Робота з криптомодулем Гряда в комп’ютерній програмі M.E.Doc

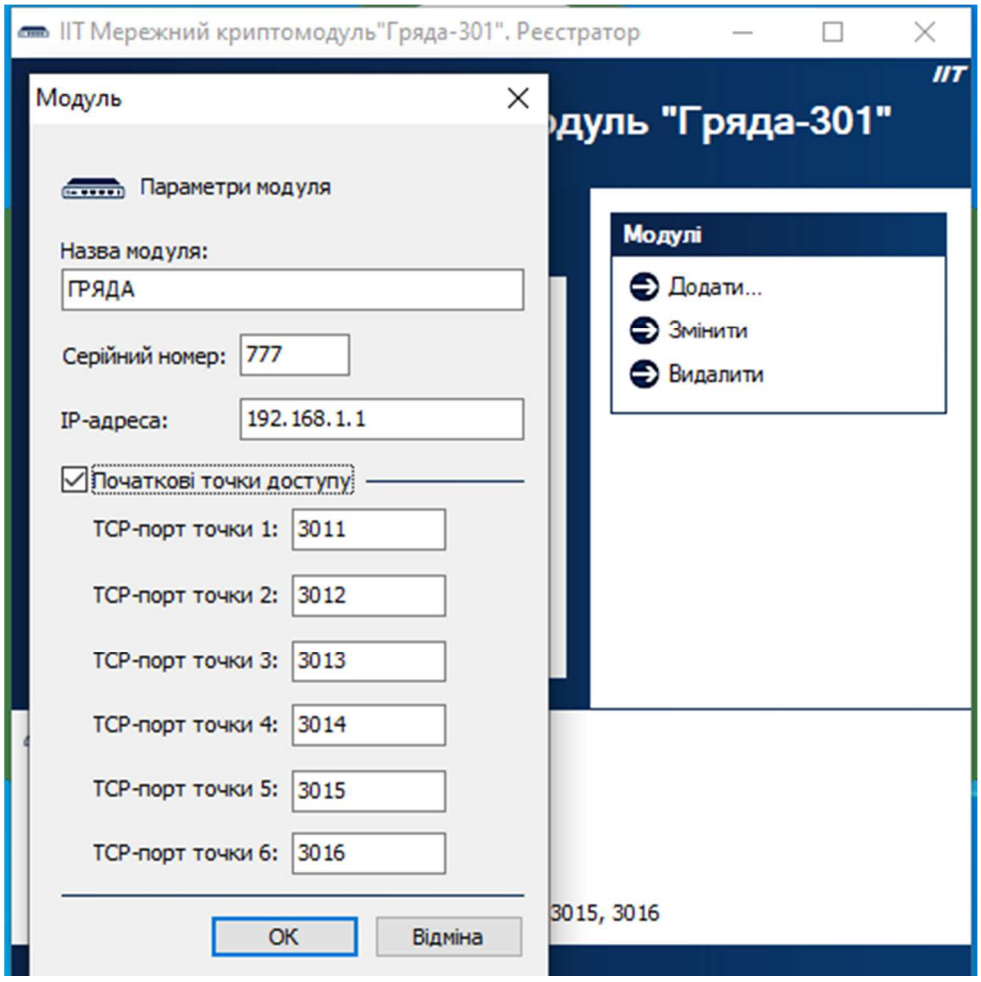
Реєстрація криптомодуля на комп’ютері користувача

Для підключення криптомодуля «Гряда» та подальшої його роботи з програмою **M.E.Doc**, необхідно виконати реєстрацію криптомодуля на ПК.

Увага! Реєстрація виконується на всіх комп’ютерах де буде використовуватись криптомодуль.
Для роботи з криптомодулем «Гряда» необхідно обов’язково забезпечити доступ до IP адреси, за якою він буде підключений, та до портів, які призначені для використання точок доступу пристрою (токенів). Доступ має бути наданий для користувачів, які будуть використовувати у роботі криптомодуль «Гряда».

Для реєстрації:

1. Встановіть утиліту від виробника криптомодуля (ІІТ) **NCMGryada301Install.exe**.
2. Після встановлення запустіть програму «Реєстратор» та натисніть **Додати**.



