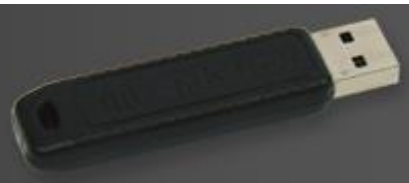
ДКПП 30.02.16.000

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖЕНИЙ
ЄААД.469535.040-ЛУ

АТ ІІТ
Апаратні засоби КЗІ



Електронний ключ “Кристал-1”

Настанова з експлуатації

ЄААД.469535.040 РЭ

Інв. №дубл	Взам. інв. №	Підп. та дата	Інв. №оригі.

Харків 2015 р.

ЗМІСТ

ВВЕДЕННЯ

Назва виробу: електронний ключ “Кристал-1” (далі - ЕК).

Шифр виробу: “ІІТ Електронний ключ Кристал-1”.

Підприємство-виробник: АТ “ІІТ”. Адреса: 61166, м. Харків, вул. Бакуліна, 12. Тел./факс: (057) 714-22-05. Код ЄДРПОУ: 22723472.

1 ОПИС ТА РОБОТА

1.1 Виріб виконує наступні функції:

- автентифікацію адміністратора ЕОМ при доступі до ключа;
- автентифікацію оператора ЕОМ при доступі до ключа;
- генерацію особистих та відкритих ключів для алгоритму ЕЦП;
- генерацію особистих та відкритих ключів для протоколу розподілу ключів;
- генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора;
- зберігання особистих ключів у внутрішній пам'яті та захист їх від НСД;
- формування і перевірку ЕЦП;
- обчислення геш-функції;
- розподіл ключових даних на основі асиметричного протоколу розподілу;
- зберігання довільних даних у внутрішній пам'яті та захист їх від НСД;
- контроль цілісності і працездатності вбудованого програмного забезпечення та ін.

1.2 Технічні характеристики виробу наведені у таблиці 1.

Таблиця 1 – Основні масогабаритні та інші технічні характеристики пристрою

Найменування	Норма
Габаритні розміри (довжина)х(діаметр), мм, не більше (без урахування кріплення)	65 х16
Маса, кг, не більше	0,015
Споживана потужність від блоку електроживлення ЕОМ +5В±10%., Вт, не більше:	0,5

1.3 Склад виробу

- електронний ключ (ЕК);
- носій інформації з інсталяційним пакетом програм (не обов'язково, може комплектуватись одним носієм на декілька виробів);
- комплект експлуатаційних документів (не обов'язково, може комплектуватись одним носієм на декілька виробів);
- комплект тари і пакування (не обов'язково, може комплектуватись одним носієм на декілька виробів).

1.4 Будова та робота виробу

1.4.1 ЕК виконаний у вигляді малогабаритного знімного USB-пристрою, який може мати програмний CCID-інтерфейс (бути CCID-пристроєм).

1.4.2 Конструктивно ЕК виконаний на двошаровій друкованій платі, яка залита компаундом, та встановлена в пластмасовий корпус, що формує зовнішній вигляд виробу. На друкованій платі встановлюються електроні компоненти ЕК та USB-з'єднувач типу A-plug (вилка).

1.4.3 ЕК виконаний у кліматичному виконанні групи 2 за ГОСТ 21552-84.

1.4.4 Електроживлення ЕК, з'єднаного з ЕОМ через USB-з'єднувач, здійснюється від блоку електроживлення ЕОМ через контакти USB- з'єднувача по ланцюгу +5В±10%.

1.4.5 Виріб може бути під'єднаний до USB-з'єднувача ЕОМ без вимкнення живлення та перезавантаження операційної системи.

1.4.6 Виріб може бути відімкнутий від USB-з'єднувача ЕОМ без вимкнення живлення та перезавантаження операційної системи.

1.5 Виріб не потребує додаткових засобів вимірювання, інструментів та приладь.

1.6 Маркування та пломбування

1.6.1 Маркування виробу складається з логотипу підприємства-виробника, умовної позначки "e.Ключ" та заводського номера 10xxxxx.

1.6.2 Маркування нанесене на корпусі виробу.

1.6.3 Захист від несанкціонованого доступу до внутрішніх вузлів виробу здійснюється за рахунок нерозбірної компаундної заливки.

1.7 Пакування

1.7.1 Виріб може бути упакований в індивідуальну або групову упаковку з прозорого пластику, яка виключає його пошкодження при зберіганні та транспортуванні, а також у групову упаковку з гофрованого картону відповідно до п.5 та 6 даної інструкції.

1.7.2 Вироби, які упакуванні у групову упаковку комплектуються одним носієм інформації з інсталяційним пакетом програм та одним комплектом експлуатаційних документів.

2 ВИКОРИСТАННЯ ЗА ПРИЗНАЧЕННЯМ

2.1 Експлуатаційні обмеження

Забороняється порушення цілісності корпусу та USB-з'єднувача при експлуатації виробу.

Увага: системний блок ЕОМ, до якої підключається ЕК, повинен бути заземлений.

Увага: у USB-з'єднувач виробу з відкритою кришкою не допускається потрапляння сторонніх предметів.

Виріб, під'єднаний до ЕОМ, призначений для експлуатації в приміщеннях з нормальними кліматичними умовами:

- температура навколишнього повітря (плюс 20+5) °С;
- відносна вологість навколишнього повітря (60 + 15)%;
- атмосферний тиск від 84 до 107 кПа (від 630 до 800 мм.рт.ст.).

У повітрі не допускається наявність пар кислот, лугів і інших агресивних домішок, що викликають корозію.

2.2 Дії в екстремальних умовах

Виріб, як електронний пристрій, не містить джерел виникнення екстремальних умов (пожежі, небезпечного випромінювання, тощо).

При необхідності швидкого знищення ключової інформації та даних користувача, які зберігаються у виробі, діяти відповідно до правил користування, які прийняті у системі, в якій використовується виріб.

2.3 Доопрацювання

Виріб не підлягає доопрацюванню.

2.4 Порядок роботи у ОС Microsoft Windows

2.4.1 Умови інсталяції програм

Драйвери та програмний комплекс конфігурування функціонують у ОС Microsoft Windows 2000/XP/2003 Server/Vista/ 2008 Server/7/8/8.1/10/2012 Server.

2.4.2 Драйвери пристрою

2.4.2.1 Призначення драйверів USB-пристрою

Драйвери пристрою призначені для:

- забезпечення коректного розпізнавання пристрою ОС ПЕОМ;
- передачі кодів команд та вхідних даних для виконання відповідних внутрішніх програм пристрою, які виконують перетворення вхідних даних у вихідні;
- отримання з пристрою результатів виконання команд та вихідних даних.

