# Тема 14. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС

## 1. Загальні положення

Протягом багатьох століть при ведені ділової переписки, заключенні контрактів і оформленні будь-яких інших важливих паперів підпис відповідальної особи або виконавця був неодмінною умовою визнання його статусу або незаперечним свідченням його важливості.

Подібний акт переслідував дві мети:

• гарантування істинності листа шляхом звірення підпису зі зразком;

• гарантування авторства документа (з юридичної точки зору).

Виконання даних вимог ґрунтується на наступних властивостях підпису:

• підпис автентичний, тобто з його допомогою одержувачу документа можна довести, що він належить власнику (на практиці це визначається графологічною експертизою);

• підпис не підроблюваний, тобто служить доказом, що тільки та людина, чий автограф стоїть на документі, міг підписати даний документ, і ніхто інший не зміг би цього зробити;

• підпис такий, що не переноситься, тобто є частиною документа і тому перенести його на інший документ неможливо;

• документ з підписом є незмінним, тобто після підписування його неможливо змінити, залишивши даний факт непоміченим;

• підпис незаперечний, тобто людина, яка підписала документ, в разі визнання експертизою, що саме вона засвідчила даний документ, не може заперечити факт підписання;

• будь-яка особа, що має зразок підпису, може, упевнитися в тому, що даний документ підписаний власником підпису.

Один із найпростіших способів аутентифікації (підписування) електронних документів є використання шифрування. При цьому відправник А шифрує документ своїм секретним ключем і відправляє отримувачу Б. Отримувач Б дешифрує документ за допомогою відкритого ключа відправника А. Якщо це йому вдається, то документ вважається істинним. Якщо отримувач

Б не зможе дешифрувати документ, то документ істинним не вважається. Такий спосіб має надзвичайно серйозний недолік, пов'язаний з тим, що він є неефективним для підписування документів значного обсягу.

Саме тому для аутентифікації електронних документів, що передаються телекомунікаційними каналами зв'язку, використовується спеціально створюваний електронний цифровий підпис (ЕЦП).

З переходом до безпаперових способів передачі і зберігання даних, а також з розвитком систем електронного переказу грошових коштів, в основі яких – електронний аналог паперового платіжного доручення, проблема віртуального підтвердження автентичності документа набула особливої гостроти. Розвиток будь-яких подібних систем тепер немислимий без існування електронних підписів під електронними документами. Однак застосування та широке поширення електронно-цифрових підписів (ЕЦП) спричинило цілий ряд правових проблем. Так, ЕЦП може застосовуватися на основі домовленостей всередині якої-небудь групи користувачів системи передачі даних, і відповідно до домовленості усередині даної групи ЕЦП повинен мати юридичну силу. Але чи буде електронний підпис мати доказову силу в суді, наприклад при оскарженні факту передачі платіжного доручення?

Хоча ЕЦП зберіг практично всі основні властивості звичайного підпису, все-таки деякі особливості реалізації електронного автографа роблять його окремим класом підписів. Тому юридичні, правові та методологічні аспекти застосування ЕЦП повинні враховувати його специфіку.

Існує кілька методів побудови схем ЕЦП, а саме:

- шифрування електронного документа (ЕД) на основі симетричних алгоритмів. Дана схема передбачає наявність у системі третьої особи (арбітра), що користується довірою учасників обміну підписаними подібним чином електронними документами. Взаємодія користувачів даною системою здійснюється за такою схемою:

- учасник А зашифровує повідомлення своїм таємним ключем $К_А$, знання якого розділено з арбітром, потім шифроване повідомлення передається арбітру із зазначенням адресата даного повідомлення (інформація, що

ідентифікує адресата, передається також у зашифрованому вигляді);

- арбітр розшифровує отримане повідомлення ключем $К_А$, виконує необхідні перевірки і потім зашифровує секретним ключем учасника В ($К_В$). Далі зашифроване повідомлення посилається учаснику В разом з інформацією, що воно прийшло від учасника А;

- учасник В розшифровує це повідомлення й переконується в тому, що відправником є учасник А.