3. У вікні програми зазначте параметри підключення до криптомодуля «Гряда»:
   - Назва модуля;
   - Серійний номер;
   - IP адреса;
   - позначку «Початкові точки доступу» (за замовчуванням порти точок доступу 3011-3016).

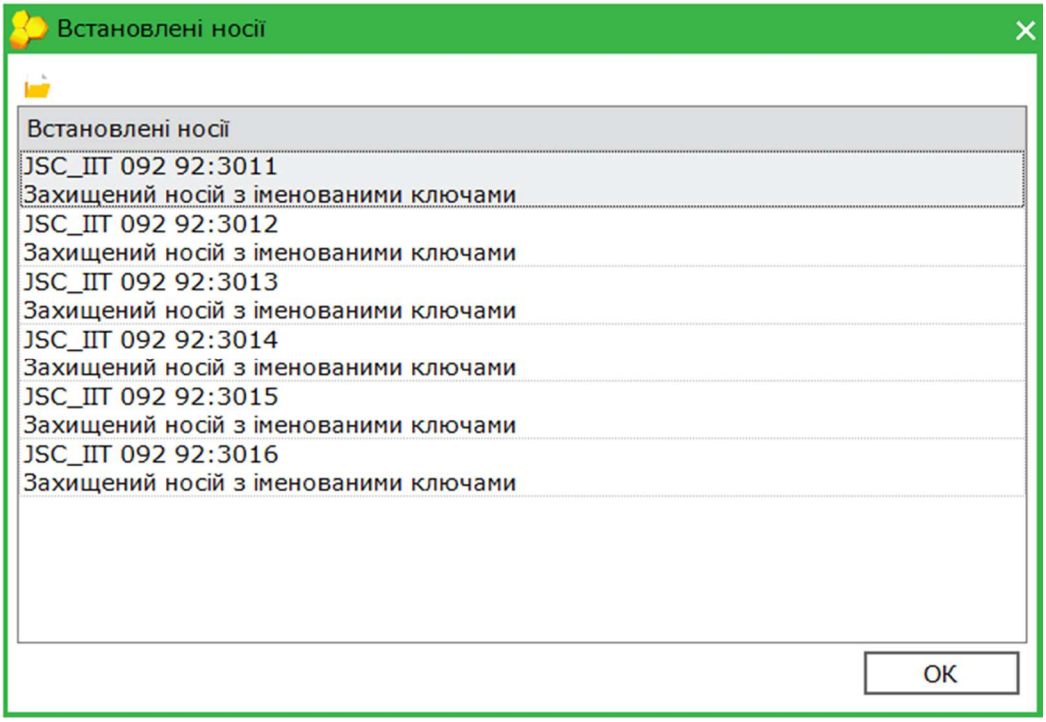
Увага! У випадку, якщо при налаштуванні модуля адміністратором було змінено порти для роботи, потрібно вказати актуальні порти для роботи пристрою.

4. Натисніть кнопку **ОК**. Програма виконає реєстрацію та збереження даних в реєстрі операційної системи.

Для повноцінного управління криптомодулем «Гряда» необхідно встановити модуль управління **NCMGryada301RemoteControlInstall.exe**.