2.4.2.2 Інсталяція драйверів USB-пристрою

При першому підключенні пристрою диспетчер пристроїв ОС знайде новий пристрій і відкриє вікно майстра інсталяції драйвера пристрою (рис. 2.1). В даному вікні необхідно вибрати опцію “Выполнить поиск драйверов на этом компьютере ”.

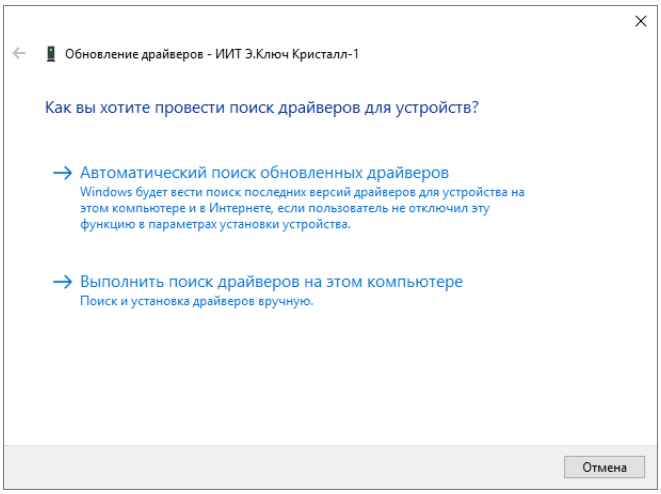


Рисунок 2.1

На наступній сторінці (рис. 2.2) необхідно натиснути кнопку “Обзор”. У вікні, що з’явилось (рис. 2.3), необхідно вказати шлях до папки, що містить файл EKeyCr1.inf, який входить до інсталяційного пакету програм пристрою, і натиснути кнопку “ОК”. На сторінці, зображеній на рис. 2.2, необхідно натиснути кнопку “Далее”.

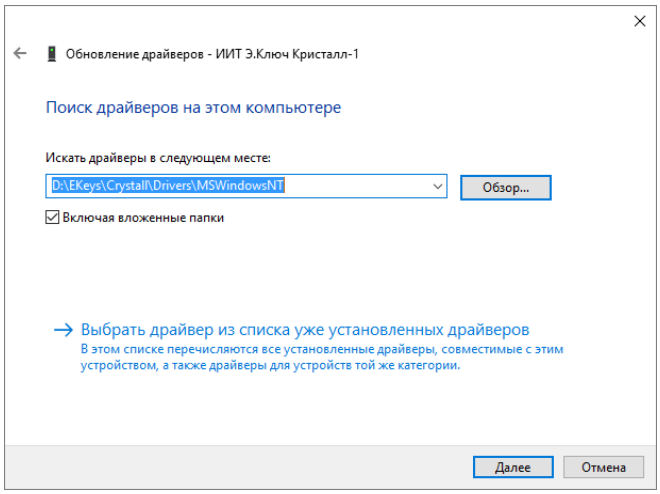


Рисунок 2.2

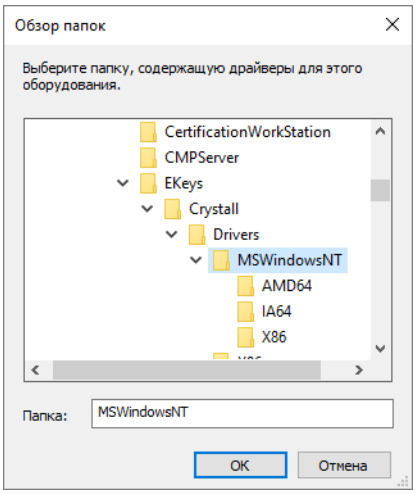


Рисунок 2.3

Після завершення інсталяції драйверу буде виведено останню сторінку майстра (рис. 2.5), на якій необхідно натиснути кнопку “Закрыть”.

Рисунок 2.5

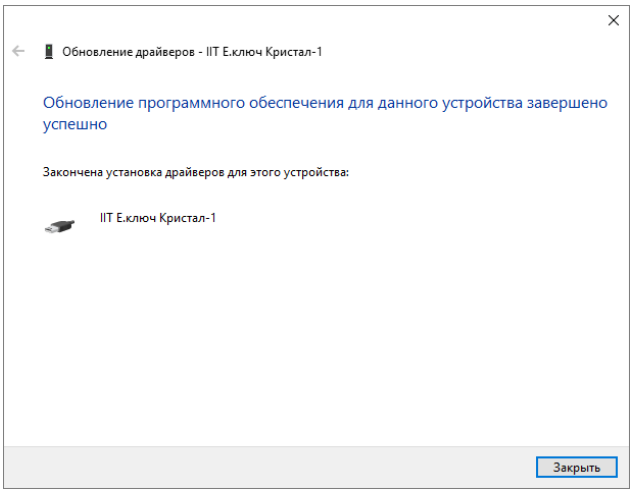


Рисунок 2.5

Після завершення інсталяції драйверу необхідно перевірити те, що драйвер пристрою було завантажено. Необхідно запустити диспетчер пристроїв ОС (рис. 2.6), розгорнути пункт “Контроллеры USB” та у списку пристроїв знайти пристрій “IIT E.Ключ Кристал-1”. Значок поряд з пристроєм повинен мати вигляд, наведений на рис. 2.6.

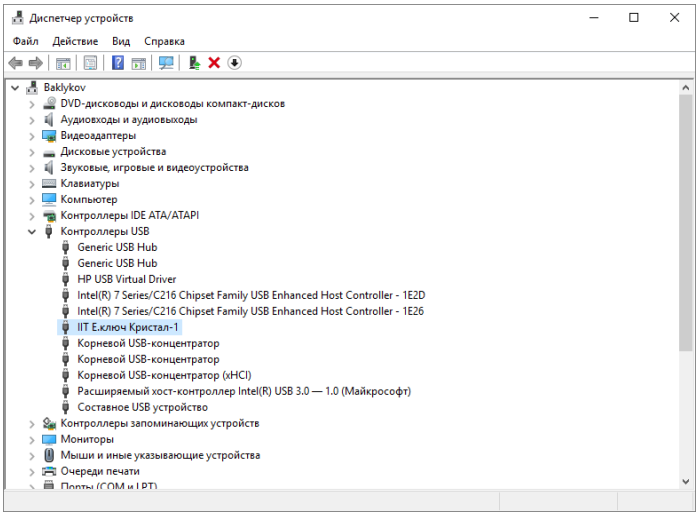


Рисунок 2.6

2.4.2.3 Призначення драйверів CCID-пристрою

Драйвери CCID-пристрою призначені для:

- забезпечення коректного розпізнавання пристрою ОС ПЕОМ;
- передачі кодів команд та вхідних даних для виконання відповідних внутрішніх програм пристрою, які виконують перетворення вхідних даних у вихідні;
- отримання з пристрою результатів виконання команд та вихідних даних.