(Авторизацією документа в даній схемі буде вважатися сам факт зашифрування ЕД секретним ключем і передача зашифрованого ЕД арбітру. Основною перевагою цієї схеми є наявність третьої сторони, що виключає будь-які спірні питання між учасниками інформаційного обміну, тобто в даному випадку не потрібно додаткової системи арбітражу ЕЦП. Недоліком схеми є наявність третьої сторони і використання симетричних алгоритмів шифрування. На практиці ця схема не отримала широкого розповсюдження.);

• використання асиметричних алгоритмів шифрування. Фактом підписання документа в даній схемі є зашифрування документа секретним ключем його відправника. Ця схема теж використовується досить рідко внаслідок того, що довжина ЕД може виявитися критичною. Застосування асиметричних алгоритмів для зашифрування повідомлень великої довжини неефективно з точки зору швидкісних характеристик, що, наприклад, для системи валових розрахунків є одним з основних показників. У цьому випадку не потрібно наявності третьої сторони, хоча вона може виступати в ролі сертифікаційного органу відкритих ключів користувачів;

• розвитком попередньої ідеї стала найбільш поширена схема ЕЦП, а саме: зашифрування остаточного результату обробки ЕД хеш-функцією за допомогою асиметричного алгоритму.

Генерація підпису відбувається наступним чином:

1. Учасник А обчислює хеш-код від ЕД. Отриманий хеш-код проходить процедуру перетворення з використанням свого секретного ключа. Після чого отримане значення (яке і є ЕЦП) разом з ЕД відправляється учаснику В.

2. Учасник В повинен отримати ЕД з ЕЦП та сертифікований відкритий ключ учасника А, а потім провести розшифрування на ньому ЕЦП, сам ЕД піддається операції хешування, після чого результати порівнюються, і якщо вони співпадають, то ЕЦП визнається істинним, в іншому випадку помилковим.

Ефективність реалізації даної схеми в порівнянні з попередньою полягає в застосуванні повільних процедур асиметричного шифрування до хеш-коду ЕД, який значно коротше самого ЕД.

Стійкість даного типу ЕЦП заснована на стійкості асиметричних алгоритмів шифрування і застосовуваних хеш-функцій.

Крім перерахованих вище існують «екзотичні» варіанти побудови схем ЕЦП (груповий підпис, незаперечний підпис, довірений підпис і т.п.). Поява цих різновидів обумовлена різноманіттям завдань, що вирішуються за допомогою електронних технологій передачі та обробки ЕД.

У загальному випадку підписаний ЕД виглядає як пара, що складається з бінарних рядків (M, S), де M представляє собою ЕД, а S – розв’язок рівняння $F_K(S) = M$, де $F_K$ є функцією з секретом. У зв'язку з вище описаним визначенням ЕЦП можна виділити наступні його властивості:

• є непідроблюваний, оскільки розв’язати рівняння $F_K(S) = M$ може тільки володар секрету К;

• однозначно ідентифікує автора, тобто людини, яка підписала цей документ;

• верифікація підпису (перевірка) проводиться на основі знання функції $F_K$;

• є таким, що не переноситься на інший ЕД; виняток становить випадок, коли для використовуваної хеш-функції знайдені колізії;

• ЕД з ЕЦП може передаватися по відкритих каналах, оскільки будь-яка зміна ЕД призведе до того, що процедура перевірки ЕЦП виявить даний факт. [8]

## 2. Атаки на ЕЦП

Широке застосування ЕЦП в різних областях електронних комунікацій призвело до того, що в криптографії вже склався великий теоретичний доробок, присвячений створенню схем ЕЦП, їх використання, а також питанням стійкості більшості схем ЕЦП і безпеки їх застосування.

Як вже зазначалося, стійкість більшості схем ЕЦП залежить від стійкості асиметричних алгоритмів шифрування та хеш-функцій. Тому даний розділ ми присвятимо опису існуючих на сьогоднішній день атак і загроз на схеми ЕЦП.