Налаштування використання криптомодуля «Гряда» в програмі M.E.Doc

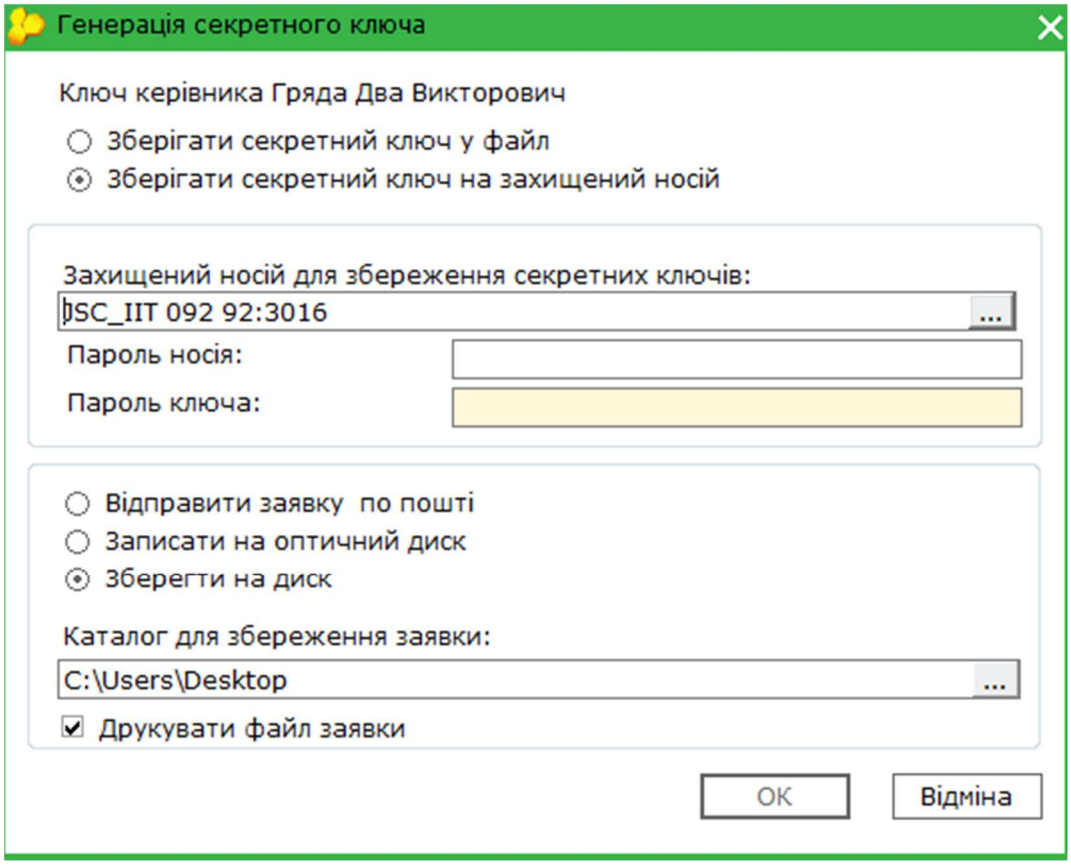
1. Оновіть програму **M.E.Doc** до версії **11.02.010**.
2. Забезпечте доступ до IP адреси, за якою підключений криптомодуль «Гряда», та до портів, які призначені для використання точок доступу пристрою (токенів). Доступ має бути наданий для користувачів, які будуть використовувати у роботі криптомодуль «Гряда».
3. Після надання доступу до мережевої IP адреси криптомодуля «Гряда» програма **M.E.Doc** автоматично визначить точки доступу та налаштує роботу з ними.
4. Для перевірки доступності криптомодуля «Гряда» в програмі **M.E.Doc** перейдіть у модуль **Адміністрування – Сертифікати** та оберіть пункт меню **Файл – Захищений носій – Встановлені носії**.
5. У вікні **Встановлені носії** будуть відображені всі доступні пристрої, у тому числі криптомодуль «Гряда», у вигляді:



Генерація ключів на криптомодуль «Гряда»

1. Перейдіть у модуль **Адміністрування – Сертифікати – Заявки на сертифікат** та натисніть **Створити**.
2. Заповніть необхідні дані відповідно до майстра створення заявок на сертифікат.
3. У вікні **Генерація секретного ключа** встановіть позначку **Зберігати секретний ключ на захищений носій** та оберіть один із доступних слотів криптомодуля «Гряда».

   Увага! На один слот криптомодуля можна генерувати декілька секретних ключів різних організацій. Кількість ключів обмежується технічними можливостями моделі криптомодуля «Гряда».