Драйвери CCID-пристроїв, яким може бути ЕК, встановлені у ОС Microsoft Windows Vista/ 2008 Server/7/8/2012 Server за замовчанням. Якщо драйвер не встановлено (наприклад, для ОС Microsoft Windows 2000/XP/2003 Server), то його можна отримати з офіційного web-сайту компанії Microsoft http://microsoft.com чи за посиланням http://iit.com.ua/download/productfiles/MSWindowsXPCCIDDriver.rar.

2.4.2.4 Інсталяція драйверів CCID-пристрою

Якщо драйвер не встановлюється автоматично диспетчер пристроїв ОС знайде новий пристрій і відкриє вікно майстра інсталяції драйвера пристрою. В якості драйвера пристрою необхідно вказати файл usbccid.sys.

Після завершення інсталяції драйверу необхідно перевірити те, що драйвер пристрою було завантажено. Необхідно запустити диспетчер пристроїв ОС (рис. 2.7), розгорнути пункт “Устройство чтения смарт-карт” та у списку пристроїв знайти пристрій “Microsoft Usbccid Smartcard Reader (WUDF)”. Значок поряд з пристроєм повинен мати вигляд, наведений на рис. 2.7.

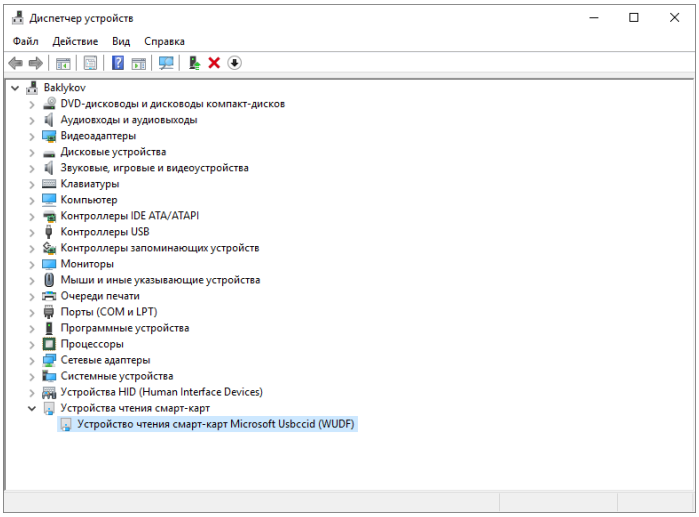


Рисунок 2.7

2.4.3 Програмний комплекс конфігурування

2.4.3.1 Призначення

Програмний комплекс конфігурування (далі - програма) призначений для встановлення параметрів електронного ключа і виконує наступні функції:

- технологічне тестування електронного ключа для перевірки працездатності при проведені технічного обслуговування;
- форматування електронного ключа;
- переведення в режим з розподілом ролей;
- зміну паролю(ів) доступу до електронного ключа;
- перегляд журналу реєстрації електронного ключа;
- ініціалізація електронного ключа в якості PKCS#11-пристрою.

2.4.3.2 Інсталяція

Для інсталяції програми необхідно запустити програму інсталяції (майстер інсталяції) EKeyCrystal1Install.exe з інсталяційного носія (оптичного диску чи ін.).

Після запуску програми інсталяції на першій сторінці (рис. 2.8) виводиться інформація про початок інсталяції. Для продовження інсталяції необхідно натиснути кнопку “Далі”, а для завершення - “Відміна”.

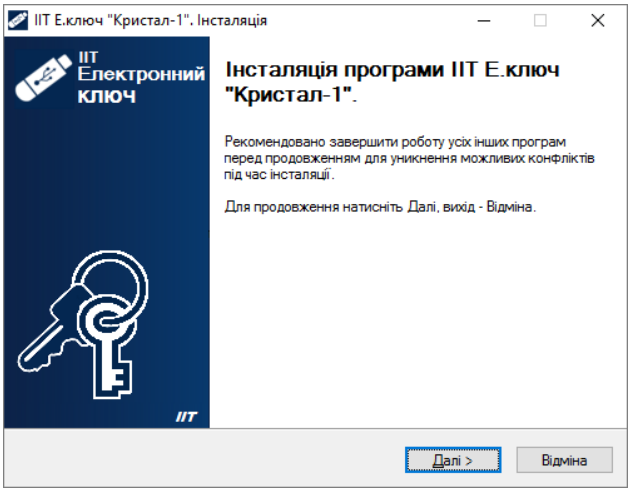


Рисунок 2.8

На наступній сторінці майстра (рис. 2.9) за необхідністю можна вказати каталог на диску до якого буде встановлено програму. Для продовження інсталяції необхідно натиснути кнопку “Далі”.

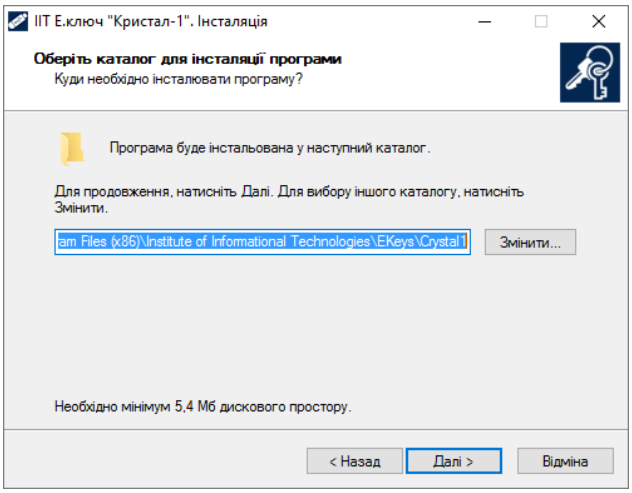


Рисунок 2.9

На наступній сторінці майстра (рис. 2.10) за необхідністю можна вказати розділ меню “Пуск” до якого буде встановлено значки запуску та деінсталяції програми. Для продовження інсталяції необхідно натиснути кнопку “Далі”.

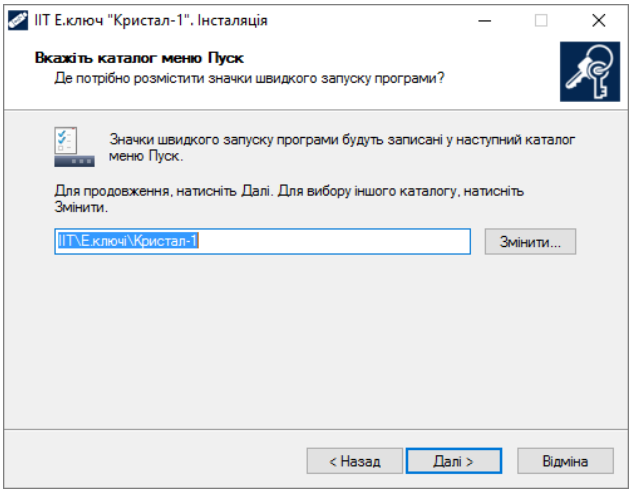


Рисунок 2.10

На наступній сторінці майстра (рис. 2.11) потрібно встановити признаки необхідності виконання майстром додаткових завдань – створення значку запуску програми на робочому столі та запуску програми після завершення інсталяції. Для продовження інсталяції необхідно натиснути кнопку “Далі”.

