УДК 004.056(043.2)

МЕХАНІЗМ НАКЛАДАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ НА ДОКУМЕНТ

Таратайко Д.В., Пепа Ю.В.
Національний авіаційний університет, м. Київ

Розглянуті питання генерації ключів для формування електронного цифрового підпису на прикладі програмного комплексу користувача Центру сертифікації ключів для фінансових установ, а також можливі методи боротьби з шахрайством щодо підміни підпису або модифікації оригінального документа.

Вступ

Однією з важливих проблем є захист електронних документів [1]. На сьогоднішній день одним з уживаних методів захисту є криптографічний захист [2] на основі електронного цифрового підпису (ЕЦП) документа [3].

Електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувала [3].

Засіб електронного цифрового підпису – програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів [2], накладення та/або перевірки електронного цифрового підпису [3].

Метою роботи є дослідження всіх етапів від генерації ключа для ЕЦП до моменту отримання підписаного документу отримувачем з метою простеження можливих вразливостей та атак на ЕЦП і розробка методів протидії шахрайству.

Актуальність роботи полягає в досліджені механізмів ЕЦП і розробка рекомендацій для уповноважених служб щодо вдосконалення механізмів генерації ключів та способів підписування документів з метою підвищення рівня безпеки процедур, пов'язаних з використанням ЕЦП в Україні.

1 Генерація ключів

За час життя згенеровані ключі можуть переходити з одного стану до іншого. Розглянемо ці процедури докладніше:

1. Генерація криптографічного ключа. Якість ключа визначається застосовуваними криптографічними алгоритмами, а також генераторами випадкових або псевдовипадкових чисел.
2. Реєстрація ключа. Ця процедура пов'язує певний ключ з об'єктом. Вона надається Центрами реєстрації ключів. Ці ж Центри знімають з обліку ключі.
3. Створення сертифікату ключа. Ця послуга реалізується Центрами сертифікації відкритих ключів для забезпечення їх автентичності [1].
4. Поширення ключа. Існують різні технології поширення ключів до споживачів, які базуються як на симетричних, так і асиметричних технологіях.
5. Інсталяція ключа. Встановлення ключа в криптографічний пристрій.
6. Збереження ключа. Ця послуга призначена для подальшого використання або резервування ключа.
7. Виведення ключа. Виготовлення з одного базового ключа цілої сім'ї ключів для співробітників.
8. Архівація ключа. Безпечне збереження ключа після його використання. Заархівовані ключі в подальшому можуть знадобитися для вирішення юридичних суперечок і претензій.
9. Відкликання ключа. В процесі компрометації ключа або підозрі про несанкціоноване використання його виводять з активного стану.

10. Зняття з обліку ключа. Цю процедуру виконує Центр реєстрації ключів перед процесом знищення ключа.
11. Знищення ключа. Виконується гарантоване знищення всіх копій ключа.

2 Накладання підпису на документ

Розглянемо процеси підписання текстового документа (файла), його перевірку, шифрування та розшифрування на прикладі програмного комплексу користувача Центру сертифікації ключів одного з комерційних банків України (рис. 1).

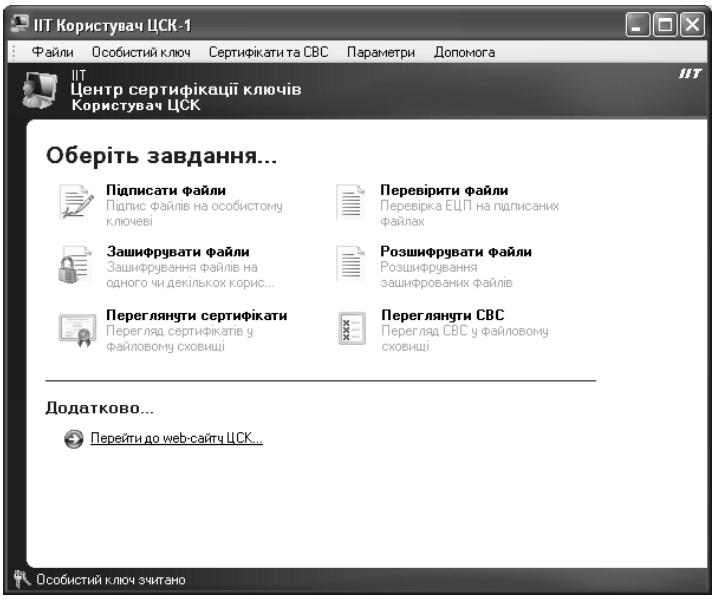


Рисунок 1. Початкова сторінка програмного комплексу для накладання ЕЦП

Програмний комплекс призначений для застосування на засобах електронно-обчислювальної техніки користувача (автоматизовані системи класу 1 [1]) Центру сертифікації ключів і виконує наступні функції:

- управління ключами користувача;
- перевірку сформованого сертифіката користувача на відповідність запиту;
- зміну паролю захисту особистого ключа;
- знищення особистого ключа;
- перевірку чинності та цілісності сертифікатів та ін.;
- захист файлів користувача;
- підпис файлів;
- перевірку файлів;
- шифрування файлів;
- розшифрування файлів.