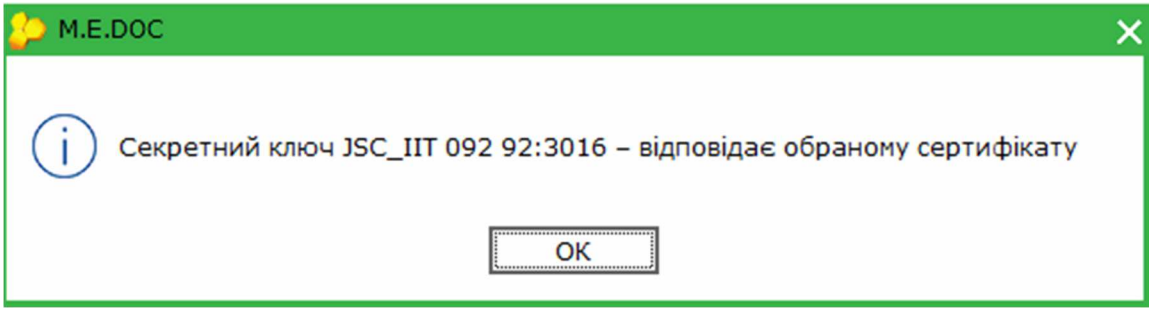


4. У полі **Пароль носія** вкажіть пароль доступу до модуля «Гряда».
5. У полі **Пароль ключа** вкажіть пароль для секретного ключа.
6. Натисніть кнопку **ОК**. Відбудеться генерація секретного ключа на криптомодуль.

Пошук відповідного секретного ключа для сертифіката

Для пошуку секретного ключа на криптомодулі «Гряда»:

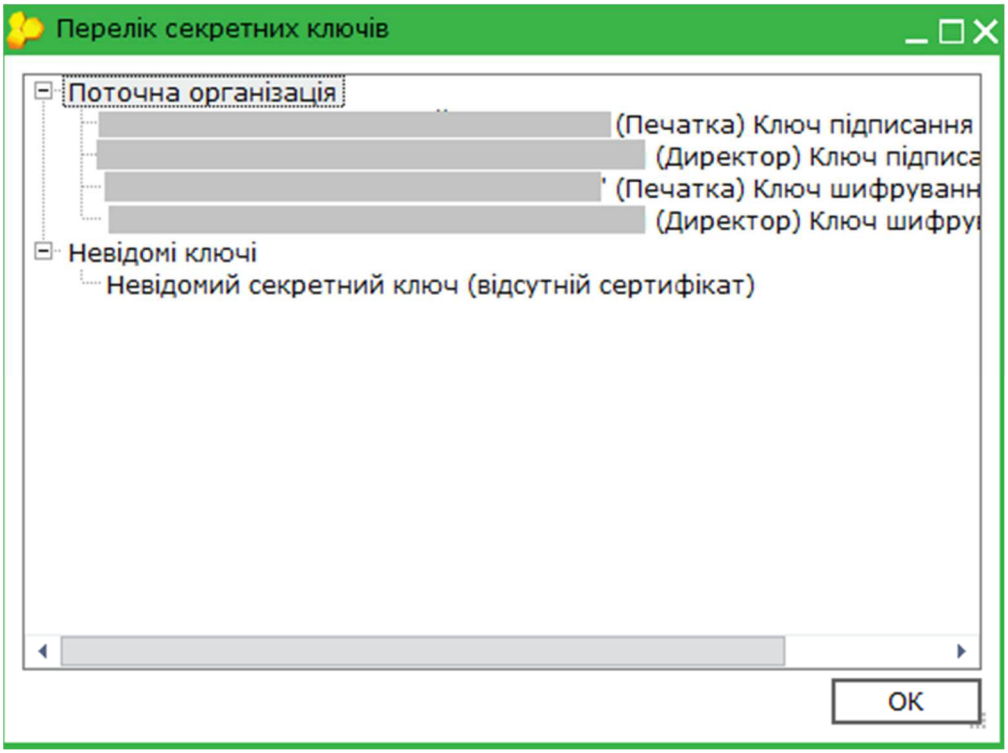
1. Перейдіть у модуль **Адміністрування – Сертифікати – Встановлені сертифікати**.
2. Встановить курсор на відповідний сертифікат та виконайте команду головного меню **Файл – Захищений носій (Token) – Пошук секретного ключа**.
3. Програма автоматично здійснить пошук та проінформує про наявність відповідного ключа:



Пошук та відображення всіх ключів на слоті модуля «Гряда»