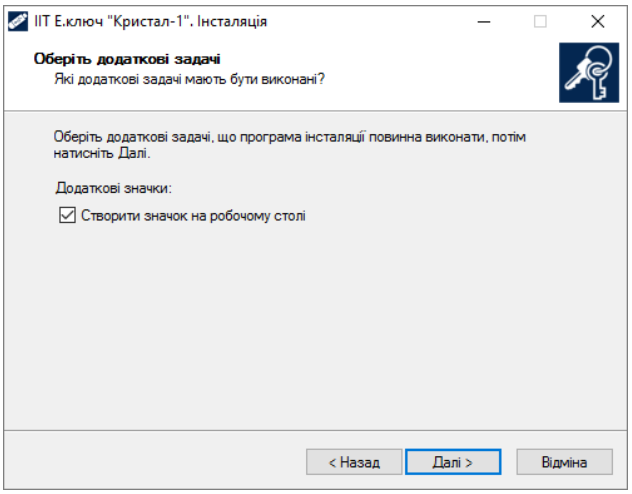


Рисунок 2.11

На наступній сторінці майстра (рис. 2.12) буде виведено інформацію про операції, що будуть виконані майстром. Для виконання інсталяції необхідно натиснути кнопку “Встановити”.

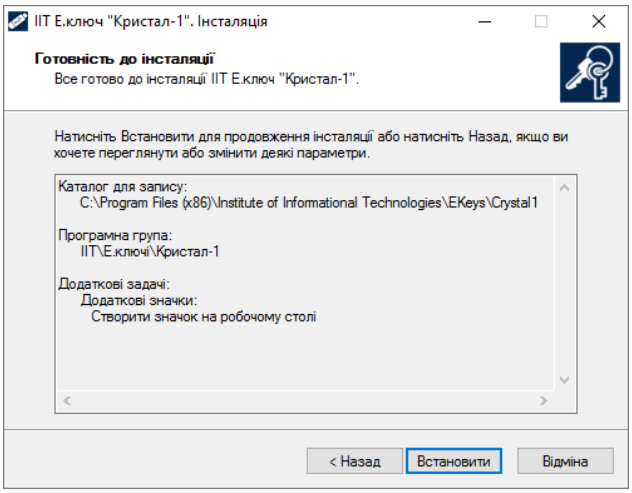


Рисунок 2.12

Після інсталяції програми, майстер завершує свою роботу (рис. 2.13).

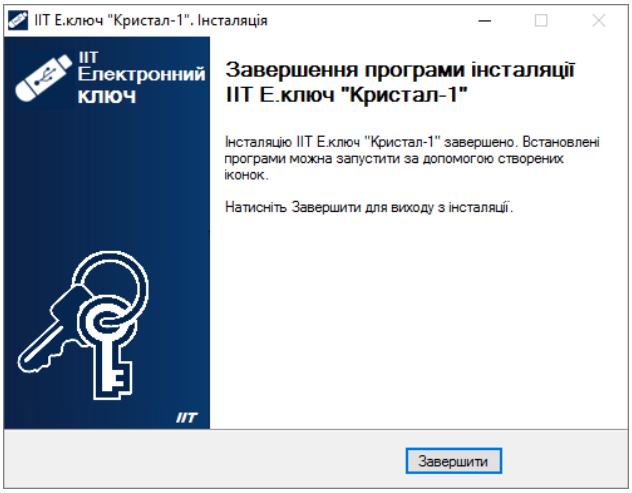


Рисунок 2.13

2.4.3.3 Порядок роботи

2.4.3.3.1 Завантаження програми

Для завантаження програми необхідно запустити модуль, що виконується EKeyCrystal1Cfg.exe через файловий менеджер ОС. Після запуску на екрані буде відображене вікно, що наведене на рис. 2.14.

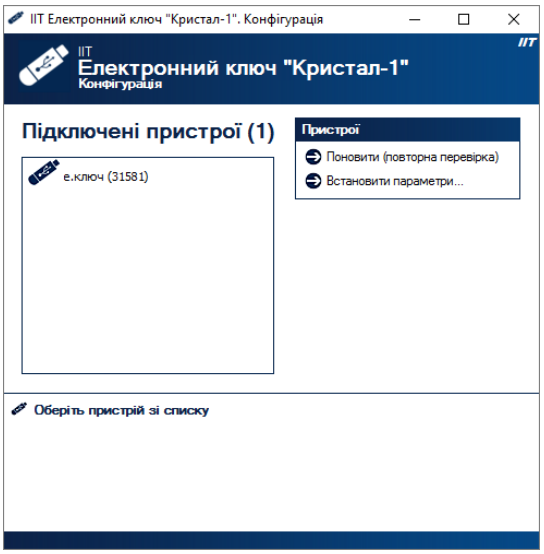


Рисунок 2.14

2.4.3.3.2 Параметри електронного ключа

У лівій панелі вікна відображається перелік підключених електронних ключів (пристроїв). Для роботи з електронним ключем необхідно обрати відповідний запис, як показано на рис. 2.15. У ніжній частині вікна буде виведено інформацію про параметри електронного ключа (пристрою).

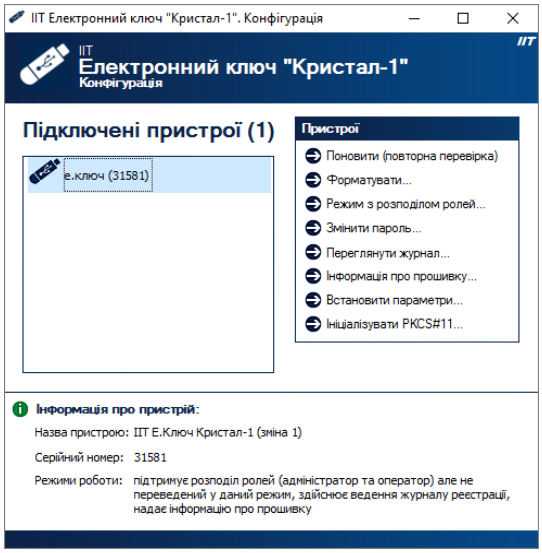


Рисунок 2.15

Для встановлення параметрів роботи пристрою необхідно натиснути посилання “Встановити параметри…”. Вікно із параметрами наведене на рис. 2.16.

У вікні параметрів встановлюються параметри протоколу розподілу ключів (необхідність використання попередніх обчислень), та параметри самотестування (необхідність виконання само тестування, та параметри алгоритму ЕЦП й протоколу розподілу ключів). Параметри само тестування впливають на швидкість роботи пристрою (при використанні самотестування), але підвищують надійність роботи.

Для збереження встановлених параметрів необхідно натиснути кнопку “Застосувати”.

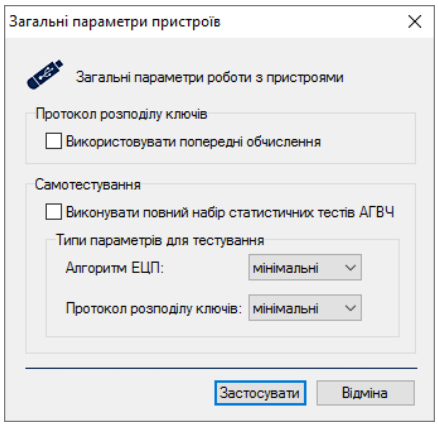


Рисунок 2.16

2.4.3.3.3 Форматування електронного ключа

Для здійснення форматування електронного ключа необхідно обрати потрібний пристрій та натиснути посилання “Форматувати”. Під час форматування вся інформація з електронного ключа знищується.

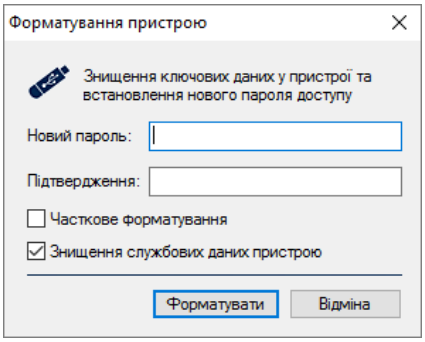


Рисунок 2.17

Після форматування необхідно задати новий пароль доступу до електронного ключа. Пароль задається у вікні що наведене на рис. 2.17.

При використанні параметру "Часткове форматування" дані історії попередніх особистих ключів протоколу розподілу ключів не будуть видалені.

Для знищення службових даних пристрою необхідно встановити опцію "Знищення службових даних пристрою". Під службовими даними розуміються дані, що доступні для запису та зчитування без участі користувача.

2.4.3.3.4 Переведення в режим з розподілом ролей

Режим з розподілом ролей надасть доступ до пристрою двом користувачам - адміністратору та оператору. Адміністратор та оператор матимуть різні повноваження.

Для переведення в режим з розподілом ролей необхідно обрати потрібний пристрій та натиснути посилання "Режим з розподілом ролей...". Перед початком зміни режиму буде виведено повідомлення оператору (рис. 2.18). Для продовження необхідно натиснути "Да", для відміни - "Нет".

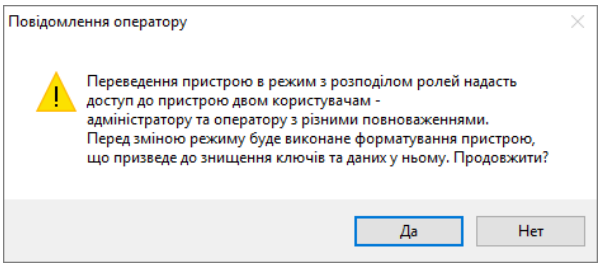


Рисунок 2.18

Вікно зі встановленням параметрів переведення в режим з розподілом ролей зображене на рис. 2.19

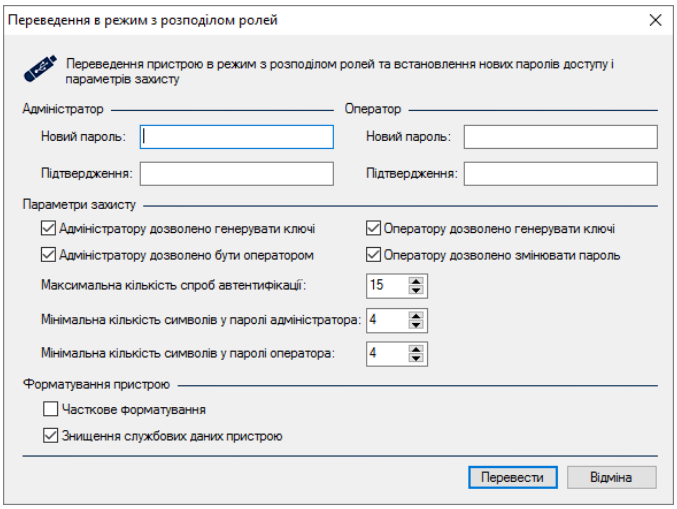


Рисунок 2.19

Для переведення пристрою необхідно вказати паролі для ролі "Адміністратор" та "Оператор", а також встановити параметри захисту для цих ролей та вказати параметри форматування пристрою. Паролі адміністратора та оператора неповинні співпадати.

Параметр "Максимальна кількість спроб автентифікації" визначає кількість спроб автентифікації адміністратором або оператором, після перевищення кількості спроб, пристрій буде заблоковано. Також під час встановлення параметрів надається можливість встановлення мінімальної кількості символів, яка повинна міститись у паролі адміністратора чи оператора.

Після встановлення необхідних параметрів, необхідно натиснути "Перевести". Після завершення переведення пристрою в режим з розподілом ролей головне вікно програми матиме вигляд, що зображене на рис. 2.20

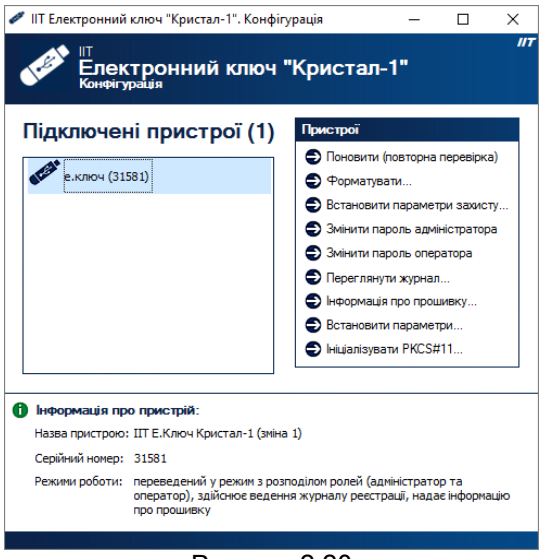


Рисунок 2.20

Примітка. Після переведення у режим з розподілом ролей повернення до звичайного режиму можливе лише після формування послідовності для виробника (п.2.4.3.4.5) та форматування пристрою паролем виробника (п.2.4.3.4.6).

2.4.3.3.5 Зміна паролю доступу до електронного ключа

Для здійснення зміни паролю доступу до електронного ключа необхідно обрати потрібний пристрій та натиснути посилання “Змінити пароль”.

Примітка. Якщо під час зміни паролю на електронному ключі знаходяться дані, що захищені в режимі використання пароля доступу до електронного ключа в якості пароля захисту даних (такий режим використовується в програмних комплексах ЦСК “ІІТ ЦСК-1” та користувача ЦСК “ІІТ Користувач ЦСК-1”), такі дані можуть бути недоступні для використання після зміни пароля. Для зміни пароля в такому разі необхідно використовувати зазначені програмні комплекси.

Вікно зміни паролю наведене на рис. 2.21. У вікні необхідно вказати старий пароль доступу та новий пароль із підтвердженням.

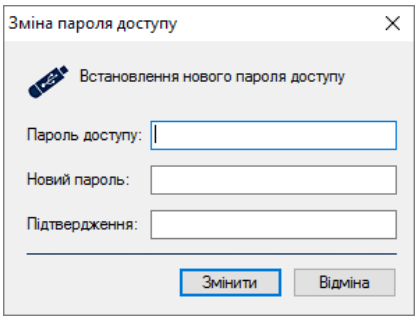


Рисунок 2.21

Примітка. Електронний ключ здійснює підрахунок кількості невдах спроб автентифікації (введене невірного пароля доступу). У випадку виконання 15 невдалих спроб автентифікації поспіль електронний ключ здійснює знищення даних та особистих ключів, які в ньому зберігаються, після чого можливе тільки його форматування. Якщо кількість невдалих спроб не перевищила 15 та виконана успішна автентифікація, лічильник невдалих спроб скидається в 0.

2.4.3.3.6 Параметри електронного ключа в режимі з розподілом ролей

У лівій панелі вікна відображається перелік підключених електронних ключів (пристроїв). Для роботи з електронним ключем необхідно обрати відповідний запис, як показано на рис. 2.22. У ніжній частині вікна буде виведено інформацію про параметри електронного ключа (пристрою).

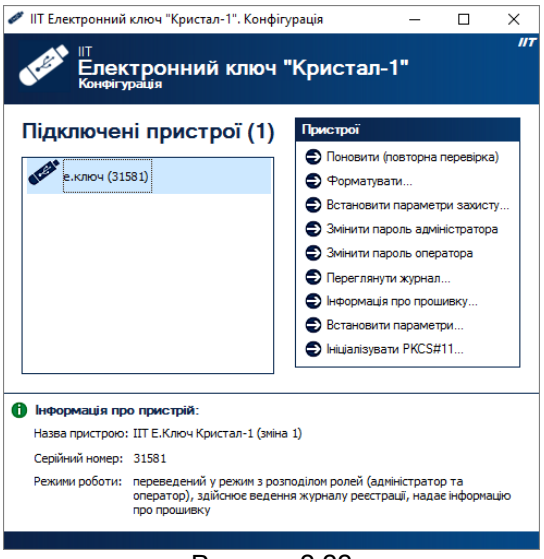


Рисунок 2.22

2.4.3.3.7 Параметри захисту пристрою в режимі з розподілом ролей

Для встановлення параметрів захисту пристрою у режимі з розподілом ролей необхідно обрати потрібний пристрій та натиснути посилання "Встановити параметри захисту". Вікно з параметрами захисту відображене на рис. 2.23.

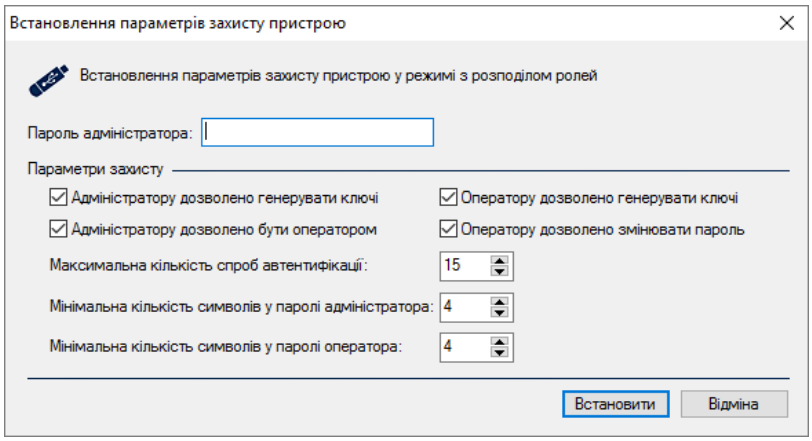


Рисунок 2.23

Для встановлення параметрів необхідно ввести пароль "Адміністратора", а також встановити параметри захисту для ролі "Адміністратор" та "Оператор".

Параметр "Максимальна кількість спроб автентифікації" визначає кількість спроб автентифікації адміністратором або оператором, після перевищення кількості спроб, пристрій буде заблоковано. Також під час встановлення параметрів надається можливість встановлення мінімальної кількості символів, яка повинна міститись у паролі адміністратора чи оператора.

Після встановлення необхідних параметрів, слід натиснути "Встановити".

2.4.3.3.8 Зміна паролю адміністратора в режимі з розподілом ролей

Примітка. Зміна пароля доступу до пристрою може призвести до втрати даних у ньому. За можливістю, необхідно проводити зміну паролю за допомогою прикладної програми (наприклад ІІТ Користувач ЦСК-1, тощо).

Для зміни паролю доступу до електронного ключа необхідно обрати потрібний пристрій та натиснути посилання “Змінити пароль адміністратора”.

Вікно зміни паролю наведене на рис. 2.24. У вікні необхідно вказати старий пароль доступу та новий пароль із підтвердженням.

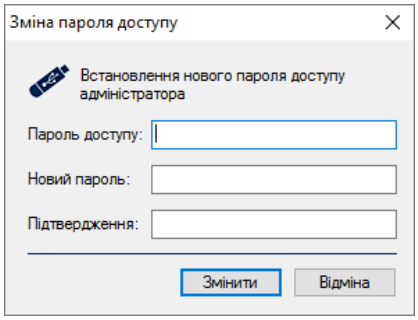


Рисунок 2.24

2.4.3.3.9 Зміна паролю оператора в режимі з розподілом ролей

Примітка. Зміна пароля доступу до пристрою може призвести до втрати даних у ньому. За можливістю, необхідно проводити зміну паролю за допомогою прикладної програми (наприклад IIT Користувач ЦСК-1, тощо).

Для здійснення зміни паролю доступу до електронного ключа необхідно обрати потрібний пристрій та натиснути посилання “Змінити пароль оператора”.

Вікно зміни паролю наведене на рис. 2.25. У вікні необхідно вказати старий пароль доступу та новий пароль із підтвердженням.

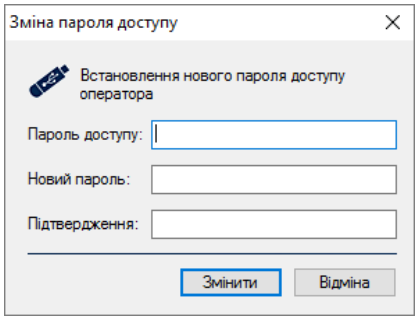


Рисунок 2.25

2.4.3.3.10 Формування послідовності для виробника в режимі з розподілом ролей

Примітка. Формування послідовності для виробника необхідне у разі якщо пристрій було заблоковано або необхідно перевести електронний ключ у звичайний режим без розподілу ролей.

Для формування послідовності для виробника необхідно обрати потрібний пристрій та натиснути пункт випадаючого меню "Сформувати послідовність для виробника …". Вікно із випадковою послідовністю наведене на рис. 2.26.

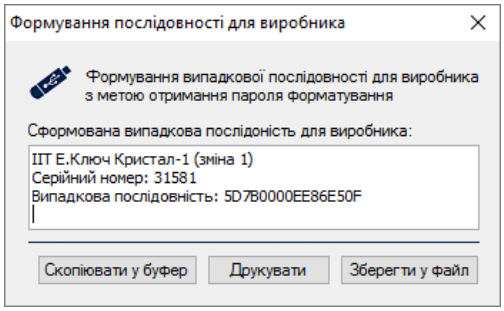


Рисунок 2.26

Сформовану послідовність можливо "Скопіювати у буфер", "Роздрукувати" та "Зберегти у файл".

Сформовану послідовність необхідно передати виробникові електронного ключа для отримання паролю для форматування.

2.4.3.3.11 Форматування паролем виробника в режимі з розподілом ролей

Примітка. Форматування паролем виробника можливе лише після відправки випадкової послідовності виробникові та отримання від виробника паролю для форматування.

Для форматування паролем виробника необхідно обрати потрібний пристрій та натиснути пункт випадаючого меню "Форматувати паролем виробника". Вікно із форматування пристрою паролем виробника наведене на рис. 2.27.

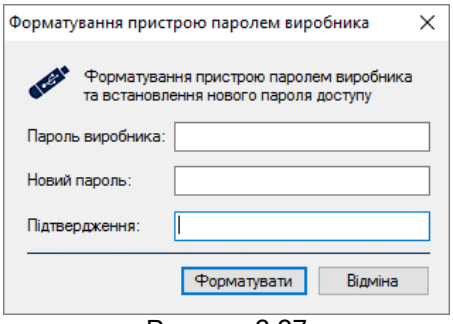


Рисунок 2.27

Для форматування пристрою необхідно вказати паролю отриманий від виробника та ввести новий паролю доступу із підтвердженням.

Після форматування пристрою паролем виробника, пристрій буде переведено до звичайного режиму без розподілу ролей. В разі необхідності пристрій можливо повторно перевести до режиму з розподілом ролей.

2.4.3.3.12 Перегляд журналу реєстрації подій

Для перегляду журналу реєстрації подій необхідно обрати потрібний пристрій та натиснути посилання "Переглянути журнал". Вікно із інформацією про події зображене на рис. 2.28.

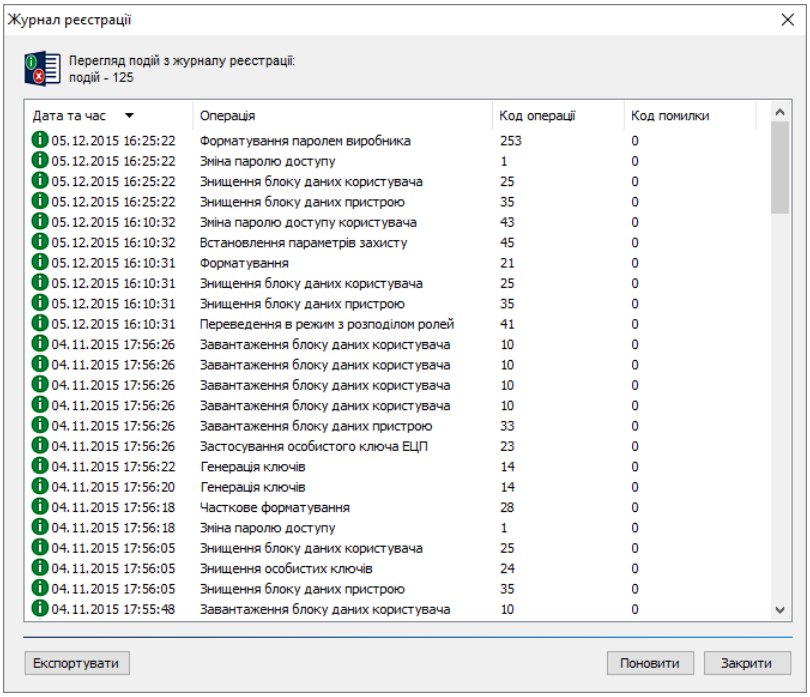


Рисунок 2.28

Для збереження подій до файлу необхідно натиснути "Експортувати".

2.4.3.3.13 Ініціалізація електронного ключа в якості PKCS#11-пристрою

Для здійснення ініціалізації електронного ключа в якості PKCS#11-сумісного пристрою необхідно обрати підключений пристрій та натиснути посилання “Ініціалізувати PKCS#11...”. Під час ініціалізації електронного ключа в якості PKCS#11-пристрою здійснюється його форматування та запис службових даних.

Вікно ініціалізації PKCS#11-пристрою наведене на рис. 2.29. Якщо електронний ключ не переведений у режим з розподілом ролей, то під час ініціалізації переведення у цей режим буде здійснене автоматично. Для цього у вікні необхідно вказати нові паролі доступу адміністратора та оператора із підтвердженнями.

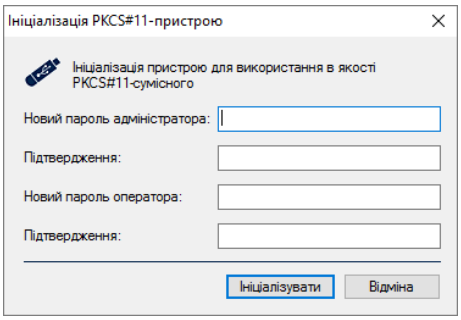


Рисунок 2.29

Якщо ініціалізація вже була виконана раніше, то буде виведене відповідне повідомлення щодо повторної ініціалізації.

У випадку успішної ініціалізації PKCS#11-пристрою буде виведене відповідне повідомлення, яке містить і інформацію про встановлення нових паролів доступу адміністратора та оператора, встановлених параметрів захисту електронного ключа та об'єму вільної пам'яті на пристрої (рис. 2.30).

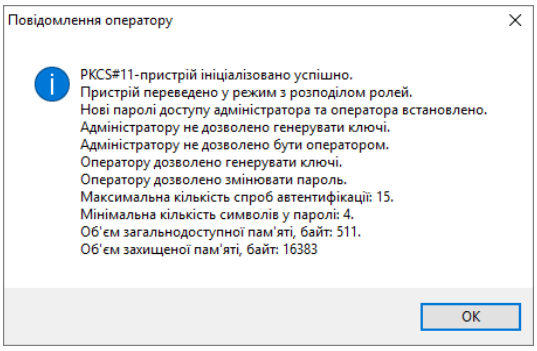


Рисунок 2.30

2.4.3.3.14 Перегляд інформації про прошивку

Для перегляду інформації про прошивку необхідно обрати потрібний пристрій та натиснути посилання "Інформація про прошивку". Вікно із інформацією про прошивку наведене на рис. 2.31.

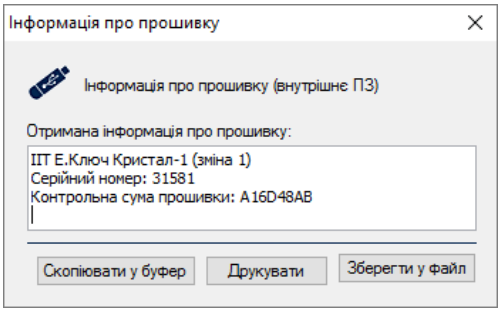


Рисунок 2.31

2.5 Порядок роботи в ОС Linux

2.5.1 Умови інсталяції програм

Програма функціонує у ОС Linux з ядром версії 2.6 (наявність системної бібліотеки роботи з USB-пристроями libusb.so) та вище. Під час роботи програма використовує власну бібліотеку роботи з USB-пристроєм (ekc1.so) чи CCID-пристроєм (ekc1ccid.so).

Для роботи CCID-пристрою у ОС сімейства Linux необхідно встановити пакет взаємодії з CCID-пристроями PCSC-Light (пакети pcsc та libccid з web-сайту http://pcsclite.alioth.debian.org/).

Також інформація про CCID-пристрій повинна бути внесена до файлу /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist (/etc/libccid_Info.plist чи ін.). Ім'я файлу та розташування можуть відрізнятись в залежності від ОС.

В кінець підрозділу ifdVenforID необхідно додати запис

<string>0x03EB</string>

В кінець підрозділу ifdProductID необхідно додати запис

<string>0x9308</string>

В кінець підрозділу ifdFriendlyName необхідно додати запис

<string>IIT E.Key Crystal-1</string>

Внести інформацію про CCID-пристрій до відповідних файлів також можна шляхом виконання командного скрипту ekc1.register.sh з інсталяційного архіву ekc1i.tar. Для інсталяції програми конфігурування пристрою необхідно розпакувати архів ekc1i.tar до будь-якого каталогу файлової системи.

2.5.2 Порядок роботи з програмами

Для завантаження програми конфігурування необхідно запустити модуль, що виконується ekc1dc через файловий менеджер ОС. Після запуску на екрані буде відображено перелік команд, які підтримує програма.

ekc1c: Command line parameters next

Enum attached ekeys : enum

Format ekey : format <SN> <Password>

Change ekey password : changepassword <SN> <OldPassword> <NewPassword>

Check ekey : check <SN> <Password>

EKey SN format - 00000..99999

EKey password length - 1..31 symbols

2.5.2.1 Перелічення встановлений електронних ключів

Для отримання переліку встановлених електронних ключів необхідно запустити програму із наступними аргументами командної строки:

ekc1c enum.

При цьому на екрані буде відображено список встановлених (підключених) електронних ключів із зазначенням їх серійних номерів. Серійний номер має діапазон 00000..99999 (наприклад, 00001).

2.5.2.2 Форматування електронного ключа

Для здійснення форматування електронного ключа необхідно запустити програму із наступними аргументами командної строки:

ekc1c format <SN> <Password>,

де <SN> - серійний номер пристрою, а <Password> - пароль доступу.

Під час форматування вся інформація з електронного ключа знищується та встановлюється новий пароль доступу до електронного ключа.

2.5.2.3 Зміна паролю доступу до електронного ключа

Для виконання зміни пароля доступу до електронного ключа необхідно запустити програму із наступними аргументами командної строки:

ekc1c changepassword <SN> <OldPassword> <NewPassword>,

де <SN> - серійний номер пристрою, а <OldPassword> та <NewPassword> - відповідно старий та новий паролі доступу.

2.5.2.4 Тестування електронного ключа

Для виконання тестування (перевірки роботоспроможності) електронного ключа необхідно запустити програму із наступними аргументами командної строки:

ekc1c check <SN> <Password>,

де <SN> - серійний номер пристрою, а <Password> - пароль доступу.

Під час тестування здійснюється самотестування електронного ключа та перевірка пароля доступу до нього.

3 ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ

3.1 Технічне обслуговування виробу здійснюється разом з ЕОМ, сумісно з якою він використовується.

3.2. Виріб не має індивідуальних особливостей технічного обслуговування.

3.3 Перевірка роботосроможності виробу здійснюється за допомогою програмного комплексу тестування та конфігурування, який знаходиться на носієві інформації з комплекту поставки виробу. Порядок перевірки наведений у п.п. 2.4.3.

4 ПОТОЧНИЙ РЕМОНТ

4.1 Виріб не підлягає ремонту.

4.2 Працездатність системи, у якій використовується виріб, відновлюється шляхом заміни виробу.

5 ЗБЕРІГАННЯ

5.1 Виріб в упакованому для транспортування виді зберігає зовнішній вигляд і працездатність після впливу наступних кліматичних факторів з наступною шестигодинною витримкою в нормальних кліматичних умовах:

- температура навколишнього повітря від мінус 40^0С до плюс 60 °С;
- відносна вологість навколишнього повітря до 98% при плюс 25°С;
- атмосферний тиск від 60 до 107 кПа (від 450 до 800 мм.рт.ст.).

5.2 Гарантійний термін зберігання 1 рік.

6 ТРАНСПОРТУВАННЯ

6.1 Виріб повен транспортуватися у пакуванні підприємства-виробника.

6.2 В упакованому виді виріб може транспортуватися під впливом наступних кліматичних та механічних факторів:

- температура навколишнього повітря від мінус 40^0С до плюс 60 °С;
- відносна вологість навколишнього повітря до 98% при плюс 25°С;
- атмосферний тиск від 60 до 107 кПа (від 450 до 800 мм.рт.ст.);
- пікове ударне прискорення 29.5 м/с^2 (3g) при частоті проходження ударів від 80 до 120 за хвилину, число ударів не менше 2000, тривалість дії імпульсу ударного прискорення 5-10 мс.

7 УТИЛІЗАЦІЯ

7.1 Перед утилізацією пристрою повинне бути виконане знищення особистих ключів та даних, які зберігаються у пристрої.