, де може використовуватись Удосконалений електронний підпис (УЕП):

1.Електронний документообіг у бізнесі (Підписання внутрішніх документів, лбмін контрактами між компаніями, затвердження актів виконаних робіт.);

2. Підписання офіційних листів у межах організації;

3. Електронне узгодження договорів та заяв у хмарних сервісах (наприклад, DocuSign, Paperless, SignNow).

3.Кваліфікований електронний підпис (КЕП)

КЕП вважається найвищим рівнем електронного підпису, який має таку саму юридичну силу, як і особистий підпис, відповідно до законодавства України. Такий підпис створюється за допомогою кваліфікованого пристрою та підкріплюється сертифікатом відкритого ключа, виданим акредитованим центром сертифікації.

Цей підпис має повну юридичну силу та визнається державними і судовими органами. Його застосовують під час оформлення офіційної документації, подання податкової звітності, участі в електронних торгах та в інших подібних випадках. Для його використання необхідно застосовувати сертифіковані засоби підпису, а також проходити підтвердження особи через офіційний центр сертифікації. Сфери

де Де можна використовувати Кваліфікований електронний підпис (КЕП)

1. У взаємодії з державними органами;

2. У судових та юридичних процесах;

3. У сфері фінансів та бугалтерії;

4. Через онлайн-сервіси та хмарні платформи.

Порівняння основних видів цифрових підписів

Таблиця 1.1

Критерій	ПЕП	УЕП	КЕП
Криптографія	Немає	Є	Є
Юридична сила	Обмежена	Середня	Повна
Сертифікат	Не потрібен	Може бути	Обов'язковий кваліфікований
Пристрій зберігання	Будь-який (браузер, телефон)	ПК, смартфон	Сертифікований носій (токен, ID карта)
Захист особи	Логін, код, email, SMS	Електронний сертифікат	Фізична ідентифікація/Дія/банківське підтвердження
Сфера застосування	Прості підтвердження	Внутрішній документообіг, бізнес	Держава, суд, податки, закупівлі

1.3. Аналіз використання цифрового підпису в Україні та за кордоном

В Україні правове регулювання цифрового підпису здійснюється через низку законодавчих актів, які визначають правовий статус електронних підписів, їх види та порядок використання. Ці акти встановлюють вимоги до створення, обігу та зберігання електронних документів, а також до захисту персональних даних при використанні електронних підписів. Вони також визначають порядок сертифікації центрів сертифікації ключів та вимоги до програмного забезпечення, що використовується для створення та перевірки електронних підписів. Нижче написаний перелік законодавчих актів:

1**. Закон України "Про електронні довірчі послуги"** (2020 р.): визначає правовий статус цифрових підписів, їх види та порядок використання. Закон передбачає три основні види підписів: простий, удосконалений та кваліфікований.

2. Закон України "Про електронні документи та електронний документообіг": регулює порядок створення, обігу та зберігання електронних документів, а також їх юридичну силу.

3. Постанови Кабінету Міністрів України: визначають порядок сертифікації центрів сертифікації ключів, вимоги до програмного забезпечення та інші аспекти функціонування системи електронного документообігу.

4. Закон України "Про захист персональних даних": забезпечує захист особистої інформації при використанні електронних підписів.

Використання цифрового підпису за кордоном

У державах Європейського Союзу правове регулювання електронного підпису базується на Регламенті ЄС №910/2014, відомому як eIDAS. Цей документ класифікує електронні підписи за рівнем надійності та юридичної сили, а також передбачає механізм взаємного визнання кваліфікованих електронних підписів між країнами-членами. Завдяки цьому кваліфікований підпис прирівнюється до власноручного з точки зору юридичної сили. Важливою складовою є функціонування єдиного реєстру довірених постачальників, що забезпечує стандартизований підхід до сертифікації та використання КЕП у межах усього Союзу. Такий підхід сприяє ефективному розвитку цифрового врядування, електронної економіки та міжнародної взаємодії між державами .

У Сполучених Штатах Америки електронні підписи визнаються на підставі законодавства, яке сформувалося під впливом Закону про електронні підписи в глобальній і національній торгівлі (ESIGN) та типового акту UETA, який діє на рівні окремих штатів. Законодавство США не визначає жорстких вимог до технології чи типів підписів, залишаючи це на розсуд сторін, які укладають угоди.

Завдяки такій гнучкості електронні підписи широко застосовуються в державному управлінні, фінансовому секторі, сфері нерухомості та в електронній комерції .

У різних країнах світу підходи до регулювання цифрового підпису є різноманітними. Наприклад, у Китаї діє централізована система електронного підпису, контрольована державою. В Індії цифрові підписи регламентуються законом про інформаційні технології, згідно з яким їх юридична сила визнається за наявності дійсного цифрового сертифіката . У Канаді правове регулювання базується на законі PIPEDA, який приділяє особливу увагу захисту персональних даних при використанні електронного підпису .

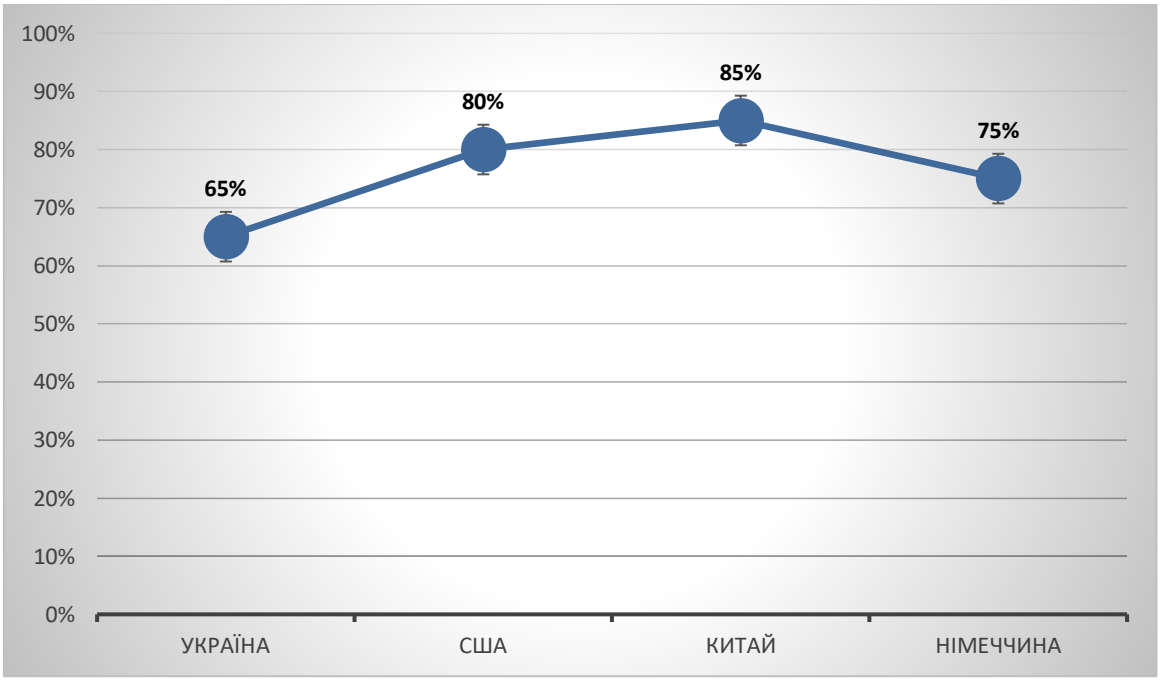

Рис. 1.3. Рівень впровадження електронного підпису в різних країнах

Проблеми та перспективи

Попри досягнення у сфері впровадження кваліфікованих електронних підписів в Україні, ця система залишається перед викликами. Серед основних труднощів слід відзначити обмежений рівень цифрової обізнаності громадян, що ускладнює масове впровадження сучасних електронних сервісів. Крім того, залишається невирішеною проблема міжнародного визнання українських КЕП, що створює бар'єри у взаємодії з іноземними партнерами та організаціями. Ще однією проблемою є нерівномірний рівень інформатизації в різних регіонах та на

підприємствах, що гальмує розвиток електронного документообігу.

Для покращення ситуації вкрай необхідною є активна інтеграція України до загальноєвропейської системи eIDAS, що дозволить забезпечити взаємне визнання підписів на міжнародному рівні. Важливу роль відіграватимуть також інформаційно-освітні кампанії, спрямовані на підвищення рівня цифрової грамотності серед населення. Перспективним напрямом розвитку є також мобільний підпис, особливо в поєднанні з державними цифровими платформами, що зробить використання КЕП більш доступним і зручним для громадян.

Варто зазначити, що ефективність впровадження цифрового підпису значною мірою залежить не лише від наявності законодавства, але й від рівня цифрової трансформації суспільства. Так, у країнах Скандинавії (зокрема Швеції, Данії та Фінляндії) цифровий підпис є інтегрованою частиною електронного урядування. Використання BankID чи NemID дозволяє громадянам не лише підписувати документи, а й здійснювати банківські операції, спілкуватися з державними установами та користуватись медичними сервісами. У таких країнах цифрова ідентичність та електронний підпис функціонують як єдина екосистема, що значно підвищує довіру користувачів до цифрових сервісів.

У Німеччині цифровий підпис активно використовується у сфері охорони здоров’я (електронні рецепти, доступ до медичних записів), у судовій практиці та комунікації з державними установами. Система Bundesdruckerei забезпечує випуск кваліфікованих сертифікатів, а завдяки інтеграції з eIDAS відбувається автоматичне визнання таких підписів іншими країнами ЄС.

На противагу цьому, в деяких країнах цифровий підпис усе ще знаходиться на етапі становлення. Наприклад, у більшості країн Африки або Південної Америки відсутня розгалужена інфраструктура довірчих послуг, а відсутність інституційної підтримки та цифрової грамотності гальмує впровадження технології на національному рівні.

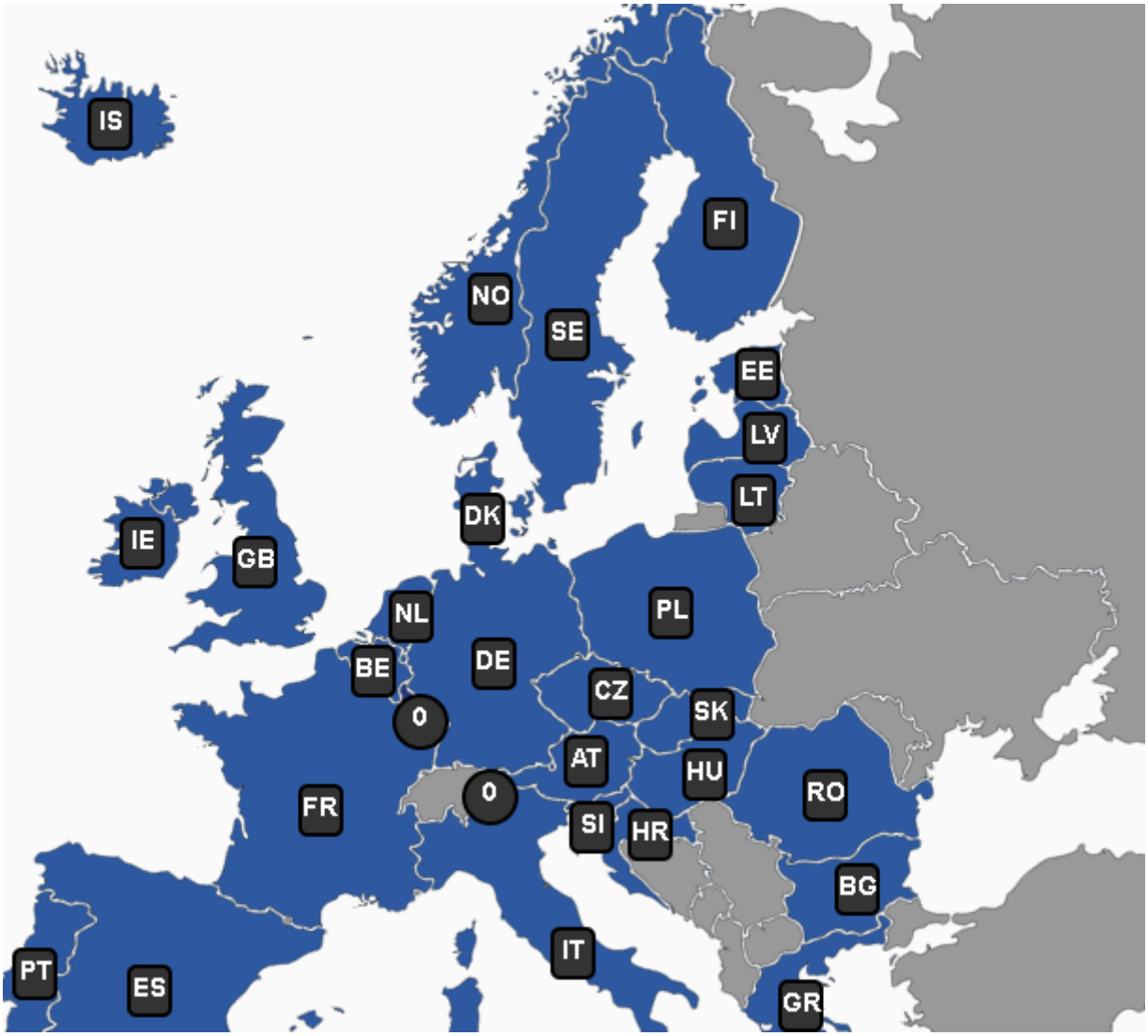

Рис. 1.4. Карта Європи з позначенням країн, що впровадили eIDAS

Інтеграція цифрового підпису у бізнес-процеси

Окрім використання у сфері державного управління, цифровий підпис набув широкого застосування і в бізнес-середовищі. Платформи на зразок DocuSign, Adobe Sign, SignNow та українського сервісу Вчасно.ЕДО стали ключовими інструментами цифрової модернізації підприємств. Вони забезпечують можливість дистанційного підписання документів із юридичною силою, сприяють автоматизації процесів узгодження договорів та дозволяють значно знизити витрати на паперовий документообіг і логістику.

Для міжнародних корпорацій, які функціонують у кількох країнах,

застосування електронного підпису дає змогу оперативно обмінюватися інформацією та укладати угоди між географічно розподіленими офісами. Такий підхід став особливо актуальним у період пандемії COVID-19, коли зросла потреба в безпечних і юридично визнаних засобах підписання документів у віддаленому режимі.

Український досвід та національні перспективи

Україна поступово, але стабільно просувається у напрямку впровадження цифрового підпису. Ініціативи, такі як Національний центр сертифікації ключів (НЦСК), **Дія.Підпис та MobileID**, сприяють активному поширенню електронного підпису як у сфері державного управління, так і в бізнес-середовищі. Зокрема, варто виділити сервіс **Дія.Підпис**, який дозволяє підписувати документи безпосередньо з мобільного пристрою, без потреби у фізичному носії (токені). Завдяки застосуванню біометричної ідентифікації та інтеграції з державними реєстрами, цей інструмент забезпечує високий рівень безпеки та зручності для користувачів.

Водночас для повноцінної інтеграції України до глобального ринку цифрових послуг необхідне міжнародне визнання українських кваліфікованих електронних підписів, зокрема в країнах Європейського Союзу. Це потребує гармонізації криптографічних алгоритмів, процедур сертифікації та приєднання до реєстрів довірених сервісів.

2. АНАЛІЗ МЕТОДІВ ЗАСТОСУВАННЯ ЦИФРОВОГО ПІДПИСУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ

2.1. Принципи роботи цифрового підпису у системах інформаційної безпеки

Цифровий підпис є одним із ключових інструментів забезпечення автентичності, цілісності та невідмовності в рамках сучасних систем захисту інформації. Його функціонування базується на використанні криптографічних механізмів, які дозволяють впевнено ідентифікувати автора повідомлення, підтверджувати його незмінність і захищати від фальсифікацій.

Основи хешування у цифровому підписі

Першим етапом створення цифрового підпису є застосування хеш-функції до повідомлення. Цей процес дозволяє отримати унікальний короткий код (хеш), який відповідає змісту документа. Особливість хеш-функцій полягає в тому, що навіть незначні зміни у вихідному тексті призводять до появи абсолютно іншого хешу. Це дозволяє миттєво виявити спроби зміни інформації після її підписання.

Хеш-функція використовується зокрема у структурах даних — хеш-таблицях, широко вживаних у програмному забезпеченні для швидкого пошуку даних. Хеш-функції використовуються для оптимізації таблиць та баз даних користуючись з того, що в однакових записів однакові значення хеш-функції.

Хеш-функція ставить у відповідність іменам ціле число від 0 до 15. Є суперечність (колізія) між «John Smith» та «Sandra Dee», яким відповідає однакове значення.

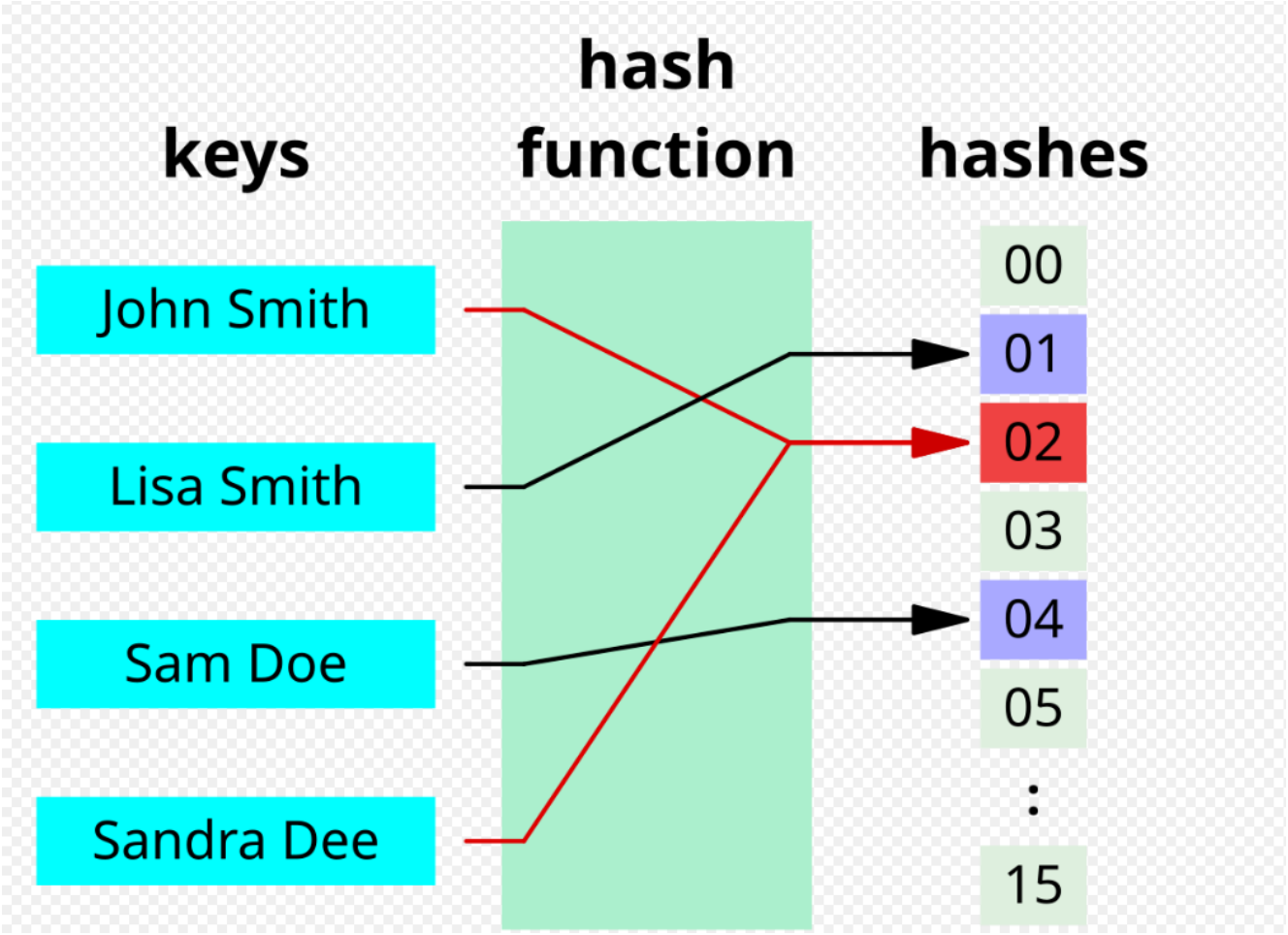

Рис. 2.1. Приклад роботи Хеш-функції

Механізм асиметричного шифрування

Цифровий підпис використовує пару криптографічних ключів — відкритий і закритий. Автор документа шифрує згенерований хеш за допомогою свого приватного ключа, створюючи підпис. Отримувач у свою чергу перевіряє підпис, розшифровуючи його відкритим ключем підписанта. Якщо хеш із розшифрованого підпису співпадає з хешем самого документа — підпис вважається дійсним. Такий підхід виключає можливість підробки, адже лише власник приватного ключа може створити справжній підпис.

Роль PKI в екосистемі цифрового підпису

Інфраструктура відкритих ключів (PKI) є базовим компонентом, який забезпечує надійність і довіру при роботі з цифровими підписами. Вона включає сертифікаційні центри, що видають сертифікати автентичності, механізми відкликання ключів, а також правила користування криптографічними засобами. PKI дозволяє перевірити справжність підписанта навіть у випадках, коли сторони не мають попередньої довіри між собою.

У корпоративному середовищі цифрові підписи широко впроваджуються в різноманітні IT-рішення, що забезпечують безпечну та ефективну роботу з електронними даними. Зокрема, вони використовуються у системах електронного документообігу для підписання як внутрішніх, так і зовнішніх документів, у засобах контролю доступу для підтвердження ідентичності користувачів, у рішеннях для зберігання інформації з метою захисту архівних даних, а також у звітних і фінансових системах для перевірки достовірності поданої інформації. Успішне впровадження цифрового підпису залежить не лише від технічної реалізації, але й від наявності чітко сформульованих внутрішніх процедур його застосування, а також належної підготовки персоналу.

Надійність цифрового підпису безпосередньо пов’язана з безпечним зберіганням приватного ключа. У разі, якщо цей ключ потрапить до рук зловмисника, існує ризик створення підроблених підписів, що компрометує всю систему безпеки. Щоб уникнути подібних загроз, використовуються апаратні носії, такі як токени чи смарт-карти, а також методи багатофакторної автентифікації та спеціалізоване програмне забезпечення, яке не дозволяє копіювати або витягувати закритий ключ із пристрою.

Сучасні технологічні тенденції вказують на необхідність адаптації цифрових підписів до нових викликів. Одним із таких викликів є інтеграція цифрового підпису в блокчейн-інфраструктури, де кожна транзакція підписується та зберігається в незмінному вигляді, що гарантує її прозорість і достовірність. Іншим напрямом розвитку є створення постквантових алгоритмів підпису, здатних протистояти потенційним загрозам з боку квантових комп’ютерів, які можуть

вивести з ладу класичні криптографічні схеми.