Для початку отримуємо власний сертифікат ключа (рис. 2).

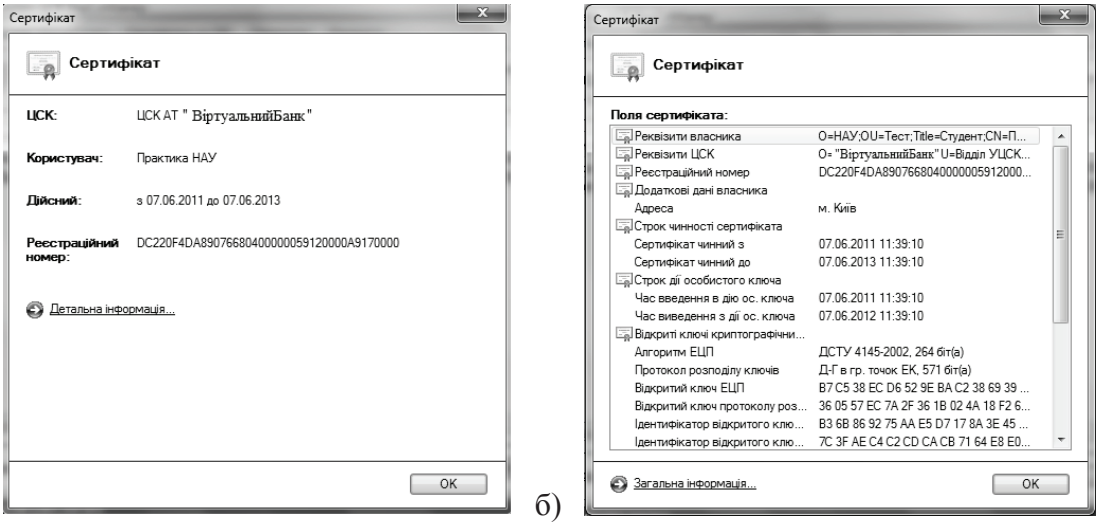
Обираємо документ, на який буде накладено ЕЦП (рис. 3). Створений документ містить додаткові дані, що додані до початкової інформації, що видно з рис. 3. ЕЦП дозволяє точно ідентифікувати особу, яка наклала ЕЦП, а також час підписування документу.

При перевірці ЕЦП підписаного електронного документу можна отримати дані про особу, яка наклала ЕЦП, та час підписання, що видно з рис. 4.

У випадку, якщо збережений документ було пошкоджено чи несанкціоновано змінено (підроблено), то результат перевірки ЕЦП дає про це знати (рис. 5).

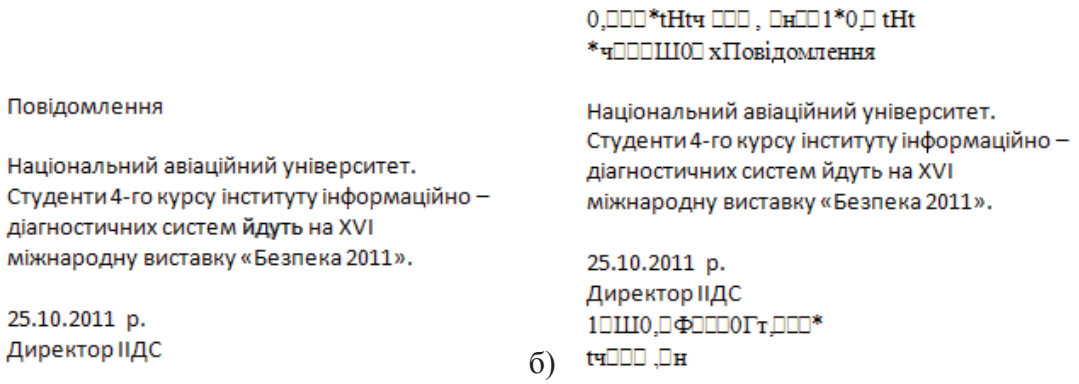
Таким чином, за допомогою накладення ЕЦП здійснюється захист інформації, а саме:

- захист від модифікації даних;



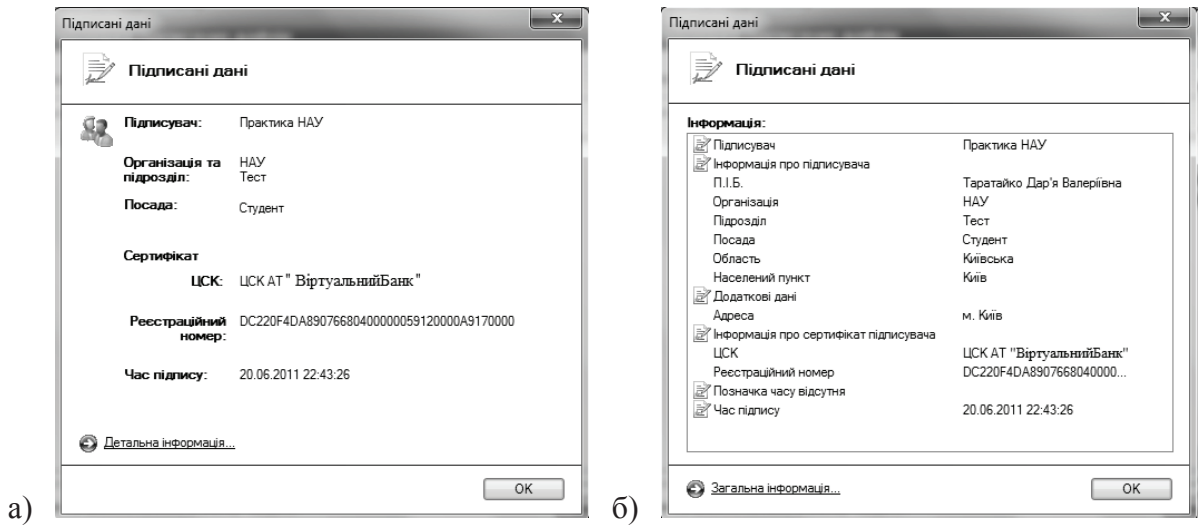
а) б)

Рисунок 2. Сертифікат криптографічного ключа (а) та ґрунтовна інформація про нього (б)



а) б)

Рисунок 3. Початковий (а) та підписаний ЕЦП (б) документи



а) б)

Рисунок 4. Перевірка ЕЦП підписаного документу

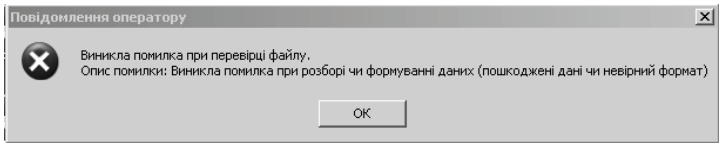


Рисунок 5. Результат перевірки автентичності документу

– захист від втрати частини даних;
– неможливість відмовитися від авторського підпису.

Крім того при використані сертифікованих засобів ЕЦП, електронний документ набирає юридичної сили, рівний силі такого ж документа на паперовому носії зі звичайним підписом ручкою/чорнилами.

Розглянемо початковий та підроблений документи (рис. 6), де змінено лише одну літеру (зафарбоване слово), а зміст документа стає за суттю кардинально різним.

а)

Повідомлення

Національний авіаційний університет.
Студенти 4-го курсу інституту інформаційно – діагностичних систем йдуть на XVI міжнародну виставку «Безпека 2011».

25.10.2011 р.
Директор ІІДС

б)

Повідомлення

Національний авіаційний університет.
Студенти 4-го курсу інституту інформаційно – діагностичних систем їдуть на XVI міжнародну виставку «Безпека 2011».

25.10.2011 р.
Директор ІІДС

Рисунок 6. Початковий та підроблений документи

Далі застосовується до всього підписаного документу один з відомих асиметричних криптографічних алгоритмів [2] для забезпечення конфіденційності даних, що видно на рис. 7, причому маємо два файли, які відрізняються один від одного певною кількістю символів, а не однією літерою, як в початковому документі.

а)

```
O-‘0”_□□□□  0Гт.□□□*
1*0,□ tHt оп_ □□□ рлр □□□0Гт,□□□*мсCGR]
1*0,□ tHt]рмбігвзга □□□0Гт,□□□*ш о □□□ тсм
□□□ лр_ми □□□0_Гт,□□□*плfxd{‘liu1*0,□ tHt
uk □□□0Гт,□□□*t
ouir1*0.□ t_ H te□□M_JL08][\]ев □□□0Гт,□□□*н
н □□□□□□ дgdejγ1*0,□ tHt c □□□:)□□□□ нЮ
,,тикв1*0,□ tHt в» □□□ _а%лотрла89У:3т □□□
ад0п65ywa □□□ wask5375w9u1*0,□ tHt
w3er&*&670{]
```

б)

```
O-‘0”_□□□□  0Гт.□□□*
1*0,□ tHt оп_ □□□ рлр □□□0Гт,□□□*мсCGR]
1*0,□ tHt]рмбігвзга □□□0Гт,□□□*ш о □□□ тсм
□□□ лр_ми □□□0_Гт,□□□*плfxd{‘liu1*0,□ tHt
uk □□□0Гт,□□□*t
ouir1*0,□ t*ч□□□Ш0□ L08][\]ев □□□0Гт,□□□*н
н □□□□□□ дgdejγ1*0,□ tHt c □□□:)□□□□ нЮ
,,тикв1*0,□ tHt в» □□□ _а%лотрла89У:3т □□□
ад0п65ywa □□□ wask5375w9u1*0,□ tHt
w3er&*&670{]
```

Рисунок 7. Результат застосування криптографічного алгоритму до початкового і підробленого документів

3 Види шахрайства

З імовірних вразливостей ЕЦП насамперед відзначимо наступні.

Закритий ключ теоретично можна обчислити на основі відкритого ключа, хоча на практиці це завдання вважається важко здійснюваним за певний проміжок часу. Обчислення ключа дозволить зловмисникові підробляти підпис легітимного користувача. Для протидії цій загрозі слід використовувати криптографічні ключі довжиною не менше 1000 бітів.

Необхідно застосувати заходи для того, щоб зловмисники не могли вивчити протокол роботи засвідчувального органу. Якщо, наприклад, запитати поспіль генерацію декількох відкритих ключів та проаналізувати закономірності, то на основі цього аналізу можна спробувати вгадати, який ключ буде згенерований для наступного запиту. Для запобігання такої небезпеки рекомендується застосовувати «сильні» способи генерації випадкових чисел, такі як, наприклад, генератор білого шуму або лічильник Гейгера.

У тих же цілях потрібно збільшити довжину ключа і значення хеш-функції – односпрямованої криптографічного функції, яка використовується в алгоритмах накладання та перевірки ЕЦП. Це на порядок зменшить імовірність підбору електронного підпису.

4 Методи боротьби

Поєднавши ЕЦП і стеганографії можна підвищити захищеність документа, проте самі ці технічні засоби також потребують захисту. Адже зловмисник може змінити як цифровий знак, так і дані, контейнер або цифровий водяний знак (ЦВЗ).

Для підвищення захищеності файлів пропонується підписувати весь контейнер (електронний документ або об'єкт авторського права) з вбудованими ЦВЗ і ЕЦП, отриманого з використанням закритого ключа автора документа. Підпис має зберігатися в засвідчувальному органі.

Будь-який легальний користувач може за допомогою відкритого ключа (всі вони зберігаються в засвідчувальному органі у відкритому доступі) перевірити справжність і незмінність файлу. ЦВЗ є гарантією того, що навіть якщо зловмисник підпише файл від свого імені, результати перевірки його електронного підпису та ЦВЗ не співпадуть і можна буде встановити порушення. ЦВЗ виступає в якості додаткового рівня захисту, який іноді важко навіть виявити, а тим більш обійти. Цей рівень захисту дозволяє довести авторство при експертизі.

Висновки

Таким чином, одночасне незалежне використання кількох технічних заходів захисту (ЦВЗ, ЕЦП, мітки часу) суттєво підвищує рівень захищеності електронного документа. Потрібно витратити чимало коштів, ресурсів та часу (місяці, навіть роки), щоб підібрати ЕЦП до електронного документа.

Література

[1] Соколов А.В. Методы информационной защиты объектов и компьютерных сетей / А.В. Соколов, О.М. Степанюк. – М.: Полигон АСТ, 2000. – 269 с.

[2] Шнайер Б. Прикладная криптография / Б. Шнайер. – М.: Триумф, 2002. – 816 с.

[3] Закон України «Про електронний цифровий підпис» від 22.05.2003 р., №852-IV // ВВР України. – 2003. – №36. – Ст. 276.