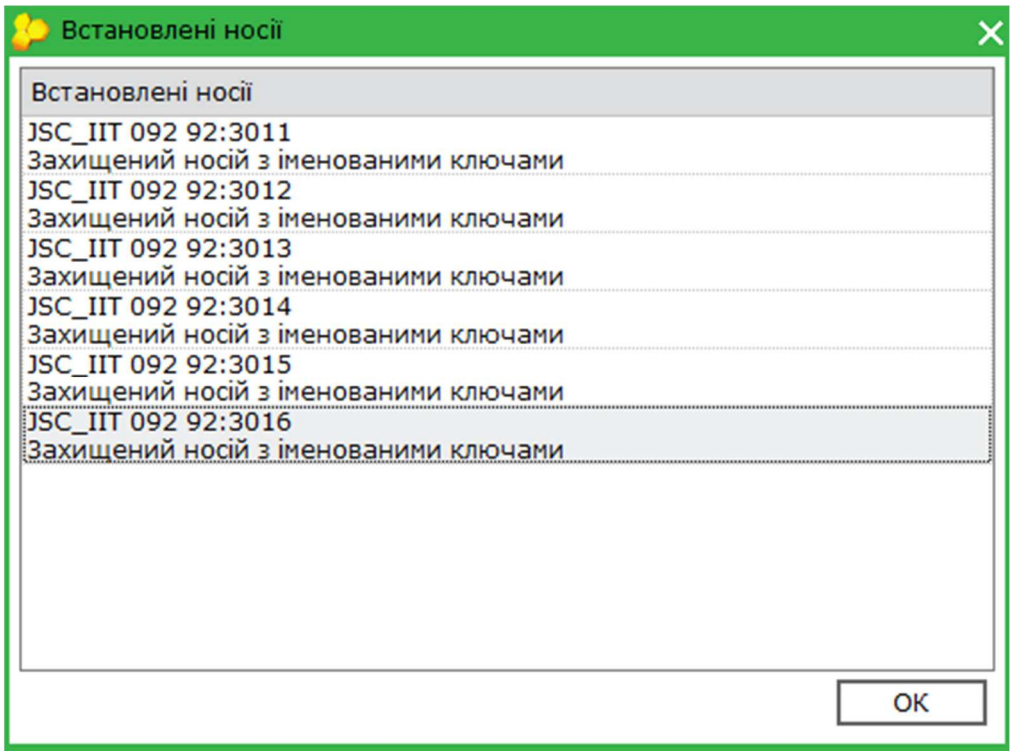
Для отримання детальної інформації про записані на токені ключі:

1. У модулі **Адміністрування – Сертифікати – Встановлені сертифікати** виконайте команду головного меню **Файл – Захищений носій (Token) – Встановлені носії**.
2. Подвійним кліком миші відкрийте необхідний носій, або натисніть кнопку **Перелік ключів** на панелі інструментів вікна **Встановлені носії**.
3. Програма автоматично зчитає доступні ключі та відобразить їх на екрані:

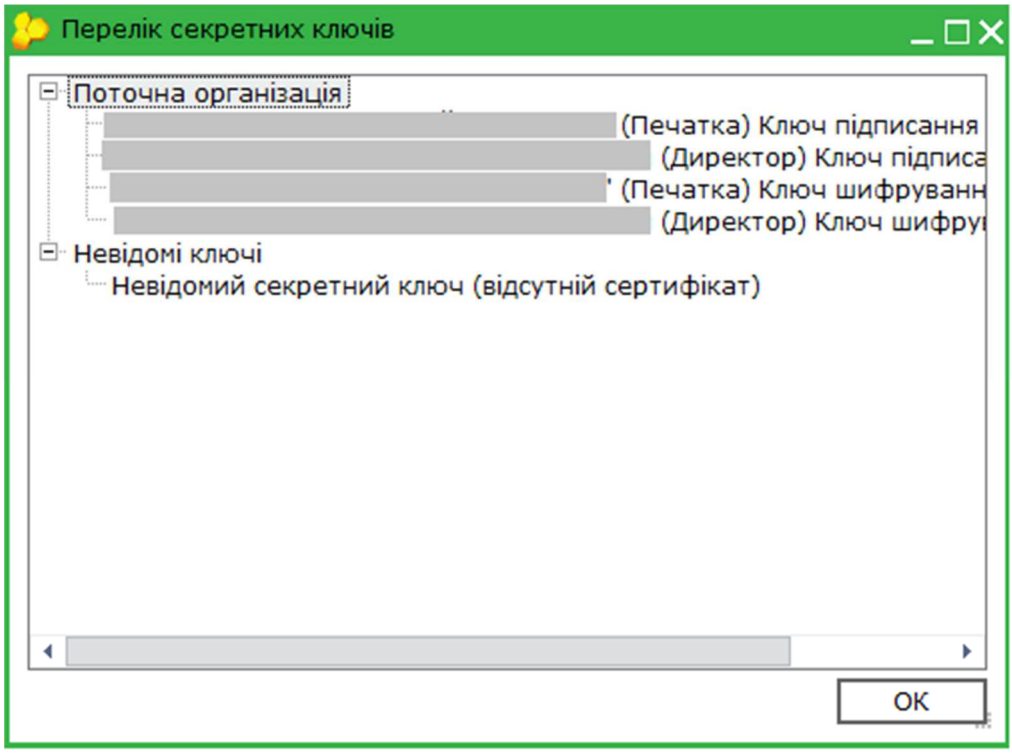


Видалення ключів з криптомодуля «Гряда»

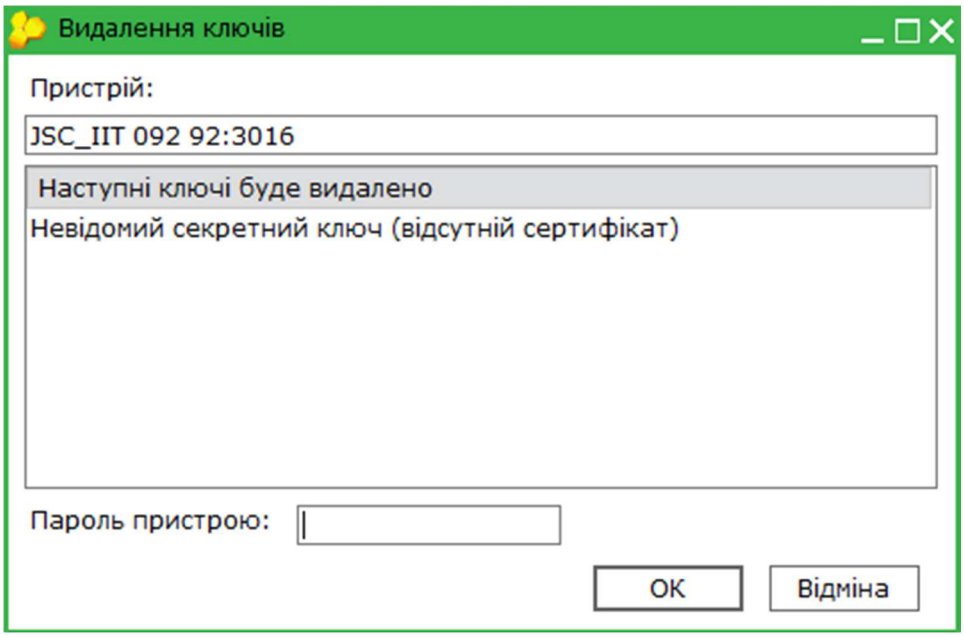
1. Перейдіть у модуль **Адміністрування – Сертифікати – Встановлені сертифікати** та виконайте команду головного меню **Файл – Захищений носій – Цілковите очищення**.
2. У вікні **Встановлені носії** оберіть необхідний слот криптомодуля «Гряда», натисніть **ОК**:



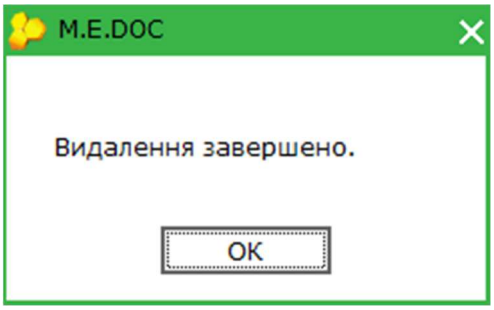
3. У вікні **Перелік секретних ключів** буде відображено доступні для видалення ключі. Установіть курсор на необхідний ключ та натисніть **ОК**:



4. У вікні **Видалення ключів** введіть пароль для доступу до пристрою «Гряда» та натисніть **ОК**:



5. Після завершення операції, програма повідомить користувача про результат:



Підписання документів та прийом повідомлень з використанням ключів, збережених на криптомодулі «Гряда»

У вікні підписання встановіть позначку **Використовувати захищений носій** та виберіть необхідний сертифікат.

Програма автоматично визначить секретний ключ на криптомодулі «Гряда» та виконає запит паролів носія та ключа: