Автори: Шпортько О. В., Савицька І. О.

Лабораторна робота № 10.

Тема. Застосування криптографічних засобів захисту інформації. Генерування і використання електронного цифрового підпису для реалізації захисту файлів користувача.

Мета. Формування вмінь і навиків організації криптографічного захисту інформації. Отримання знань методів і способів генерування електронних цифрових підписів та навиків використання відповідного програмного забезпечення. Закріплення знань файлової структури, вмінь і навиків використання можливостей диспетчерів файлів та поштових систем для пересилання фалів іншим користувачам.

Теоретичні відомості

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

З переходом до цифрових способів передачі й зберігання даних, а також з розвитком систем електронного переказу коштів, в основі яких – електронний аналог паперового платіжного доручення, проблема віртуального підтвердження автентичності документа набула особливого значення. Розвиток будь-яких подібних систем тепер немислимий без існування електронних підписів під електронними документами**.**

Правовий статус електронного цифрового підпису в Україні визначається Законом України «Про електронний цифровий підпис», згідно якого, електронний цифровий підпис – це 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 підписувача.

Одним з органів, пов'язаних з сертифікацією ключів, є Акредитований центр сертифікації ключів Інформаційно-довідкового департаменту Державної фіскальної служби (АЦСК ІДД ДФС), одним з основних завдань якого є безкоштовне надання послуг електронного цифрового підпису (далі - ЕЦП) органам державної влади, органам місцевого самоврядування, підприємствам, установам та організаціям всіх форм власності, іншим суб’єктами господарської діяльності та фізичним особам.

ІІТ Користувач ЦСК-1 – це програма, розроблена для застосування на комп’ютерній техніці клієнтів АЦСК ІДД ДФС для виконання наступних функцій:

- накладення ЕЦП на будь-яку інформацію в електронному вигляді (текстові, відео-, аудіо- файли, файли баз даних тощо), а також для криптографічного захисту інформації, шляхом її направленого шифрування;
- генерації ключів підписувачів АЦСК ІДД ДФС, резервного копіювання особистого ключа з одного носія ключової інформації на інший, знищення особистого ключа;
- перевірки сертифіката підписувача;
- формування та передачі до АЦСК ІДД ДФС запиту на блокування/скасування сертифіката підписувача;
- доступу до сертифікатів АЦСК ІДД ДФС, серверів АЦСК ІДД ДФС, сертифікатів інших підписувачів та списку відкликаних сертифікатів з метою перегляду і пошук сертифікатів підписувачів у файловому сховищі, визначення статусу сертифікатів підписувачів, перевірки цілісності сертифікатів.

Для отримання практичних навичок захисту інформації шляхом створення ЕЦП використаємо програму *ІІТ Користувач ЦСК-1*, головні переваги якої – простота використання, безкоштовне використання та легальність використання на території України.

Підготовчий етап заняття. Актуалізація знань

1. Віднайдіть ваш файл з описом різновиду апаратного засобу захисту чи зламу захисту та скопіюйте його в буфер обміну.
2. Створіть нову папку для організації криптографічного захисту та вставте в неї скопійований файл.
3. Для генерації та використання ЕЦП встановіть програму *ІІТ Користувач ЦСК-1*. Для цього завантажте архівний файл інсталяційного пакету програми з веб-сайту за посиланням http://acskidd.gov.ua/korustyvach_csk чи віднайдіть цей архівний файл інсталяції на сайті АЦСК ІДД ДФС. Розпакуйте архівний файл та здійсніть інсталяцію ПЗ, виконавши наступні дії:
   3.1. Завантажте інсталятор ПЗ – файл *EUInstall.exe*, ознайомтеся з положеннями ліцензійної угоди та натисніть кнопку **Далі**;
   3.2. Якщо вас не влаштовує стандартне розташування файлового сховища, то змініть його розташування, натиснувши кнопку **Змінити** та обравши відповідний каталог (не той, що створений для криптографічного захисту файлів). Для продовження інсталяції натисніть кнопку **Далі**;
   3.3. За необхідності дозвольте створення ярлика на робочому столі та завантаження ПЗ після завершення його інсталяції. Для цього необхідно проставити відповідні позначки в меню **Додаткові значки**. Для продовження інсталяції натисніть кнопку **Далі**;

3.4. У вікні готовності до інсталяції натисніть кнопку **Встановити**.

Генерація особистого ключа та отримання сертифікатів від ПАТ КБ «ПриватБанк»

4. Оскільки АЦСК ІДД ДФС видає сертифікати юридичним особам та фізичним особам-суб'єктам підприємницької діяльності, а не окремим фізичним особам, то **отримайте ключ** (використано дані https://docs.google.com/document/d/1y6TBhCn5v8NnrnCyQjjmM2vm-Q3ECXloaepNoW2E7Ts/edit?_=0.3562585416687598) **від ПАТ КБ «ПриватБанк»**. Для цього:

4.1. Перейдіть на сайт ПАТ КБ «ПриватБанк» та увійдіть у Приват24;

4.2. Оберіть у власному кабінеті Приват24 посилання **Усі послуги – Бізнес – Електронний цифровий підпис – Завантажити сертифікат** (рис. 1). При потребі встановіть та завантажте додаткове програмне забезпечення;

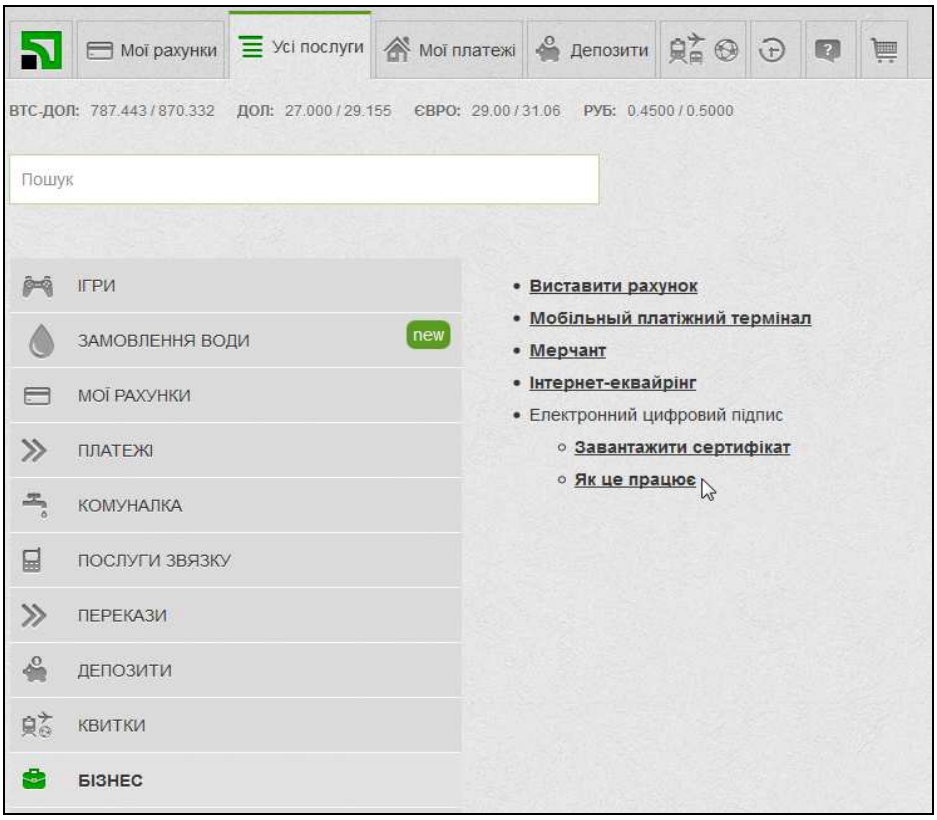

Рис. 1. Початок генерації ключа від ПАТ КБ «ПриватБанк»

4.3. Заповніть заявку на отримання сертифіката. Зверніть увагу, що поле **E-mail** обов'язкове для заповнення, а прізвище, ім'я та по-батькові мають співпадати з паспортними даними і не містити зайвих розділових знаків попереду і всередині, як на рис. 2. Не забудьте перевірити точність написання електронної пошти з дотриманням прописних літер. Образ екрану з реєстраційними даними для отримання ключа збережіть у файлі *Screen.doc*. Після корегування та перевірки даних натисніть кнопку **Дані вірні**;

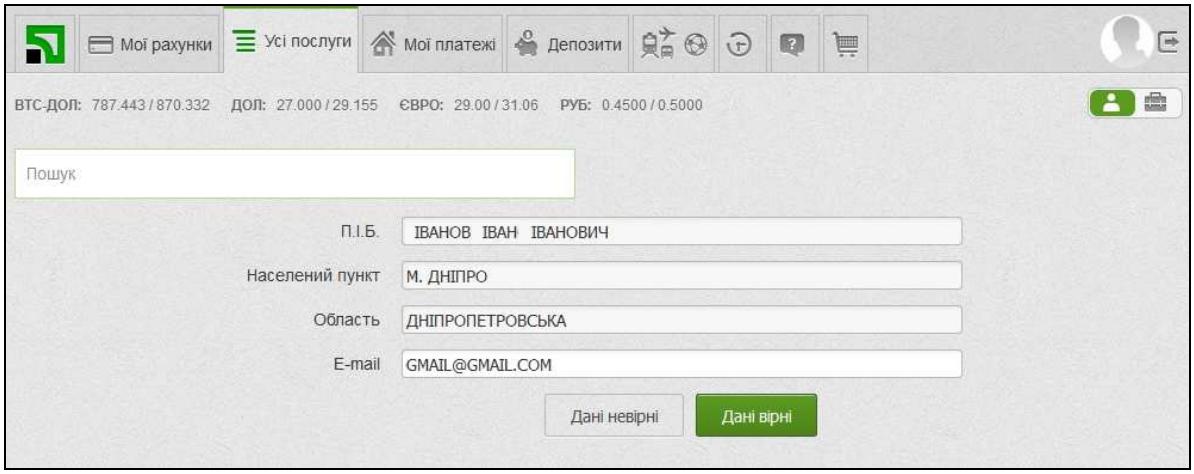

Рис. 2. Перевірка особистих даних для генерації ключа від ПАТ КБ «ПриватБанк»

4.4. Оберіть каталог, в якому у вас є права на запис, для створення в ній файлу–сховища ключів. Запам'ятайте цей каталог для подальшого використання ключа;

4.5. Введіть та підтвердіть пароль на файл–сховище ключів. Мінімальна довжина паролю – 8 символів, він може включати у себе букви латинського алфавіту та цифри. **Нікому і ніколи не повідомляйте цей пароль**;

4.6. На наступній сторінці введіть пароль, що надійшов у SMS або мобільному додатку **Privat24**, встановіть прапорець навпроти пункту **Я ознайомлений та згоден з Умовами та правилами надання банківських послуг і підтверджую коректність даних відправлених мною** та натисніть **Далі**;

4.7. Ознайомтеся з інформацією щодо створеного ключа та згенерованих сертифікатів. Завершіть роботу з Приват24.

5. Перевірте наявність файла-сховища ключів у вказаному вами каталозі. Цей файл повинен мати розширення *jks*. **Нікому і ніколи не передавайте цей файл. Це – ваш особистий електронний підпис з обмеженим терміном дії.**

6. Завантажте сертифікати для використання згенерованих ключів. Для цього:

6.1. Перейдіть на сайті акредитаційного центру сертифікації ключів ПАТ КБ «ПриватБанк» до розділу **Сертифікати** (https://acsk.privatbank.ua/certs);

6.2. Введіть ваші дані (наприклад, ПІБ чи ІПН) та натисніть кнопку **Знайти**;

6.3. Завантажте віднайдені сертифікати і відомості про них у папку з файлом-сховищем ключів за допомогою посилань справа. Які розширення мають файли сертифікатів та файли відомостей про них? Перегляньте відомості ваші про сертифікати. Перегляньте відомості про сертифікати у вікні їх властивостей.

6.4. **Скопіюйте завантажені сертифікати** також у каталог файлового сховища програми *ІІТ Користувач ЦСК-1* АЦСК ІДД ДФС.

Використання електронного ключа для накладання електронного цифрового підпису

7. Завантажте програму *ІІТ Користувач ЦСК-1* (рис. 3);

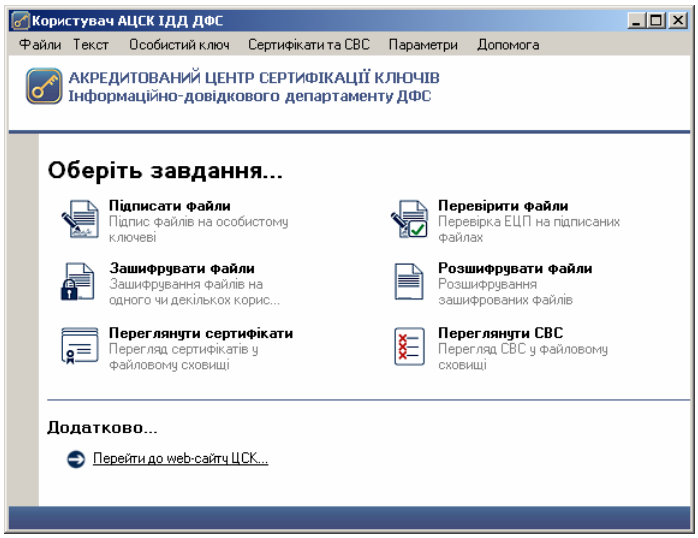

Рис. 3. Робочий стіл програми *ІІТ Користувач ЦСК-1*

8. Перегляньте наявні сертифікати з файлового сховища та перевірте наявність у ньому ваших сертифікатів (рис. 4). При відсутності ваших сертифікатів у переліку спробуйте використати інші позиції поля зі списком верхньої частини вікна. Коли ж і це не допоможе, то повторно скопіюйте завантажені сертифікати АЦСК ПАТ КБ «ПриватБанк» у каталог файлового сховища програми *ІІТ Користувач ЦСК-1*, перезавантажте цю програму та перегляньте наявні сертифікати знову.

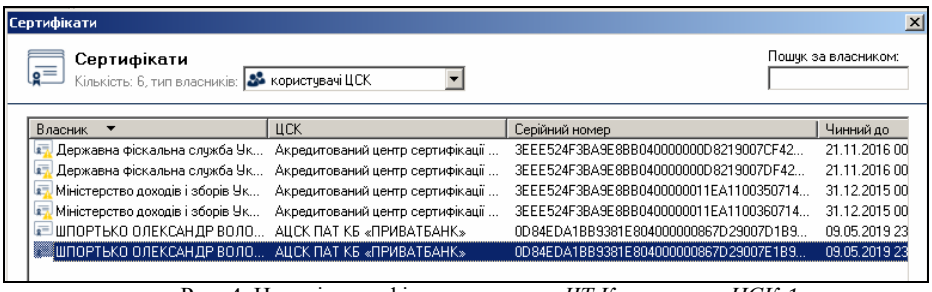

Рис. 4. Наявні сертифікати програми *ІІТ Користувач ЦСК-1*

9. Накладіть електронний цифровий підпис на ваш файл з описом різновиду апаратного засобу захисту чи зламу захисту, але лише після перевірки наявності ваших сертифікатів у файловому сховищі (див. попередній пункт). Для цього:

9.1. На робочому столі програми оберіть посилання **Підписати файли** (див. рис. 3);

9.2. У вікні захищеного робочого столу оберіть носій інформації, на якому зберігається ваш ключ, або **оберіть файл ключа у розділі файлова система (каталоги користувача)**. У відповідне поле введіть пароль захисту особистого ключа (рис. 5) та повторіть його у полі нижче і натисніть кнопку **Зчитати**;

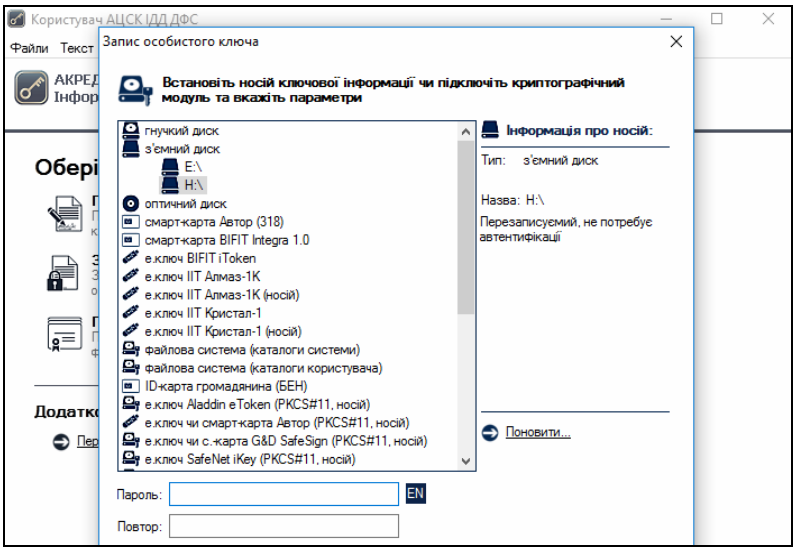

Рис. 5. Зчитування особистого ключа в програмі *ІІТ Користувач ЦСК-1*

9.3. Додайте файл для накладання ЕЦП, оберіть формат ЕЦП *з позначкою часу від ЕЦП* (рис. 6), самостійно забезпечте додавання до файла сертифікату та натисніть кнопку **Підписати**. Яке розширення має файл з накладеним ЕЦП?

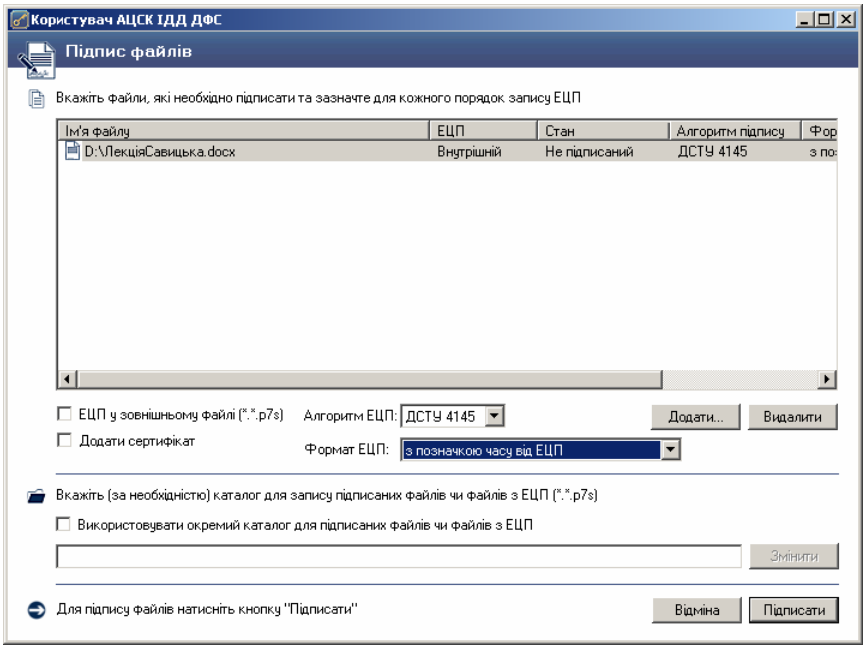

Рис. 6. Параметри накладання ЕЦП в програмі *ІІТ Користувач ЦСК-1*

Закріплення вмінь використання електронного ключа та сертифікатів

10. Самостійно перевірте ЕЦП підписаного файла.
11. Самостійно зашифруйте та розшифруйте ваш файл з описом різновиду апаратного засобу захисту чи зламу захисту. Яке розширення має зашифрований файл? Як на нього додатково накласти ЕЦП?
12. Завантажте сертифікати до електронних ключів ПАТ КБ «ПриватБанк» двох ваших колег. Скопіюйте їх у каталог файлового сховища програми *ІІТ Користувач ЦСК-1*. Використовуючи можливості пункту головного меню **Текст – Зашифрувати**, зашифруйте ваш улюблений анекдот, обравши для сертифікатів отримувачів свій сертифікат та сертифікати цих колег. Перешліть зашифрований текст електронною поштою своїм колегам. Чи вдалося їм розшифрувати зашифрований текст за допомогою пункту меню програми **Текст – Розшифрувати** (рис. 7)? Які ще додаткові відомості при цьому відображаються? Образ екрану з розшифруванням тексту збережіть у файлі *Screen.doc*.
13. Самостійно встановіть програму *PrivateSign* від ПАТ КБ «ПриватБанк» для вашої операційної системи для накладання/перевірки ЕЦП і шифрування/розшифровування файлів

(https://acsk.privatbank.ua/program). Виконайте в ній ці базові операції. Які додаткові відомості при перевірці ЕЦП видає ця програма?

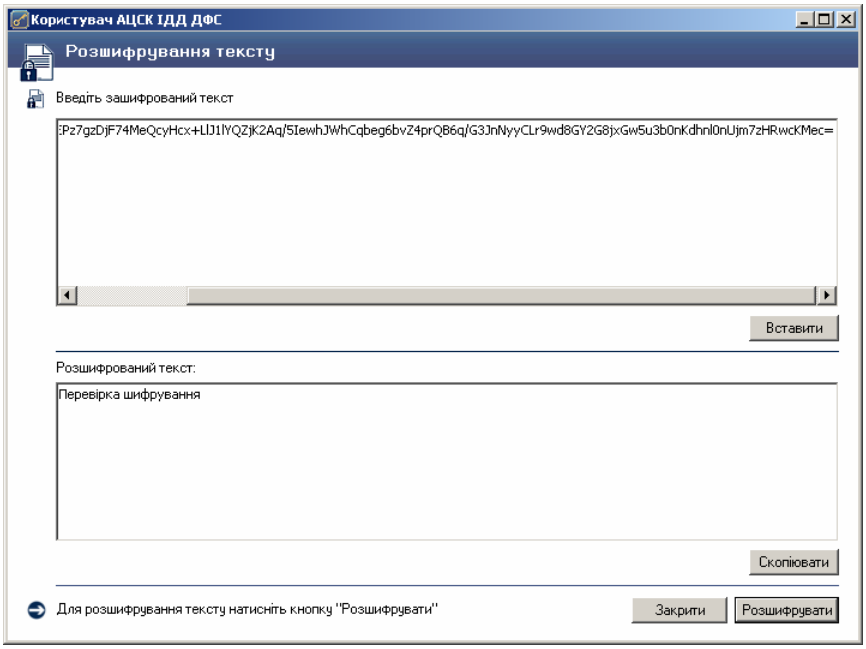

Рис. 7. Розшифрування зашифрованого тексту в програмі *ІІТ Користувач ЦСК-1*

Генерація особистого ключа користувачем для подання звітності в ДФС (лише для майбутніх керівників організацій та СПД)

14. Для генерації особистого ключа від ДФС виконайте наступні дії:
    14.1. Вставте носій інформації, на який в подальшому буде згенеровано особистий ключ;
    14.2. Завантажте встановлену програму генерації ключів АЦСК ІДД ДФС;
    14.3. В головному меню програми **Особистий ключ** оберіть пункт **Згенерувати ключі**. У вікні **Генерація ключів**, що з'явиться на екрані, додатково проставите відмітку **Використовувати окремий ключ для протоколу розподілу**, як на рис. 8, та натисніть кнопку **Далі**;

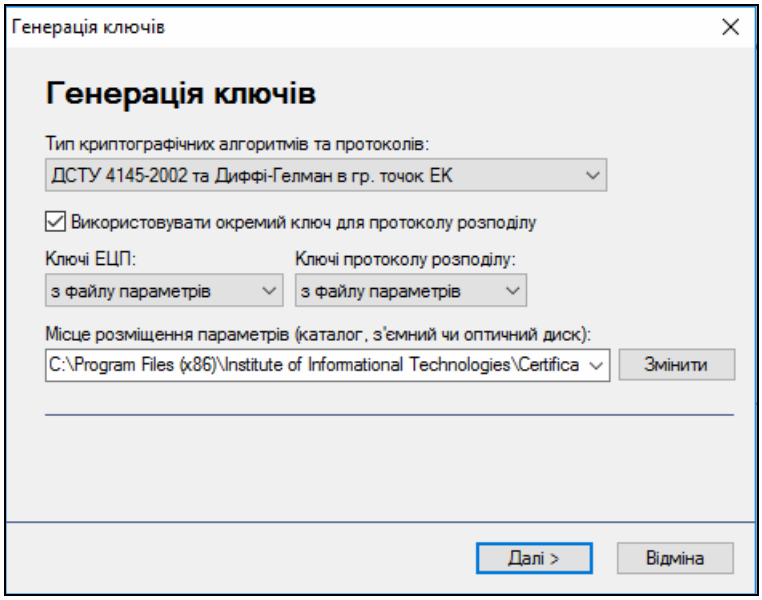

Рис. 8. Меню **Особистий ключ** програми *ІІТ Користувач ЦСК-1*

    14.4. У вікні захищеного робочого столу, що з'явився після натискання кнопки **Далі**, оберіть носій інформації, на який буде записано ключ. У відповідне поле введіть пароль захисту особистого ключа (аналогічно рис. 5), повторіть його у полі нижче та натисніть кнопку **Записати**.
    14.5. Після генерації особистого ключа з'явиться два вікна запитів на формування сертифікатів підписування та шифрування, в яких натисніть кнопки **ОК**.
    14.6. Для створення запитів до ДФС на отримання сертифікатів в папці для сертифікатів та СВС доповніть автоматично згенероване ім'я файлу вашим ПІБ, як на рис. 9, після чого послідовно натисніть кнопки **Далі** та **Завершити**.

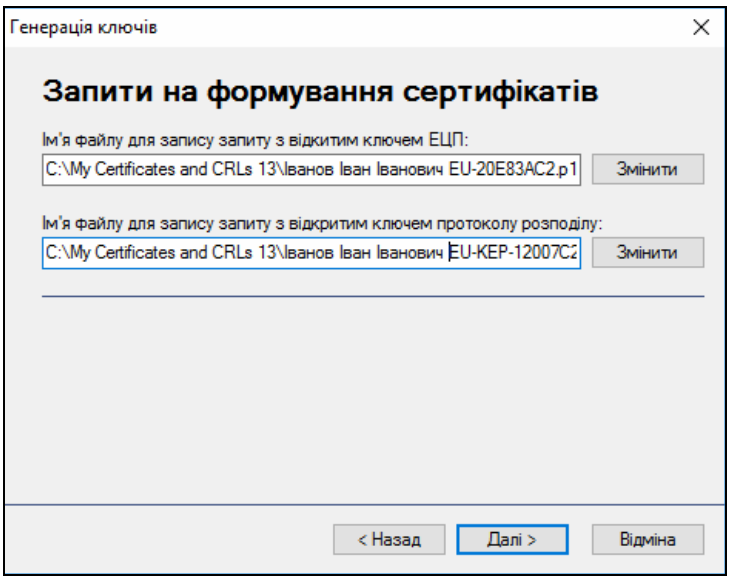

Рис. 9. Заповнення запиту на формування сертифікатів

14.7. Перевірте наявність згенерованого ключа на носії інформації.

14.8. Для отримання сертифікатів до цього ключа в подальшому, під час професійної діяльності, необхідно подавати реєстраційні документи з згенерованими файлами запитів до ДФС.

Завершальний етап заняття. Повторення вивченого матеріалу.

15. **Якщо ви не плануєте використовувати ЕЦП та шифрування найближчим часом, то відкличте сформований сертифікат за допомогою відповідного посилання на сторінці https://acsk.privatbank.ua/service та видаліть файл-сховище ключів.**
16. Створіть електронний лист з формулюваннями та відповідями на контрольні запитання у своїй поштовій скриньці на сайті *gmail.com*. Приєднайте до цього листа файл *Screen.doc*, підписаний ЕЦП та зашифрований файл, PDF-файл з описом вашого сертифіката. Тему листа сформуйте за шаблоном *<група>_<номер лабораторної>_<прізвище ім'я>*, наприклад: *ЕК51_ЛР10_Величко Володимир*. Надішліть створений лист на адресу LRZaxInf@gmail.com.

Контрольні запитання.

1. Чому для шифрування даних на сьогодні крім обраних алгоритмів найчастіше використовуються ключі?
2. Які алгоритми шифрування називаються симетричними, а які – асиметричними, які відкритими, а які – закритими?
3. Яке призначення відкритих ключів?
4. Де і навіщо зберігаються закриті ключі?
5. Яке призначення файла-сховища ключів та сертифікатів? Як їх отримати? Який з цих файлів зберігають на захищених носіях, а які – вільно поширюють серед колег?
6. Що необхідно встановити на комп'ютері для накладання/перевірки ЕЦП та шифрування/розшифровування файлів?
7. Чому розмір зашифрованого файла найчастіше перевищує розмір вхідного файла?