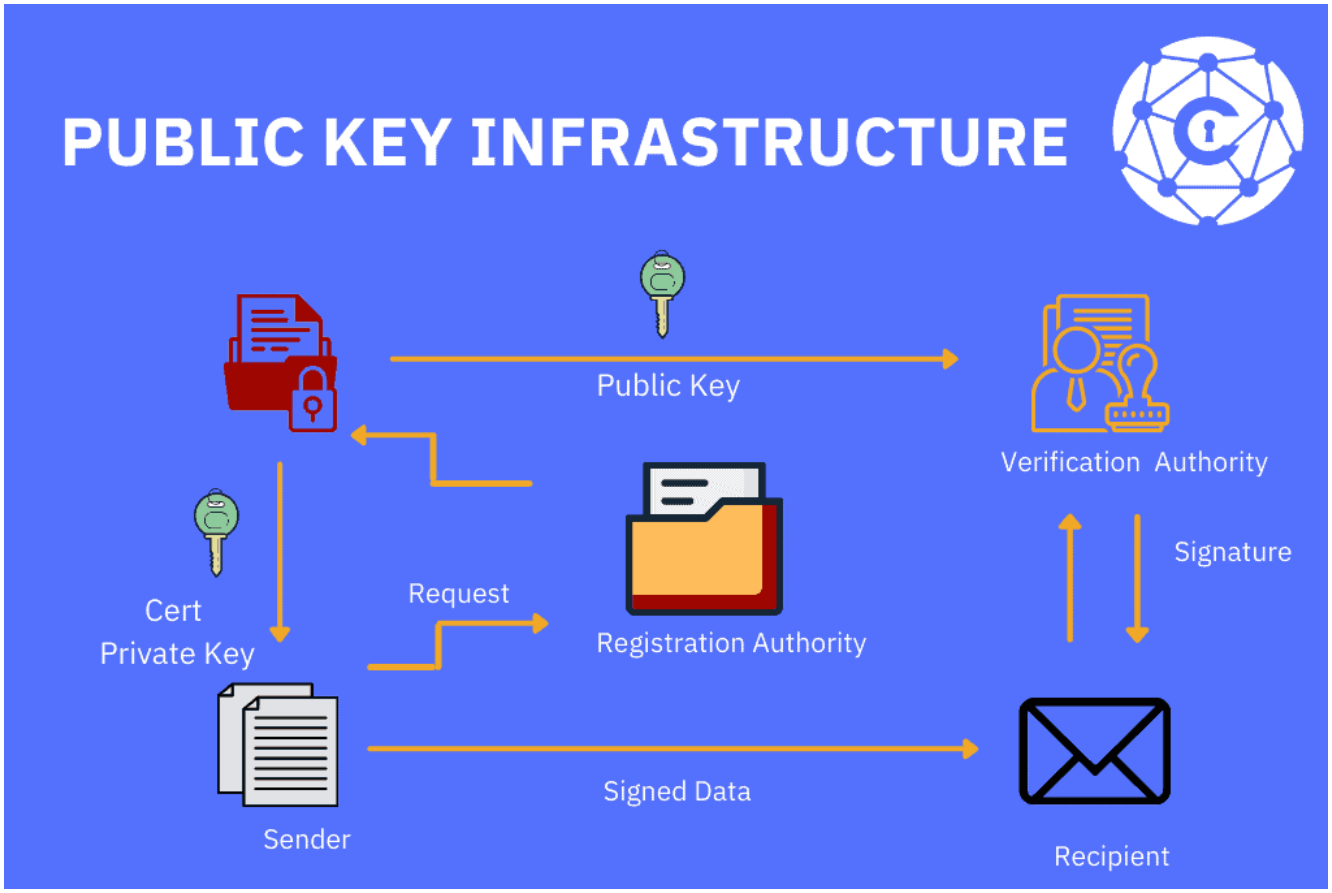

Рис. 2.2. Схема роботи інфраструктури відкритих ключів (PKI) у процесі цифрового підпису

Криптографічні алгоритми електронного підпису

Фундаментом цифрового підпису є використання асиметричної криптографії. Серед найбільш поширених алгоритмів можна виділити RSA, DSA та ECDSA.

RSA (Rivest–Shamir–Adleman) є одним із перших публічних алгоритмів, застосовуваних для створення цифрового підпису. Його стійкість забезпечується складністю розкладання великих чисел на прості множники. Для відповідності сучасним вимогам безпеки рекомендується використовувати ключі довжиною не менш ніж 2048 біт.

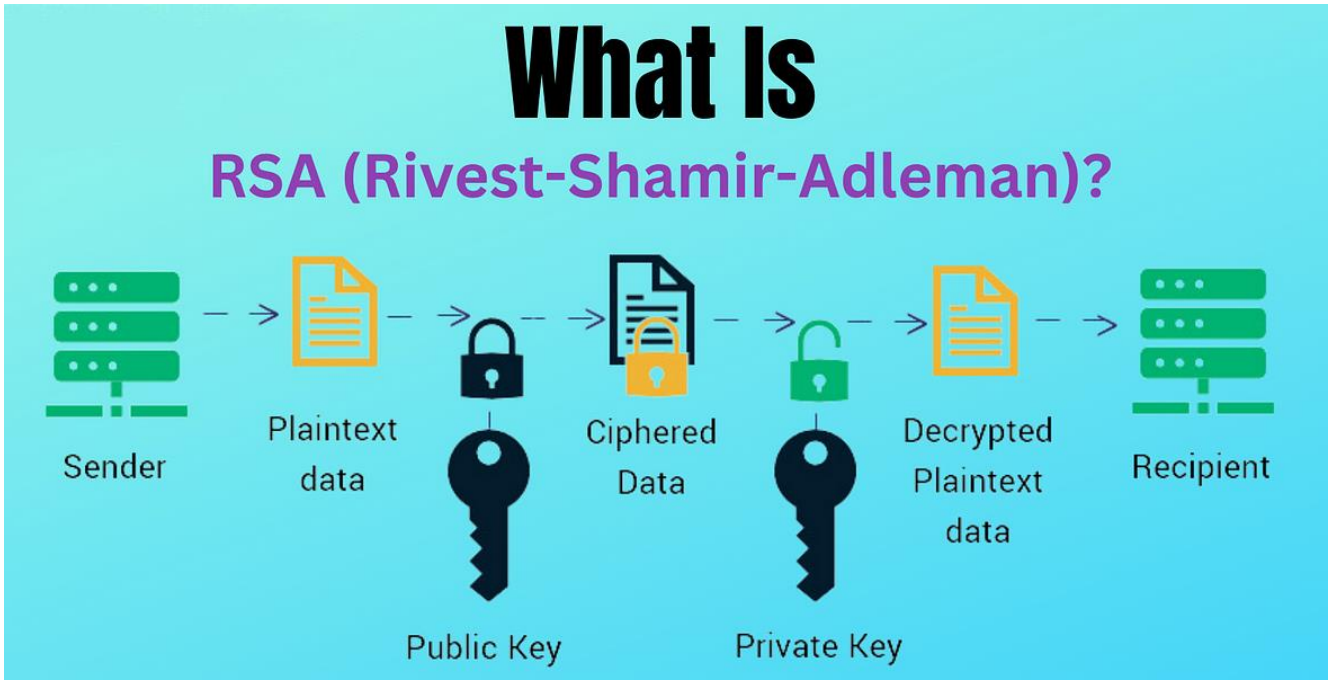

Рис.2.3. Схема роботи алгоритму RSA у безпеці даних

1.Sender (Відправник) — надсилає повідомлення (наприклад, через мережу).

2.Plaintext Data (Відкритий текст) — оригінальні дані, які потрібно захистити.

3.Public Key (Публічний ключ) — використовується для шифрування даних. Публічний ключ отримувача доступний будь-кому.

4.Ciphered Data (Зашифровані дані) — результат шифрування відкритого тексту публічним ключем.

5.Private Key (Приватний ключ) — використовується для розшифрування. Знаходиться лише у власника (отримувача).

6.Decrypted Plaintext Data (Розшифрований текст) — після дешифрування, дані знову стають доступними у відкритому вигляді.

7.Recipient (Одержувач) — отримує повідомлення у зрозумілому вигляді.

Ключова особливість RSA:

Шифрування виконується за допомогою публічного ключа, а розшифрування —приватного, що забезпечує безпечну передачу інформації навіть у незахищених каналах зв’язку.

DSA (Digital Signature Algorithm) був стандартизований Національним інститутом стандартів і технологій США (NIST) і ґрунтується на складності

обчислення дискретного логарифму в межах певного модуля. На відміну від RSA, DSA забезпечує більш швидке формування підпису, але його перевірка займає більше часу.

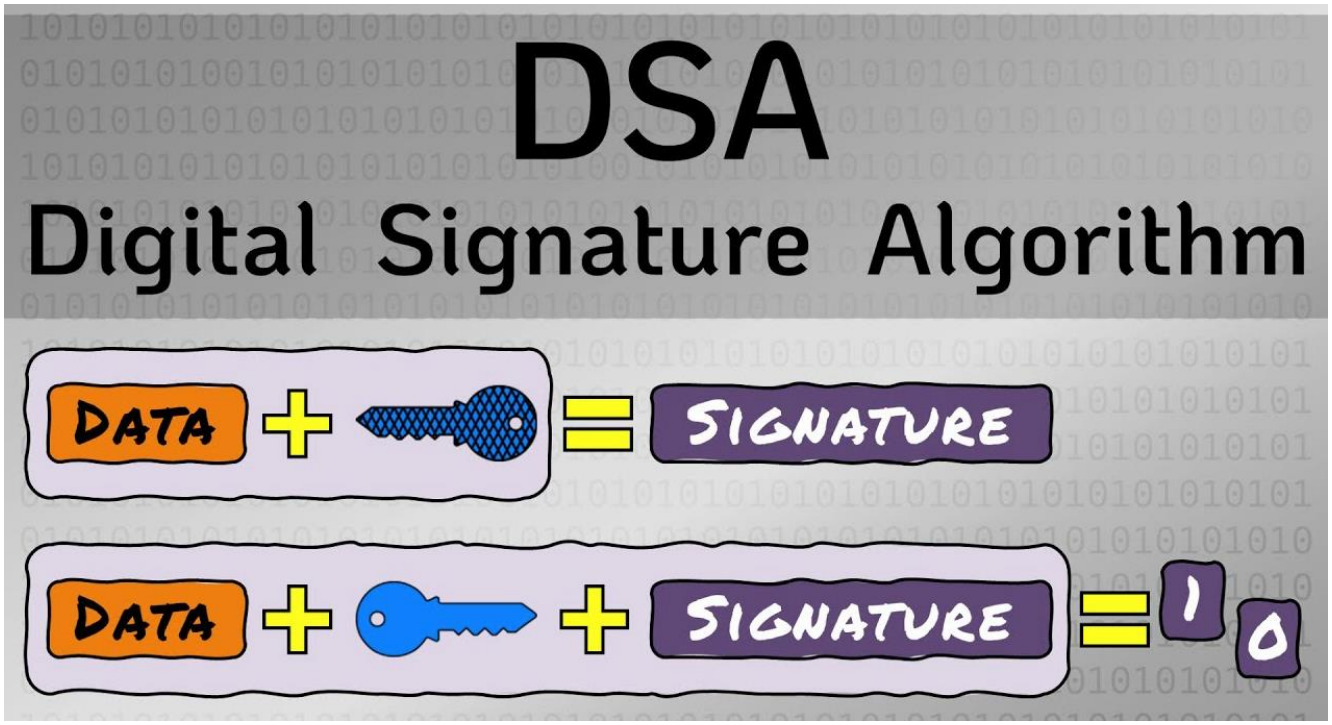

Рис.2.4. Схема роботи цифрового підпису DSA

1.Верхній блок — створення підпису:

DATA + секретний ключ = Підпис

Відправник використовує дані (повідомлення) і свій закритий ключ (синій ключ з лініями) для створення цифрового підпису.

Цей підпис гарантує, що дані справді походять від власника ключа і не були змінені.

2. Нижній блок — перевірка підпису: DATA + відкритий ключ + Підпис = TRUE/FALSE (1 або 0)

Отримувач використовує: Дані (DATA), відкритий ключ (світло-блакитний ключ), цифровий підпис —щоб перевірити, чи справжній підпис.

Результат перевірки — ☑ (1), якщо все правильно, або ✕ (0), якщо підпис підроблений або повідомлення змінено.

ECDSA (Elliptic Curve Digital Signature Algorithm) — це сучасний тип алгоритму підпису, що базується на використанні еліптичних кривих. Його головна перевага полягає у високому рівні безпеки при меншій довжині ключів. Наприклад, 256-бітний ключ ECDSA забезпечує рівень захисту, еквівалентний 3072-бітному ключу RSA. Через це ECDSA широко застосовується у сфері мобільних технологій, фінансових сервісів та в системах на базі блокчейну.

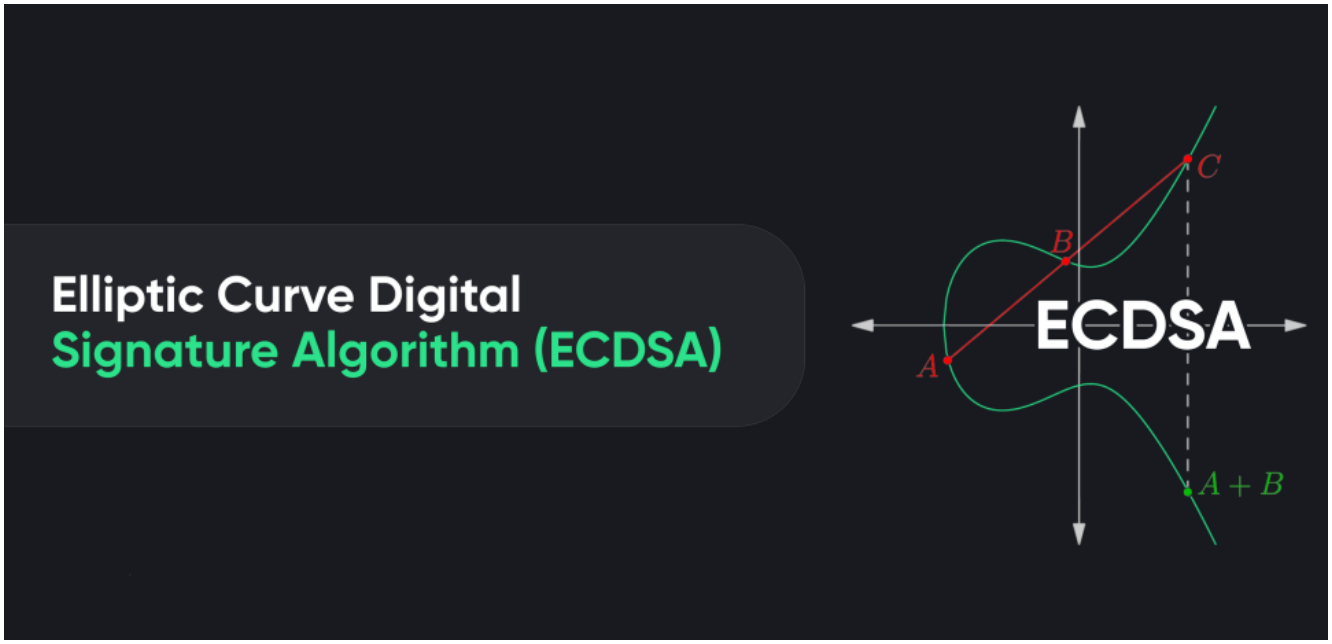

Рис. 2.5. Візуалізація алгоритму цифрового підпису ECDSA

Ця картинка ілюструє принцип роботи алгоритму цифрового підпису на основі еліптичних кривих — ECDSA (Elliptic Curve Digital Signature Algorithm).

- A і B — точки на еліптичній кривій.
- Пряма, що з'єднує A і B, перетинає криву в третій точці C.
- Відбиття цієї точки щодо осі X (пунктирна лінія) дає A + B, що є результатом операції додавання точок на еліптичній кривій.

В контексті цифрового підпису це означає що ECDSA використовує складні математичні операції над точками на еліптичній кривій для створення та перевірки

підписів:

- Всі обчислення базуються на складності знаходження дискретного логарифма на еліптичній кривій, що забезпечує високу криптографічну стійкість навіть при невеликій довжині ключа.
- Наприклад, ключ 256 біт у ECDSA надає схожий рівень безпеки, як 3072-бітовий RSA.

Порівняльна характеристика криптографічних алгоритмів цифрового підпису

Таблиця 2.1

Алгоритм	Тип криптографії	Рівень безпеки	Швидкість створення підпису	Швидкість перевірки підпису	Рекомендована довжина ключа	Типові сфери застосування
RSA	Асиметричний	Високий (при 2048+ біт)	Середня	Висока	2048-3072 біт	Підпис документів, SSL/TLS, PGP
DSA	Асиметричний	Високий (при 2048+ біт)	Висока	Низька	2048 біт	Державні підписи, сертифікація
ECDSA	Асиметричний (еліптичні криві)	Дуже високий (при 256 біт)	Висока	Висока	256 ≈ 3072 біт RSA	Блокчейн, мобільні системи, електронні гаманці

Хоча цифрові підписи вважаються надійними, вони не є абсолютно захищеними. Серед основних загроз — компрометація приватного ключа, атаки на хеш-функції та експлуатація вразливостей у процесі підписання.

Наприклад, використання ненадійної хеш-функції, яка схильна до колізій (як це сталося з MD5), може дозволити зловмиснику змінити вміст документа без порушення цілісності самого підпису. Іншим поширеним ризиком є replay-атака, коли справжній підпис перехоплюється й повторно використовується для іншого документа.

Також існує ризик, пов’язаний із неналежним зберіганням приватного ключа. У разі його викрадення стороння особа зможе підробляти підписи, видаючи їх за

справжні. Тому для безпечного зберігання приватного ключа рекомендується застосовувати спеціальні апаратні засоби, такі як токени, смарт-карти чи апаратні модулі безпеки (HSM).

Підсумовуючи викладене, слід зазначити, що цифровий підпис є одним із ключових інструментів забезпечення інформаційної безпеки в електронному середовищі. Його функціонування базується на принципах асиметричної криптографії, що дозволяє гарантувати автентичність, цілісність і незаперечність даних.

Алгоритми цифрового підпису, такі як RSA, DSA та ECDSA, відіграють вирішальну роль у реалізації криптографічного захисту. Кожен із них має свої особливості, переваги та сфери застосування, але всі вони спрямовані на досягнення одного — створення надійного механізму підтвердження особи відправника та захисту від несанкціонованих змін інформації.

Важливо також враховувати потенційні вразливості цифрового підпису, зокрема можливість компрометації приватного ключа, атаки на хеш-функції чи повторне використання перехоплених підписів. З метою мінімізації таких ризиків слід використовувати сучасні, перевірені криптографічні протоколи та засоби захищеного зберігання ключової інформації, зокрема апаратні токени,смарт-карти.

Таким чином, цифровий підпис є не лише технічним засобом захисту, але й інструментом довіри, який забезпечує безпеку критично важливих інформаційних процесів у багатьох галузях — від державного управління до фінансових та комерційних систем.

2.2. Огляд криптографічних алгоритмів, що використовуються для цифрового підпису

Цифровий підпис є одним із ключових засобів забезпечення автентичності, цілісності та незаперечності електронних документів і повідомлень. Для його реалізації застосовується низка криптографічних методів, заснованих на вирішенні

складних математичних задач. У цьому розділі буде представлено додатковий огляд алгоритмів і методів, які відіграють важливу роль у сучасних системах цифрового підпису.

Рис. 2.6. Основний принцип асиметричної криптографії

Відкритий ключ (оранжевий контур)

Призначення: використовується для зашифрування даних.

Надається всім — будь-хто може скористатися ним для шифрування повідомлення.

Процес шифрування:

Початкові (оригінальні) дані беруться користувачем.

Вони зашифровуються за допомогою відкритого ключа.

В результаті — виходять зашифровані дані, які можна передавати через незахищені канали.

Закритий ключ (синій контур)

Призначення: використовується для розшифрування зашифрованих даних.

Зберігається в таємниці власником ключової пари.

Процес розшифрування:

Отримувач використовує свій закритий ключ, щоб розшифрувати отримані дані. Він відновлює оригінальні дані.

Алгоритми на основі еліптичних кривих

Криптографія, що базується на еліптичних кривих (ECC — Elliptic Curve Cryptography), стрімко набуває популярності завдяки здатності забезпечувати високий рівень захисту при використанні коротших ключів порівняно з класичними алгоритмами на кшталт RSA чи DSA.

Одним із найпоширеніших представників цієї категорії є алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm). Його головна перевага полягає в тому, що для досягнення того самого рівня безпеки, що й RSA, він потребує значно меншого обсягу ключів і менших обчислювальних ресурсів. Зокрема, для криптозахисту на рівні 128 біт достатньо 256-бітного ECC-ключа, тоді як RSA для цього знадобиться 3072 біти.

Алгоритми на основі еліптичних кривих активно застосовуються у сучасних протоколах захисту інформації, серед яких **TLS 1.3**, **SSH**, **IPsec**, а також у криптовалютних системах на зразок *Bitcoin, Ethereum* та інших децентралізованих мережах.

Основні переваги ECC-алгоритмів:

1.Менші розміри ключів при збереженні криптостійкості;

2.Підвищена продуктивність на пристроях із обмеженими ресурсами;

3.Скорочення обсягу даних, що передаються.

До недоліків таких алгоритмів відносять технічну складність їх реалізації та необхідність уважного вибору параметрів кривих, оскільки вразливість цих параметрів може призвести до компрометації всієї системи.

Алгоритми постквантової криптографії

У зв’язку зі стрімким розвитком квантових технологій традиційні криптографічні алгоритми опинилися під потенційною загрозою, оскільки квантові комп’ютери здатні ефективно вирішувати задачі, що лежать в основі **RSA**, **DSA** та

ECC, зокрема факторизацію та обчислення дискретного логарифму. Ця проблема зумовила активний розвиток напряму постквантової криптографії **(PQC)**.

До найбільш перспективних алгоритмів цифрового підпису, стійких до квантових атак, належать:

SPHINCS+ — алгоритм, який базується виключно на хеш-функціях і не залежить від математичних задач, що можуть бути вирішені квантовим комп'ютером.

Dilithium — представник криптографії на решітках, включений до фіналістів конкурсу NIST зі стандартизації постквантових алгоритмів.

Falcon — ще один алгоритм на основі решіток, який вирізняється високою ефективністю та компактними розмірами підписів.

Особливістю цих алгоритмів є те, що вони забезпечують розміри ключів і підписів, співмірні з традиційними системами, водночас залишаючись захищеними від квантових обчислень.

Алгоритми цифрового підпису на основі хеш-функцій

До окремої категорії належать алгоритми, що використовують криптографічні хеш-функції для формування підписів. Їх принцип ґрунтується на побудові хеш-ланцюгів і хеш-дерев, що дозволяє створювати надійні односторонні функції.

Яскравими представниками цієї групи є:

Lamport Signature — один із перших практичних алгоритмів цифрового підпису. Його основним недоліком є значна довжина підпису та обмеження на одноразове використання ключів.

Merkle Signature Scheme (MSS) — удосконалення схеми Лампорта, що дозволяє створювати багаторазові підписи за допомогою хеш-дерев.

Попри певні обмеження, ці алгоритми вважаються перспективними для постквантової криптографії через їхню стійкість до квантових атак.

Алгоритми з компактним підписом

В умовах використання цифрового підпису на пристроях із обмеженими ресурсами, зокрема в смарт-картах, IoT-пристроях і мобільних системах, важливе

значення мають алгоритми з невеликим розміром підпису. Серед них особливе місце посідає:

BLS (Boneh–Lynn–Shacham Signature) — дозволяє формувати надзвичайно компактні підписи, що займають лише кілька десятків байт завдяки використанню парних криптографічних операцій на еліптичних кривих. Окрім цього, BLS підтримує можливість агрегування кількох підписів в один.

Основні переваги:

1.Мінімальний обсяг підписів;

2.Підтримка агрегування підписів;

3.Високий рівень криптостійкості.

Недоліки:

1.Складність реалізації;

2.Необхідність забезпечення підтримки парних операцій на еліптичних кривих.

Агреговані та групові цифрові підписи

Агреговані цифрові підписи дозволяють поєднувати кілька підписів, створених різними користувачами, в один компактний підпис. Це особливо корисно для зменшення обсягів переданих даних і прискорення перевірки підписів.

Яскравим прикладом є Aggregate BLS Signatures, що знайшли широке застосування в сучасних блокчейн-мережах другого покоління.

Групові цифрові підписи дають змогу будь-якому члену певної групи підписати повідомлення так, що перевіряючий зможе переконатися у справжності підпису, але не зможе визначити, хто саме його створив. Такі технології застосовуються в системах анонімного голосування, захищених форумах і приватних криптовалютних мережах, зокрема в *Monero*.

Порівняльний аналіз сучасних алгоритмів

Таблиця 2.2

	Довжина	**Розмір**	**Стійкість до**	**Швидкість**

Алгоритм	ключа (біт)	підпису (байт)	квантових атак	створення/перевірки
RSA (3072)	3072	384	Ні	Середня / Середня
ECDSA(256)	256	64	Ні	Висока / Висока
Dilithium II	~2048	2040	Так	Висока / Висока
SPHINCS+	~8192	7856	Так	Низька / Середня
BLS (256)	256	32	Ні	Висока / Висока

Ця таблиця демонструє, що вибір алгоритму залежить від пріоритетів системи — захисту від квантових атак, швидкості чи розміру підпису.

Крім базових алгоритмів цифрового підпису, існують криптографічні схеми, які реалізують додаткові функції:

Підпис із відкладеним розкриттям (Timed-release signatures) — дає змогу створювати підпис, який можна перевірити лише після настання певної дати або часу. Такий підхід застосовується, наприклад, у системах електронних торгів і timed smart contracts.

Підпис із підтвердженням (Confirmable signatures) — дозволяє одержувачу переконатися в достовірності підпису, але без можливості підтвердити його третій стороні без згоди підписувача. Використовується в електронному голосуванні або приватних угодах.

Підпис з відмовою (Undeniable signatures) — автор підпису не може заперечити факт його створення, однак верифікація такого підпису вимагає участі самого підписувача. Подібні схеми використовуються для підписання конфіденційних документів.

Анонімні підписи (Anonymous signatures) — дають можливість здійснювати підпис без розкриття особистості підписувача. Такі рішення застосовують у приватних блокчейн-проєктах та системах захищеного електронного голосування.

На практиці вибір алгоритму цифрового підпису залежить не тільки від рівня криптостійкості, а й від технічних параметрів: швидкості генерації ключів і підпису, часу перевірки, обсягу пам’яті та енергоспоживання.

Як приклад можна розглянути:

RSA з довжиною ключа 3072 біти потребує значно більше ресурсів і пам’яті, ніж **ECDSA** з 256 бітами за однакового рівня безпеки. **SPHINCS+**, хоч і стійкий до квантових атак, формує великі за розміром підписи (до 8 КБ), що ускладнює його використання в мобільних або IoT-пристроях. Алгоритм **BLS** дозволяє об’єднувати підписи кількох користувачів, що особливо зручно для децентралізованих систем, наприклад у мережі Ethereum 2.0.

Практичне порівняння показників роботи алгоритмів в умовах серверного середовища

Таблиця 2.3

Алгоритм	**Генерація ключа**	**Створення підпису**	**Перевірка підпису**	**Розмір підпису**
RSA (2072 біт)	800 мс	5 мс	1 мс	384 байти
ECDSA (256 біт)	50 мс	0.5 мс	0.5 мс	64 байти
BLS (256 біт)	100 мс	1 мс	0.8 мс	32 байти
SPHINCS+	2000 мс	20 мс	10 мс	7-8 КБ

Алгоритми цифрового підпису активно використовуються в багатьох галузях. Вони забезпечують надійність і юридичну значимість електронного документообігу, дозволяють підтверджувати достовірність фінансових операцій у банківській сфері та авторизовувати електронні платежі. У системах електронного врядування цифровий підпис гарантує захищеність електронних звернень, голосувань та петицій. Крім того, ці алгоритми відіграють важливу роль в організації інформаційної безпеки підприємств, де їх використовують для захисту службового листування, конфіденційних даних і системних журналів. Окреме значення цифрові підписи мають у технологіях блокчейну та криптовалют, де вони відповідають за підтвердження транзакцій та створення смарт-контрактів.

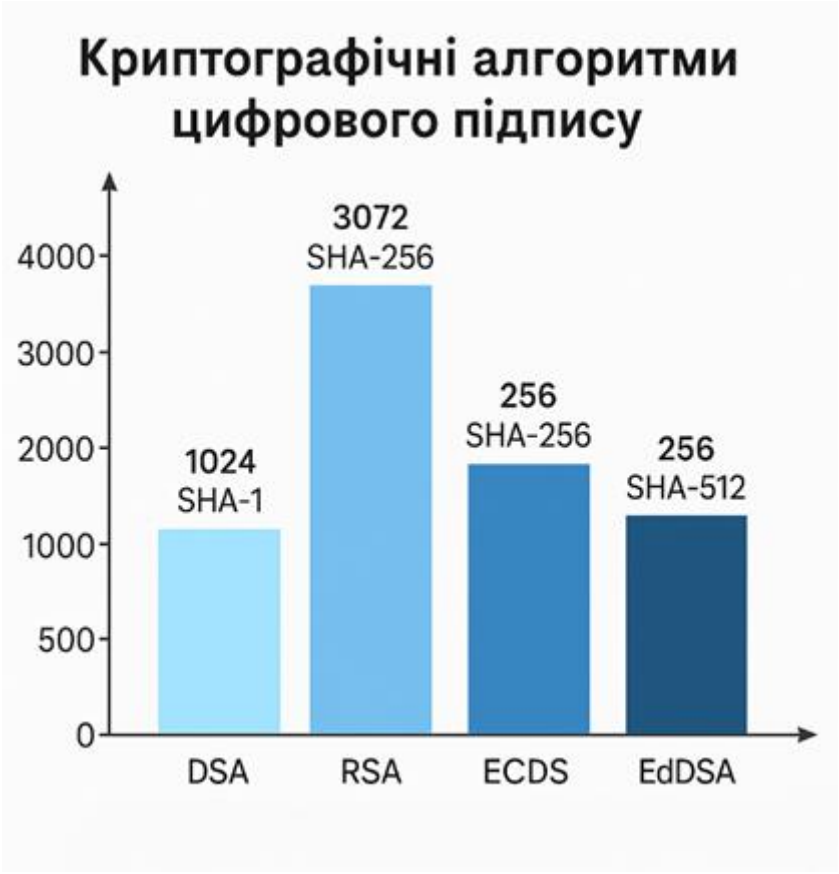

Рис. 2.7. Аналіз алгоритмів цифрового підпису за довжиною ключа та хеш-функцією

Цифри на осі Y на даному малюнку позначають довжину криптографічного ключа в бітах, що використовується відповідним алгоритмом цифрового підпису для забезпечення заданого рівня безпеки.

2.3. Порівняльний аналіз методів впровадження цифрового підпису в організаційних середовищах

У сучасну епоху цифрової трансформації бізнес-процесів, державного управління та суспільного життя ***цифровий підпис*** (ЦП) набув значення не лише як технологічне рішення, а як основний компонент системи інформаційної безпеки, юридичної довіри та електронного документообігу. Його застосування дає змогу здійснювати ідентифікацію особи, перевіряти цілісність переданих даних і

забезпечувати юридичну силу документів. Обрання оптимального способу реалізації ЦП суттєво впливає на продуктивність роботи організацій, рівень захисту цифрових операцій та відповідність нормативно-правовим вимогам.

Класифікація способів впровадження цифрового підпису

Існує кілька підходів до реалізації цифрового підпису, які відрізняються способом зберігання й обробки криптографічних ключів, рівнем інтеграції в робочі процеси та типом взаємодії користувача з системою:

Програмні засоби (Software-based PKI) – передбачають використання програмних рішень, які зберігають ключі безпосередньо на пристрої користувача (жорсткий диск, захищена директорія).

Апаратні рішення (Hardware-based PKI) – базуються на використанні токенів, смарт-карт та інших фізичних носіїв, що гарантують захищене середовище для зберігання ключів.

Хмарні сервіси (Cloud-based signatures) – передбачають зберігання ключів у віддалених захищених модулях на серверах провайдерів довірчих послуг.

Мобільні підписи (Mobile ID) – забезпечують можливість підпису документів через мобільні застосунки або SIM-карти із вбудованим модулем ідентифікації.

API-інтеграція – дозволяє безпосередньо вбудовувати функціонал ЦП у внутрішні інформаційні системи компанії за допомогою прикладних інтерфейсів.

Кожен із зазначених методів має власні переваги та обмеження, які стають очевидними лише при розгортанні в реальному організаційному середовищі.

Для здійснення об'єктивного порівняння ефективності різних методів впровадження цифрового підпису необхідно враховувати низку ключових характеристик.

Насамперед, важливим є **рівень інформаційної безпеки**, який визначається захистом криптографічних ключів, стійкістю до кібератак та якістю використовуваних алгоритмів шифрування.

Не менш значущою є **зручність використання**, що залежить від простоти роботи з інтерфейсом, швидкості здійснення операцій та потреби у навчанні

персоналу.

Важливо також оцінити **масштабованість** рішення, тобто його здатність ефективно функціонувати за умов збільшення кількості користувачів чи обсягів документообігу.

Порівняльна характеристика підходів

Таблиця 2.4

Метод	Безпека	Зручність	Масштабованість	Сумісність	Вартість	Відповідність
Програмні рішення	Середня	Висока	Висока	Висока	Низька	Висока
Апаратні рішення	Висока	Середня	Обмежена	Середня	Висока	Висока
Хмарні сервіси	Висока	Висока	Висока	Висока	Середня	Висока
Мобільні підписи	Висока	Висока	Висока	Середня	Середня	Висока
API-інтеграція	Варіюється	Висока	Висока	Висока	Висока	Висока

Аналіз практичних реалізацій

Програмні рішення.

Цей тип підходу популярний серед малого бізнесу, оскільки не вимагає складної інфраструктури. Ключі користувачів зберігаються у файлових контейнерах, наприклад, у Windows CryptoAPI. Основна перевага — легкість у встановленні й використанні, проте існує ризик доступу до ключів зі сторони шкідливого ПЗ.

Приклад: бухгалтерські програми на зразок «M.E.Doc» активно використовують

локальні сертифікати для підпису звітів.

Апаратні рішення.

Ці рішення забезпечують максимальний рівень захисту, оскільки ключі ніколи не залишають захищеного носія. Застосовуються в банківських структурах, податкових органах та установах з підвищеними вимогами до безпеки.

Приклад: НБУ, ДПС та інші державні органи користуються токенами та смарт-картами для службовців.

Хмарні сервіси.

Використовують модулі HSM (Hardware Security Module), у яких ключі зберігаються у зашифрованому вигляді. Користувачі підписують документи онлайн без потреби в інсталяції додаткового ПЗ.

Приклад: сервіс «Вчасно.ЕЦП» дозволяє бізнесу швидко й масово підписувати договори, рахунки-фактури, акти тощо.

Мобільні підписи.

Цей підхід активно розвивається у державах із сильною цифровою інфраструктурою. Підпис активується через мобільний додаток або Mobile ID.

Приклад: в Естонії функціонує система e-Residency, що дозволяє дистанційне підписання документів навіть для іноземних громадян.

API-інтеграція.

Забезпечує найглибший рівень впровадження, дозволяючи інтегрувати ЦП у внутрішні процеси компанії (наприклад, workflow, CRM, EDM-системи).

Приклад: системи DocuSign, Adobe Sign або українська платформа «Трембіта» дозволяють державним органам автоматизувати послуги.

Рис. 2.8. Візуалізація способів інтеграції цифрового підпису

На малюнку зображено чотири основні підходи до впровадження цифрового підпису в середовище організації: використання програмного забезпечення, апаратних рішень, хмарних сервісів і мобільних технологій. Кожен підхід представлено у вигляді окремого значка з відповідною графічною позначкою, що відображає його взаємодію з основною інформаційною системою установи. Інфографіка чітко показує місце кожного з варіантів у загальній системі впровадження цифрового підпису, а також дає можливість порівняти їхню інтеграцію у внутрішню структуру процесів.

Системні труднощі у впровадженні цифрового підпису

Попри очевидні переваги, впровадження цифрового підпису в організаційне середовище нерідко супроводжується низкою труднощів. Серед них – як технічні, так і поведінкові бар’єри. Зокрема, працівники можуть демонструвати опір змінам через брак мотивації або небажання освоювати нові інструменти, які здаються їм зайвими або складними. У деяких установах проблема посилюється недостатнім

рівнем цифрової грамотності, що ускладнює ефективне використання сучасних технологій. Крім того, ринок рішень для електронного підпису досі залишається фрагментованим: різноманітність форматів і відсутність уніфікованих стандартів створюють труднощі з сумісністю між системами. Ще одним викликом є правова неоднозначність – невідповідність між національними і міжнародними нормами може заважати міжнародному документообігу.

Подолання цих бар'єрів потребує системного підходу: доцільно починати з пілотних ініціатив, поступово розширюючи масштаб впровадження, супроводжуючи процес навчанням персоналу, технічною підтримкою та постійним моніторингом прогресу.

3. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ ЦИФРОВОГО ПІДПИСУ В ОРГАНІЗАЦІЇ

3.1. Визначення вимог до інфраструктури електронного підпису

Інфраструктура електронного підпису (ІЕП), зокрема її ключова складова —

інфраструктура відкритих ключів (PKI), відіграє вирішальну роль у забезпеченні кіберзахисту організацій. Вона забезпечує функціональність створення, розповсюдження, управління життєвим циклом і анулювання сертифікатів, а також дозволяє перевірити автентичність підписаних електронних даних. Для її повноцінної роботи необхідно сформулювати і реалізувати вимоги технічного, організаційного, правового та функціонального характеру, які забезпечать стабільність, безпеку та масштабованість електронного підпису.

Рис.3.1. Життєвий цикл сертифіката у PKI

Цей малюнок ілюструє етапи існування цифрового сертифіката в межах інфраструктури відкритих ключів (PKI — Public Key Infrastructure). Вона допомагає зрозуміти, як створюється, використовується та припиняється дія сертифіката.

Технічні аспекти

Надійне функціонування інфраструктури електронного підпису потребує

дотримання низки технічних вимог. Однією з базових є безпечне збереження ключової інформації. Приватні ключі повинні зберігатися в захищених середовищах — як апаратних, так і програмних. Серед ефективних рішень — використання смарт-карт, криптографічних токенів або пристроїв з апаратними модулями захисту (HSM).

Порівняння технічних рішень для захисту ключів

Таблиця 3.1

Рішення	Опис	Рівень захисту	Приклад використання
Смарт карта	Зберігає ключ у мікросхемі	Високий	Банки, держструктури
Криптотокен	USB-пристрій для зберігання ключа	Високий	КЕП в Україні
HSM-модуль	Апаратний сервер шифрування	Дуже високий	Великі підприємства
Програмне зберігання	У файловій системі пк	Середній	Малий бізнес

Система повинна працювати на основі сучасних криптоалгоритмів, які гарантують високу стійкість до атак. До таких належать RSA з довжиною ключа не менше 2048 біт, еліптична криптографія (ECDSA), а також новітні постквантові підходи, які тільки набирають поширення.

Безперебійна робота ІЕП забезпечується шляхом впровадження систем резервування, балансування навантаження і використання кластерних технологій. Це дозволяє забезпечити високу доступність сервісу та зменшити ймовірність технічних збоїв.

Не менш важливою є сумісність інфраструктури з існуючим програмним забезпеченням та сервісами. Для цього використовуються відкриті стандарти, такі як X.509, PKCS#7 або XMLDSig, які гарантують можливість взаємодії з іншими IT-системами.

Крім того, система має забезпечувати ведення детального аудиту. Усі дії, що

стосуються створення, перевірки та відкликання підпису, повинні автоматично фіксуватися у надійно захищених логах, що дозволяє виявляти підозрілі дії та реагувати на інциденти.

Організаційні засади

З точки зору організаційного впровадження, інфраструктура електронного підпису потребує чітко сформованих регламентів. Перш за все, слід розробити внутрішні нормативні документи, які визначають порядок отримання, використання, зупинення та відкликання сертифікатів.

Важливо також передбачити структуру ролей і відповідальностей усіх учасників процесу. Це дозволяє мінімізувати ймовірність помилок і забезпечити ефективне функціонування ІЕП на всіх рівнях — від технічного до адміністративного.

Освітній компонент також має велике значення. Персонал, що працює з інфраструктурою підпису, повинен проходити навчання й постійно оновлювати знання щодо нових загроз і змін у нормативній базі.

Щоб уникнути небажаних наслідків, в організації повинна функціонувати система управління ризиками, яка включає процедури виявлення, оцінки та оперативного реагування на інциденти, пов’язані з безпекою криптографічних ключів або системним порушенням.

Нормативно-правові положення

Законодавче забезпечення є невід’ємною частиною будь-якої системи електронного підпису. ІЕП повинна відповідати чинному законодавству України, зокрема Законам «Про електронні документи» та «Про електронні довірчі послуги». Для міжнародної взаємодії важливою є відповідність Регламенту eIDAS, прийнятому в ЄС.

Важливо забезпечити підтримку різних рівнів довіри до підпису, зокрема простого, удосконаленого та кваліфікованого. Це дозволяє використовувати інфраструктуру в різних контекстах — як у внутрішніх процесах, так і у правових спорах.

Окрім цього, необхідно мати юридично оформлені домовленості з усіма

зацікавленими сторонами — сертифікаційними центрами, розробниками програмного забезпечення, провайдерами послуг. Це дозволяє чітко регламентувати відповідальність за безпеку та підтримку інфраструктури.

Функціональні характеристики

Інфраструктура повинна мати розвинений функціонал, що дозволяє автоматизувати основні операції. Ідеальним є такий підхід, коли процеси створення, оновлення та відкликання сертифікатів відбуваються автоматично, без необхідності постійного втручання з боку користувача.

Крім того, повинна бути реалізована ефективна система управління життєвим циклом ключів. Це включає моніторинг терміну їх дії, попередження про необхідність оновлення, а також перевірку чинності сертифікатів за допомогою протоколів OCSP або CRL.

Гнучкість інфраструктури проявляється у її здатності масштабуватись у міру зростання потреб організації. Це дає змогу впроваджувати рішення як для малих установ, так і для великих підприємств без радикальної перебудови системи.

Мобільність також є важливою характеристикою. Підтримка електронного підпису на мобільних пристроях, можливість використання додатків на кшталт «Дія» або інтеграція з хмарними рішеннями значно підвищують зручність і доступність технології.

Захист основних компонентів

Безпечність ІЕП передбачає комплексний підхід до захисту критично важливої інфраструктури. Сервери, які обробляють ключову інформацію, повинні бути фізично захищеними: встановленням систем відеонагляду, біометричного контролю доступу та іншими засобами обмеження.

Мережева інфраструктура також має бути відповідно сегментована. Це означає виділення окремих ізольованих зон для критичних елементів системи, що мінімізує можливість несанкціонованого доступу ззовні.

Необхідно регулярно оновлювати всі програмні та апаратні компоненти системи. Застосування актуальних патчів та оновлень забезпечує відповідність сучасним стандартам інформаційної безпеки.

Крім того, потрібно передбачити наявність ефективного механізму відновлення після збоїв. Резервне копіювання налаштувань, сертифікатів та баз даних дає змогу швидко відновити функціональність у разі аварії.

Орієнтація на користувача

Успіх використання інфраструктури електронного підпису значною мірою залежить від її доступності для кінцевих користувачів. Важливо, щоб інтерфейс був інтуїтивно зрозумілим і не вимагав спеціальних технічних знань.

Система повинна підтримувати всі розповсюджені формати файлів, які можуть бути підписані: це PDF, XML, CMS, P7S та інші. Це гарантує сумісність з більшістю документів, що обробляються в організаціях.

Також необхідно забезпечити можливість перевірки підпису без додаткових технічних засобів. Сервіси, які дозволяють перевірити достовірність документа за кілька кроків, значно спрощують використання ІЕП у щоденній роботі.

3.2. Розробка політики застосування цифрового підпису в організації

В умовах цифрової трансформації інформаційних процесів в організаціях, забезпечення достовірності та цілісності даних набуває стратегічного значення. Цифровий підпис, як інструмент захисту електронних транзакцій, вимагає не лише впровадження відповідних технічних засобів, а й створення чітких правил його використання. Для цього необхідно сформулювати нормативний документ, який би регламентував усі етапи застосування цифрового підпису в організаційному середовищі, починаючи від генерації ключів і завершуючи аудитом операцій із підписаними даними.

Впровадження політики застосування цифрового підпису в організації відбувається поетапно. Спершу здійснюється аналіз потреб підприємства щодо електронного документообігу, визначаються доцільні типи електронного підпису, а також призначаються відповідальні особи за їх використання. Далі розробляються внутрішні регламенти та процедури, які узгоджуються і затверджуються на рівні керівництва. Після офіційного прийняття політики

організовується навчання персоналу для належного використання цифрового підпису. Завершальним етапом є безпосереднє впровадження технології в робочі процеси організації та подальший аудит застосування підписів для контролю їх ефективності і дотримання вимог безпеки.

Рис.3.2. Схема впровадження політики застосування цифрового підпису в організації

Така політика використання цифрового підпису покликана забезпечити послідовність і передбачуваність дій усіх учасників документообігу, а також відповідність правовим вимогам і стандартам інформаційної безпеки. Зміст цього

документа повинен охоплювати базові поняття, правила взаємодії користувачів, технічні вимоги до засобів підпису, механізми управління ключами та контрольні процедури. Водночас особлива увага має приділятися дотриманню нормативно-правової бази як на національному, так і на міжнародному рівнях, що дозволить уніфікувати процеси з урахуванням глобальних стандартів і підвищити правову силу електронних документів.

Урахування нормативної бази

Політика повинна відповідати українському законодавству (Закон «Про електронні довірчі послуги», накази Мінцифри) та міжнародним стандартам — eIDAS, ISO/IEC 27001, NIST SP 800-63

Таблиця 3.2

Причина перегляду	**Частота**
Зміни в законодавстві	По мірі змін
Виявлені інциденти безпеки	Негайно після події
Технічні зміни у системі ЦП	Після впровадження нових засобів
Планове оновлення	Щороку

Політика, розроблена відповідно до потреб організації, передбачає створення внутрішньої системи правил, що охоплює як працівників установи, так і залучених зовнішніх користувачів, які беруть участь у формуванні, підписанні або перевірці електронних документів. Усі дії щодо цифрового підпису мають здійснюватися на основі прозорих процедур, за яких визначено відповідальних осіб, порядок взаємодії структурних підрозділів, вимоги до обладнання та програмного забезпечення.

Важливим аспектом політики є регламентація типів електронного підпису, що можуть застосовуватися залежно від категорії документа або рівня його чутливості. Залежно від рівня захисту визначається доцільність використання простого, удосконаленого чи кваліфікованого підпису, причому перевага надається тим варіантам, що передбачають сертифікацію ключів відповідно до вимог законодавства. Особливу роль у цьому відіграють криптографічні алгоритми, які

мають бути сучасними, стійкими до атак і сертифікованими.

Система цифрового підпису має функціонувати в межах інфраструктури відкритих ключів, що передбачає централізоване керування сертифікатами, автоматизовану перевірку їх дійсності та логування всіх дій, пов’язаних із підписанням. У цій моделі важливо, щоб усі користувачі мали доступ до актуальної інформації про статус сертифікатів, а також можливість безпечно ідентифікувати себе для отримання ключів. При цьому необхідно забезпечити захищене зберігання приватних ключів, застосовуючи апаратні носії або сертифіковані хмарні рішення.

У процесі формування політики важливо також передбачити порядок управління ключами впродовж усього їх життєвого циклу. Це охоплює створення ключів, їх активне використання, регулярне оновлення, а також знищення у разі втрати актуальності або компрометації. Усі ці дії мають бути документально зафіксовані та здійснюватися під контролем уповноважених осіб. Система ротації ключів дозволяє підтримувати високий рівень безпеки і знижує ризики, пов’язані з тривалим використанням одних і тих самих засобів підпису.

Розробка політики неможлива без урахування людського фактора, який суттєво впливає на ефективність інформаційної безпеки. Персонал, що працює з електронним підписом, повинен бути поінформований про правила його використання, обізнаний із можливими загрозами та здатний дотримуватися встановлених процедур. Для цього організація має впровадити постійне навчання працівників, проводити інструктажі та періодичну перевірку знань. Крім того, слід організувати внутрішній моніторинг дотримання політики, який може включати регулярні аудити, перевірки логів і аналіз інцидентів.

Значну роль у політиці цифрового підпису відіграє також механізм реагування на надзвичайні події. Йдеться про ситуації, коли відбувається втрата ключа, підозра на його компрометацію, помилкове підписання документа або технічні збої у функціонуванні інфраструктури. У таких випадках політика має передбачати чіткий алгоритм дій: повідомлення відповідальних осіб, тимчасове блокування доступу, скасування сертифіката, відновлення цілісності документів. Резервні процедури також повинні бути частиною загальної системи безпеки.

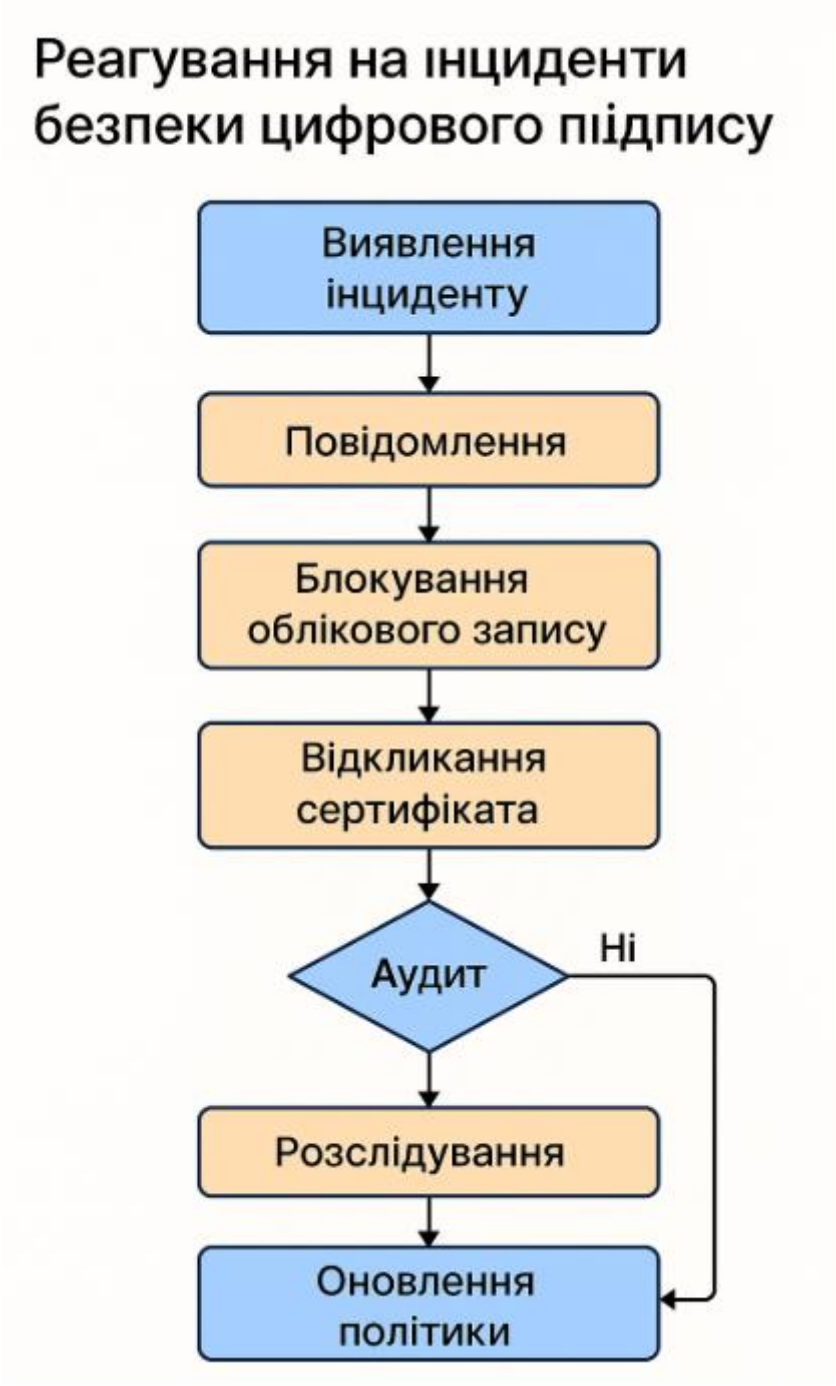

Рис. 3.3. Схема реагування на інциденти безпеки цифрового підпису

Цей малюнок показує послідовність дій у разі інциденту безпеки, пов’язаного з цифровим підписом. Процес починається з виявлення загрози, після чого відповідальні особи отримують сповіщення. Далі виконується блокування

облікового запису, відкликання сертифіката, проведення розслідування та аудит. Завершується все оновленням політики для запобігання подібним випадкам у майбутньому.

З метою підвищення зручності використання, політика цифрового підпису має бути представлена у форматах, що легко сприймаються користувачами, зокрема PDF або HTML, і розміщена на внутрішньому порталі організації. Доцільним є включення прикладів застосування, частих запитань (FAQ), а також супроводження документа журналом змін.

У разі інцидентів, пов’язаних із цифровим підписом, організація повинна дотримуватись чітко визначеного алгоритму дій. Зокрема, передбачається негайне інформування уповноважених осіб, тимчасове блокування облікових записів, скасування сертифікатів, розслідування інциденту, відновлення цілісності документів і, за потреби, оновлення політики. Це дозволяє оперативно реагувати на загрози і мінімізувати наслідки для інформаційної безпеки.

Для повноцінного функціонування політики слід забезпечити її регулярне оновлення з урахуванням змін у технологічному середовищі, нормативному полі та внутрішніх потреб організації. Оскільки стандарти безпеки та вимоги до електронного підпису постійно еволюціонують, статичний підхід до політик є неприйнятним. З цією метою створюється група з перегляду політики, яка аналізує зміни у правовому полі, нові технічні рішення та результати внутрішніх аудитів.

Крім того, важливо, щоб політика була доступною та зрозумілою для всіх користувачів. Для цього вона має бути опублікована на внутрішньому порталі організації або в електронній системі документообігу, мати зручну структуру та супроводжуватися прикладами застосування. Усі оновлення повинні супроводжуватися супровідними поясненнями або додатковими інструкціями.

Під час розробки політики застосування цифрового підпису організація має враховувати як національні вимоги, так і міжнародні рекомендації. На рівні України ключовими орієнтирами є Закон «Про електронні довірчі послуги», вимоги до кваліфікованих постачальників довірчих послуг, а також накази Міністерства цифрової трансформації. З міжнародної точки зору важливо

орієнтуватися на регламент eIDAS, стандарти ISO/IEC серії 27000, а також рекомендації таких організацій як ENISA та NIST.

У підсумку, політика цифрового підпису є багатовимірним документом, який інтегрує в собі вимоги безпеки, організаційної ефективності та правової визначеності. Її впровадження дозволяє не лише захистити інформаційні потоки, а й вибудувати культуру цифрової відповідальності всередині організації. Саме тому створення такої політики має бути пріоритетом для кожної сучасної установи, що прагне забезпечити довіру до своїх цифрових сервісів і захистити критично важливу інформацію від внутрішніх і зовнішніх загроз.

3.3. Рекомендації щодо інтеграції цифрового підпису з внутрішніми системами контролю цілісності даних

У сучасних умовах, коли електронна інформація все більше визначає ефективність функціонування організацій, питання її достовірності, незмінності та автентичності набуває пріоритетного значення. Хоч цифровий підпис сам по собі є важливим інструментом підтвердження цілісності даних, його ефективність значно зростає при впровадженні в контексті внутрішніх систем безпеки. До таких систем належать механізми виявлення змін у даних, системи управління журналами подій, засоби захисту конфіденційності та резервного копіювання, що в сукупності утворюють багаторівневу модель контролю над інформаційними потоками.

На рисунку зображено архітектуру інтеграції цифрового підпису з внутрішніми системами контролю цілісності даних. Підписані файли проходять перевірку цілісності за допомогою системи моніторингу змін (FIM), результати якої надходять у систему управління подіями безпеки (SIEM) для подальшого аналізу та збереження журналів. Одночасно, система запобігання витоку даних (DLP) контролює збереження та передачу інформації, забезпечуючи її конфіденційність і відповідність політикам безпеки. Така взаємодія дозволяє виявляти спроби підробки або зміни документів на ранніх етапах та гарантує цілісність і достовірність даних в інформаційному середовищі організації.

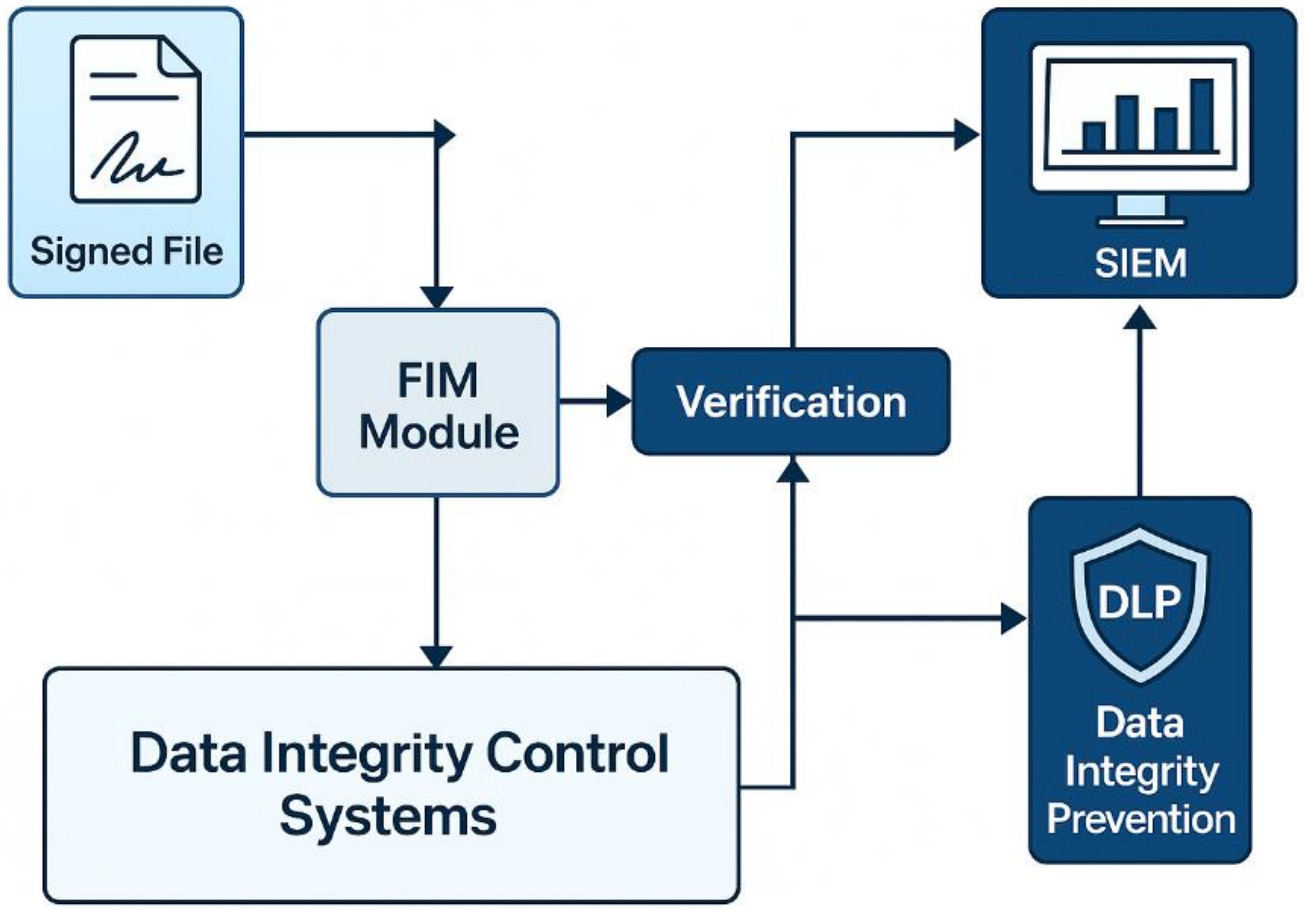

Рис. 3.4. Архітектура інтеграції цифрового підпису з внутрішніми системами контролю цілісності даних

Реалізація цифрового підпису має відбуватись відповідно до сформованої політики безпеки організації, яка регламентує обробку електронних документів, дій користувачів та порядок доступу до даних. Формування чітких процедур перевірки підписів, їх періодичної верифікації, а також ведення журналів таких перевірок дозволяє не лише підвищити надійність зберігання критичної інформації, а й спростити аудит та інцидент-менеджмент у разі порушень.

Особливу увагу слід приділити механізмам, що дозволяють фіксувати будь-які зміни у файлах. Якщо вбудувати цифровий підпис у такі засоби, як системи контролю цілісності файлів, з’являється можливість відстежувати зміни не лише за допомогою хеш-функцій, а й через криптографічну перевірку автентичності. Це дозволяє підтвердити, що конкретний документ не змінювався від моменту

підписання, і встановити автора змін у разі потреби. Для підвищення рівня безпеки варто передбачити зберігання підписів у відокремленому захищеному середовищі або додавати їх безпосередньо до об’єкта, що захищається, у вигляді метаданих.

У корпоративній практиці доцільно передбачити фіксацію всіх дій, пов’язаних із цифровими підписами, у централізованих системах журналювання, таких як SIEM. Це дозволяє не лише отримувати повну історію взаємодії користувачів із підписаними документами, а й оперативно виявляти аномальні ситуації — наприклад, спроби перевірки підписів із непередбачених джерел або невідповідність між хешем і криптографічним підписом. Подібні дії можуть свідчити про спроби втручання в дані, і їхня автоматизована фіксація сприяє ефективному реагуванню на інциденти.

Підвищити ефективність роботи з підписаними файлами дозволяє впровадження автоматизованих процедур перевірки, коли документ проходить верифікацію на етапі кожного звернення до нього. У системах управління контентом або документообігом важливо забезпечити таку функціональність, щоб будь-яке відкриття чи редагування документа передбачало перевірку чинності цифрового підпису, а в разі невідповідності — блокування дій користувача або фіксацію події.

На малюнку зображено процес перевірки цифрового підпису всередині системи контролю версій. Документ надходить до системи, яка автоматично аналізує його цифровий підпис. Якщо підпис дійсний, документ зберігається як автентичний. Якщо ж виявляється зміна у вмісті документа, яка не супроводжується перепідписом, система фіксує зміну та повідомляє про недійсний підпис. Такий механізм дозволяє запобігти використанню модифікованих файлів без належної авторизації, забезпечуючи цілісність на кожному етапі збереження або редагування даних.

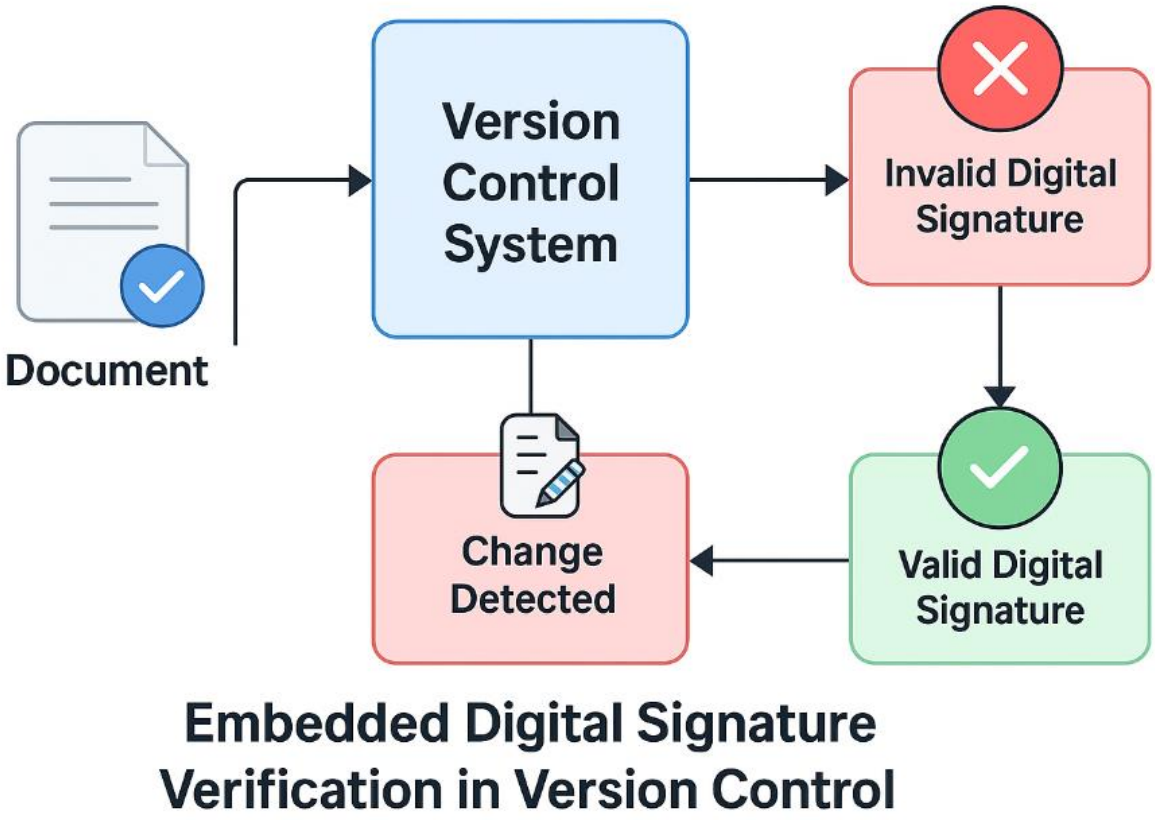

Рис.3.5 – Вбудована перевірка цифрового підпису в системі контролю версій

Особливу цінність цифровий підпис має для систем резервного копіювання та відновлення даних. Захист копій цифровими підписами дозволяє зберігати впевненість у тому, що дані, які потрапляють до архіву, не були змінені або підроблені. Під час відновлення резерву важливо не лише фізично витягти дані, а й переконатись у їхній автентичності. Перевірка підпису в таких випадках повинна стати стандартною процедурою.

Під час розробки внутрішньої архітектури безпеки доцільно реалізовувати перевірку цифрового підпису як окрему сервісну функцію, доступну для інших систем через API. Така мікросервісна архітектура дозволяє централізовано виконувати операції перевірки, не дублюючи логіку в кожному модулі. Це особливо важливо в умовах багатокомпонентного програмного середовища, де різні підсистеми — бухгалтерські, управлінські, кадрові — взаємодіють між собою.

У питаннях збереження цілісності журналів подій цифровий підпис може використовуватися для захисту блоків записів, що дозволяє швидко виявляти спроби редагування або видалення даних. Якщо кожен блок журналу підписаний, будь-яка зміна навіть одного запису зруйнує цілісність всього блоку. Таким чином, зловмисник не зможе змінити інформацію без явного цифрового сліду.

У складних автоматизованих процесах, де документи проходять кілька етапів узгодження, цифровий підпис може бути прив'язаний до кожного етапу workflow. Це створює логічну послідовність дій, що підтверджується криптографічно, і дозволяє контролювати, хто саме, коли та за яких умов погодив певну дію. Такий підхід знижує ризик помилок та несанкціонованих змін у процесі прийняття рішень.

Інтеграція цифрового підпису в IT-середовище організації вимагає також уніфікації форматів даних, які використовуються для перевірки. Забезпечення підтримки як P7S, так і XMLDSig або XAdES дає змогу гнучко використовувати підпис у різних програмних системах, а також перевіряти його як в офлайн-, так і в онлайн-режимі — через централізований веб-сервіс чи локальний клієнт.

Необхідно приділяти увагу також організаційним аспектам. Персонал, що має справу з обробкою підписаних документів, повинен проходити навчання з верифікації підписів та виявлення потенційних ознак компрометації. Створення чіткої структури розмежування прав доступу та зон відповідальності дозволяє уникнути конфліктів і знижує ризик внутрішніх загроз. Важливо також проводити регулярні перевірки як технічної справності системи цифрового підпису, так і актуальності алгоритмів і криптографічних бібліотек, які використовуються.

Таким чином, впровадження цифрового підпису в систему контролю цілісності даних не є одноразовим заходом, а вимагає створення комплексної архітектури, де кожен компонент відіграє свою роль у забезпеченні надійного та довіреного середовища. Така інтеграція підвищує не лише рівень інформаційної безпеки, а й прозорість процесів, що, в свою чергу, сприяє довірі з боку партнерів, клієнтів і державних структур.

Висновки

У роботі проведено дослідження проблеми забезпечення цілісності даних в організації за допомогою цифрового підпису, визначено його роль у сучасних системах інформаційної безпеки та сформульовано відповідні рекомендації щодо впровадження.

Проаналізовано наявні законодавчі, технічні та організаційні аспекти застосування цифрового підпису. Розглянуто його функції щодо автентифікації, забезпечення цілісності даних та невідмовності у цифровому середовищі. Зокрема, цифровий підпис дозволяє виявляти несанкціоновані зміни у даних та підтверджувати авторство документів у правовому полі.

У ході дослідження розглянуто різні види цифрових підписів (ПЕП, УЕП, КЕП), порівняно алгоритми криптографічного підпису (RSA, ECDSA, SPHINCS+ тощо), а також здійснено огляд практик впровадження електронного підпису в Україні та за кордоном. Особливу увагу приділено кваліфікованому електронному підпису як найбільш надійному засобу юридичного підтвердження електронних транзакцій.

Розроблено рекомендації щодо впровадження цифрового підпису в організації, які включають:

1.формування політики електронного підпису;

2.визначення технічних вимог до інфраструктури (PKI);

3. інтеграцію підпису у внутрішні системи контролю цілісності даних (SIEM, DLP, EDM тощо);

4.створення механізмів реагування на інциденти, пов’язані з компрометацією ключів або недійсністю сертифікатів.

Використання цифрового підпису у поєднанні з внутрішніми системами контролю дозволяє забезпечити вищий рівень достовірності та юридичної захищеності даних, які циркулюють в організації. Впровадження зазначених заходів підвищує рівень інформаційної безпеки, знижує ризики втрати або

спотворення даних та сприяє створенню довірчого середовища для цифрової взаємодії.

Таким чином, правильно організоване впровадження цифрового підпису є дієвим інструментом для забезпечення цілісності інформації в організації та має стратегічне значення в умовах зростання кількості кібератак і цифрової трансформації бізнес-процесів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Особливості електронного підпису та переваги його використання. URL: https://signy.online/osoblivosti-elektronnogo-pidpisu-ta-perevagi-jogo-vikoristannya/ (дата звернення: 20.04.2025).

2. Bezviz – електронний підпис. URL: https://bezviz.info/life/3245-podpis-elektroniczny (дата звернення: 20.04.2025).

3. National Institute of Standards and Technology (NIST) URL: https://csrc.nist.gov/glossary/term/digital_signature (дата звернення: 20.04.2025).

4. Adobe eSignatures Regulations. URL: https://helpx.adobe.com/legal/esignatures/regulations/united-states.html (дата звернення: 20.04.2025).

5. Checkbox — електронний підпис у Кишені. URL: https://checkbox.ua/blog/elektronnyj-pidpys-u-kysheni/ (дата звернення: 20.04.2025).

6. Важливі питання про електронний підпис. URL: https://blog.zakupivli.pro/nayvazhlivishe-pro-elektronniy-pidpis-vidpovidayemo-na-zapitannya/ (дата звернення: 20.04.2025).

7. Journal VITI — стаття про електронний підпис. URL: https://journal.viti.edu.ua/index.php/cicst/article/view/85/ (дата звернення: 20.04.2025).

8. Журнал НАУ — електронний підпис. URL: https://jrnl.nau.edu.ua/index.php/SBT/article/view/12370 (дата звернення: 20.04.2025).

9. Oberig IT — методи автентифікації електронного підпису. URL:https://oberig-it.com/statti/metody-avtentyfikacziyi-elektronnogo-pidpysu-zabezpechte-pravylnyj-balans-mizh-bezpechnoyu-ta-zruchnoyu-avtentyfikacziyeyu/ (дата звернення: 20.04.2025).

10. Вчасно.КЕП — URL: https://cap.vchasno.com.ua/stvoryty-elektronnyj-pidpys-onlajn/ (дата звернення: 20.04.2025).

11. TechTarget — Digital Signature Definition — URL: https://www.techtarget.com/searchsecurity/definition/digital-signature (дата звернення: 20.04.2025).

12. Global Sign — URL: https://www.globalsign.com/en/document-signing (дата звернення: 20.04.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)