Наведемо **класифікацію атак на схеми ЕЦП**:

• атака з відомим відкритим ключем. Вона є, очевидно, найслабкішою з усіх перерахованих нижче, оскільки зловмисник завжди може отримати відкритий ключ користувача;

• атака з відомими підписаними повідомленнями. Противник крім відкритого ключа має ще й набір підписаних повідомлень;

• проста атака з вибором підписаних повідомлень. Противник має можливість вибирати підписані повідомлення, при цьому відкритий ключ він отримує після вибору повідомлень;

• спрямована атака з вибором повідомлень. Являє собою варіант попередньої і відрізняється тим, що, отримуючи підписані повідомленя, противник знає відкритий ключ;

• адаптивна атака з вибором повідомлень. У даній атаці противник знає відкритий ключ, може вибирати підписані повідомлення і, крім того, має підписи усіх раніше підписаних повідомлень.

Кожна атака на схему ЕЦП переслідує певні цілі (загрози), які можна розділити на наступні класи:

• повне розкриття. Противник знаходить секретний ключ користувача;

• універсальна підробка. Противник знаходить алгоритм, функціонально еквівалентний алгоритму генерації ЕЦП;

• селективна підробка. Підробка підпису для повідомлення, обраного противником;

• екзистенційна підробка. Підробка підпису хоча б для одного випадково вибраного повідомлення.

Оцінка стійкості схеми ЕЦП проводиться відносно пари (атака-загроза), тобто стійкість ЕЦП можна визначити як здатність підпису протистояти досягненню противником строго визначеної мети при проведенні атаки на схему ЕЦП.

На практиці застосування ЕЦП дозволяє запобігти або виявити такі **дії порушника** (він по відношенню до системи може бути як внутрішнім, так і зовнішнім):

• відмова одного з учасників від факту відправлення повідомлення. Учасник інформаційного обміну А заявляє, що він не посилав повідомлення учаснику В, хоча насправді посилав;

• модифікація прийнятого ЕД. Учасник В, прийнявши повідомлення, змінят його і стверджує, що саме дане повідомлення він прийняв від учасника А;

• підробка повідомлення. Учасник В створює повідомлення і стверджує, що дане повідомлення він прийняв від учасника А, хоча насправді А нічого не передавав;

• нав'язування повідомлень в процесі передачі. Зловмисник переохоплює обмін повідомленнями між А і В і модифікує їх;

• імітація надіслати повідомлення. Зловмисник намагається відправляти повідомлення від імені одного з учасників інформаційного обміну.

При цьому слід врахувати, що існують порушення, від яких неможливо захистити систему обміну повідомленнями, а саме:

• повтор передачі повідомлення. Зловмисник або один з учасників інформаційного обміну намагається знову передати раніше відправлене повідомлення. Подібні порушення особливо поширені в системі електронного переказу коштів;

• фальсифікація часу відправлення повідомлення.

Протидія таким порушенням може ґрунтуватися на використанні тимчасових вставок і суворому обліку вхідних повідомлень. [11, 12, 13, 14]

## 3. Алгоритми ЕЦП: Ель-Гамаля (EGSA), DSA, ГОСТ Р34.10-94

Надійний та зручний для реалізації на персональних комп'ютерах алгоритм цифрового підпису був розроблений у 1984 році американцем арабського походження Тахером Ель Гамалем. У 1991 році Національний інститут стандартів (НІСТ) США обгрунтував перед комісією Конгресу США вибір цього алгоритму як бази для відповідного національного стандарту. Найменування EGSA має походження від слів El Gamal Signature Algorithm (алгоритм цифрового підпису Ель Гамаля).

*Ідея EGSA* базується на тому, що для практичної неможливості фальсифікації ЕЦП може бути використана практично нерозв'язувана задача дискретного логарифмування.

*Послідовно розглянемо алгоритм електронного цифрового підпису Ель Гамаля.* [8]

1) Відправник, який має підписати свій документ, вибирає деяке велике просте ціле число $P$. Це число є відкритим і передається усім отримувачам документів відправника. Реальні значення близькі до $2^{1024}(\approx 10^{308})$

**Приклад.** Відправник вибирає число $P = 11$.

2) Відправник вибирає також велике ціле число $G$, яке має задовольняти умовам $1 < G < P$. Це число також є відкритим і передається усім отримувачам документів відправника. Реальні значення близькі до $2^{512}(\approx 10^{154})$.

**Приклад.** Відправник вибирає число $G = 2$.

3) Відправник вибирає ціле число $X$, яке має задовольняти умовам $1 < X < P$. Це число є секретним ключем відправника для підписування документів.

**Приклад.** Відправник вибирає секретний ключ X= *8.*

4) Відправник обчислює число $Y = G^X mod\ P$. Це число є відкритим ключем відправника, яке використовується отримувачами для

перевірки його підпису. Це число також передається усім отримувачам документів відправника.

**Приклад.** Відправник обчислює число $Y = G^X \ mod P = 2^8 \ mod \ 11 = 3$.

5) Відправник обчислює хеш-значення $H$ свого документу М. Кількість біт хеш-значення має бути на одиницю меншою кількості біт значення $P$-$1$. У загальному випадку хеш-значення $H$ документу М відправника має задовольняти умовам $1 < H < (P - 1)$.

**Приклад.** Відправник обчислює хеш-значення $H$ свого документу $M$ і отримує $H = 5$. Згадані умови стосовно кількості біт виконуються. Дійсно, значення $H = 5$ має 3 біта, а значення $P - 1 = 10$ має 4 біта.

6) Відправник вибирає випадкове ціле число $K$, яке має задовольняти умовам $1 < K < (P - 1)$. Крім того, числа $K$ і $P$-$1$ мають бути взаємно простими, тобто їх найбільший спільний дільник $НСД(K, P-1) = 1$. Це число також є секретним числом відправника для підписування його документу М.

**Приклад.** Відправник вибирає випадкове ціле число $K = 9$.

7) Відправник обчислює ціле число $a = G^K \ mod P$. Це число є першою складовою електронного цифрового підпису його документу.

**Приклад.** Відправник обчислює число $a = G^K \ mod P = 2^9 \ mod \ 11 = 6$.

8) Відправник знаходить ціле число й, використовуючи рівняння $H = (X \cdot a + K \cdot b) \ mod \ (P-1)$. Це число є другою складовою електронного цифрового підпису його документу.

**Приклад.** Відправник знаходить ціле число $b$ із рівняння

$H = (X \cdot a + K \cdot b) \ mod \ (P - 1)$ або $5 = (8 \cdot 6 + 9 \cdot V) \ mod \ 10$. Це число можна знайти шляхом послідовного перебору:

$b = 1$; $(8 \cdot 6 + 9 \cdot 1) \ mod \ 10 = 7$;

$b = 2$; $(8 \cdot 6 + 9 \cdot 2) \ mod \ 10 = 6$;

$b = 3$; $(8 \cdot 6 + 9 \cdot 3) \ mod \ 10 = 5$.

Отримуємо $b = 3$.

9). Відправник передає отримувачу документ М, а також його електронний цифровий підпис у вигляді пари чисел $S = (a, b)$.

**Приклад.** Відправник передає отримувачу документ M, а також його електронний цифровий підпис у вигляді пари чисел $S = (6, 3)$.

Отримавши документ M, а також його електронний цифровий підпис $S = (a, b)$, отримувач повинен перевірити, чи відповідає цей підпис документу.

1) Отримувач обчислює хеш-значення H отриманого документу M.

**Приклад.** Отримувач обчислює хеш-значення $H$ документу M і отримує $H = 5$.

2) Отримувач обчислює ціле число $A_1 = (Y^a \cdot a^b) \bmod P$.

**Приклад.** Отримувач обчислює ціле число $A_1 = (Y^a \cdot a^b) \bmod P = (3^6 \cdot 6^3) \bmod 11 = 10$.

3) Отримувач обчислює ціле число $A_2 = G^H \bmod P$.

**Приклад.** Отримувач обчислює ціле число $A_2 = G^H \bmod P = 2^5 \bmod 11 = 10$.

4) Отримувач порівнює знайдені числа $A_1$ і $A_2$. Ці числа будуть рівні тоді і тільки тоді, коли електронний цифровий підпис відповідає документу, тобто відправником документу M є дійсно власник секретного ключа X, і що відправник підписав саме цей документ M.

**Приклад.** ЕЦП $S = (6, 3)$ відповідає отриманому документу $M$.

Використання алгоритму електронного цифрового підпису Ель Гамаля вимагає вибору щоразу іншого випадкового цілого числа K. Інакше, якщо зловмисник розкриє повторно використовуване відправником число K, то він зможе розкрити і його секретний ключ X.

Отже, алгоритм Ель-Гамаля являє собою протокол з обчисленнями і цифровим підписом вважається пара чисел. (Обчислення що проводяться в протилежну сторону базуються на практично нерозв'язній задачі дискретного логарифмування).

У 1991 році Національний інститут стандартизації і технологій (NIST) США опублікував стандарт на ЕЦП (Digital Signature Standard, DSS), в основі якого – алгоритм DSA. Він є аналогом механізму, запропонованим Ель Гамалем, але з деякими змінами, зокрема за рахунок зменшення числового порядку одного з параметрів схеми.

У даному стандарті підпис – це два великих цілих числа, отримані відповідно до процедур і параметрів, визначеним в DSS.

Алгоритм DSA є «класичним» прикладом схеми ЕЦП на основі використання хеш-функції і асиметричного алгоритму шифрування.

Стійкість системи в цілому заснована на складності знаходження дискретних логарифмів в кінцевих полях.

*DSA* [7, 9]

Даний алгоритм є частиною американського стандарту DSS.

В алгоритмі використовується одно направлена хеш-функція H(x).

Стандарт визначає використання алгоритму SHA-1.

Параметри:

$p$ – просте число $L$ бітів, де $L$ набуває значення кратне 64 в діапазоні від 512 до 1024;

$q$ – 160 – бітовий множник $p - 1$;

$a = g^{(p-1)/q} \bmod p$, де $g < p - 1$, для якого $g^{(p-1)/q} \bmod p > 1$;

$y = a^x \bmod p$, де $x < q$;

$m$ – текст.

Ключ підпису: $(y, p, q, a)$.

Ключ верифікації: (x).

Підписування:

$k$ – випадкове число, $k < q$;

$r = (a^k \bmod p) \bmod q$ – обчислення першої частини підпису;

$s = (k^{-1}(H(m) + xr)) \bmod q$ – обчислення другої частини підпису.

Підпис: $(r , s)$.

Верифікація:

$w = s^{-1} \bmod q$;

$u_1 = (H(m) \cdot w) \bmod q$;

$u_2 = (rw) \bmod q$;

$v = ((a^{u_1} \cdot y^{u_2}) \bmod p) \bmod q$, якщо $v = r$, то підпис справжній.

*ГОСТ Р34.10-94* [7, 9]

Даний алгоритм є російським стандартом цифрового підпису.

Цей алгоритм використовує одно направлену хеш-функцію H(x). Стандарт визначає використання хеш-функції ГОСТ Р34.11-94, яка основана на симетричному алгоритмі ГОСТ 28147-89.

Параметри:

*p* – просте число, довжина якого лежить в діапазоні 509-512 біт, або 1020-1024 біт;

*q* – просте число, множник p – 1, довжиною від 254 до 256 біт;

*a* – випадкове число, $a < p-1$, $a^q \bmod p = 1$;

$y = a^x \bmod p$, де $x < q$;

Ключ підпису: *(p, q, a, y)*.

Ключ верифікації: *(x)*.

Підписування:

*k* – випадкове число, $k < q$;

$r = (a^k \bmod p) \bmod q$ – обчислення першої частини підпису;

$s = (xr + k(H(m))) \bmod q$ – обчислення другої частини підпису;

Якщо $H(m) \bmod q = 0$, необхідно встановити його в 1.

Якщо $r = 0$ (або $s=0$), то необхідно вибрати інше значення *K* і почати знову.

Підпис: $(r \bmod 2^{256}, s \bmod 2^{256})$.

Верифікація:

$v = H(m)^{q-2} \bmod q$;

$z_1 = (sv) \bmod q$;

$z_2 = ((q - r) \cdot v) \bmod q$;

$u = \left((a^{z_1} \cdot y^{z_2}) \bmod p\right) \bmod q$, якщо $u = r$, то підпис справжній.

## 4. Арбітраж ЕЦП

Практичне застосування ЕЦП, крім процедур генерації та перевірки електронного підпису, вимагає присутності системи розбору конфліктних ситуацій (арбітраж ЕЦП). Будь-який алгоритм ЕЦП подібних процедур у

своєму описі не містить. Це пов'язано з тим, що побудова схем арбітражу пов'язана з контекстом використання ЕЦП, так як його проведення – не стільки технічне, скільки організаційне завдання.

У більшості існуючих систем використання арбітражу ЕЦП засновано на тому, що підписати повідомлення може тільки власник секретного ключа (в цьому випадку відповідальність за його компрометацію покладається на користувача). Це твердження не можна вважати вірним у випадку, коли $h(m_1) = h(m)$, тобто один і той же підпис з'являється під двома різними повідомленнями. Арбітр у подібному випадку не зможе вирішити суперечку, що виникла, хоча очевидно, що хтось з учасників знайшов лазівки для хеш-функції. Тому в більшості випадків процедури арбітражу будуть неповними, за винятком варіанта, коли схеми ЕЦП розроблені спеціально з врахуванням проведення подібного розгляду. З існуючих на сьогоднішній день схем електронного підпису арбітраж найефективніше може бути проведений для ЕЦП, побудованих на основі симетричного шифрування за участю третьої сторони. При використання схем ЕЦП, побудованих без участі арбітра, слід з особливою старанністю вибирати процедуру підписання ЕД, щоб арбітр у випадку виникнення спірної ситуації міг вирішити, яка зі сторін є правою.

Конкретна реалізація процедур арбітражу залежить насамперед від потреб користувачів, технічної реалізації ЕЦП і від обставин, через які виникла необхідність у проведенні арбітражу. Для прикладу розглянута процедура, що виникла при відмові користувача від факту підписання документа $m$, при цьому в якості використовуваної ЕЦП береться алгоритм DSA.

Тут вихідними даними є загальнодоступні параметри DSA – $p, q, g$; ЕД – $m$ і підпис – $r, s$. ЕД і підпис представляються арбітру учасником В, який хоче довести, що даний підпис належить учаснику А; в свою чергу, учасник А відмовляється визнати, що даний підпис був ним згенерований.

Насамперед арбітр вимагає від учасника А пред'явлення секретного ключа. Ця вимога для будь-якого користувача ЕЦП в конкретній описаній системі має виконуватися беззастережно. Арбітр перевіряє відкритий ключ із загальнодоступного довідника на відповідність представленого секретного

ключа. У випадку не співпадання арбітр звертається в центр сертифікації відкритих ключів та вимагає надання завіреного учасником А документа, що містить відкритий ключ. Якщо з'ясовується, що відкритий ключ в загальнодоступному довіднику не співпадає із зазначеним у документі, винним визнається центр сертифікації відкритих ключів. Коли відкриті ключі в довіднику і в документі збігаються, це означає, що пред'явлений некоректний секретний ключ, і учасник А визнається винним.

У разі, якщо відкритий і секретний ключі відповідають раніше створеним зразкам, арбітр виконує наступні обчислення:

$W = s^{-1} mod\ q$

$ul = (h\ (m)\ w)\ mod\ q$

$u2 = (rw)\ mod\ q$

$v = ((g^{ul} y^{u2})\ mod\ p)\ mod\ q$

Завершальною фазою є перевірка рівності $v = r$. Якщо вона виконується, то підпис визнається дійсним, якщо ні – помилковим.