ДКПП 30.02.16.000

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖЕНИЙ
ЄААД.469535.153-ЛУ

АТ ІІТ
Апаратні засоби КЗІ

Електронний ключ “Алмаз-1К”

Настанова з експлуатації

ЄААД.469535.153 РЭ

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

Харків 2018 р.

ЗМІСТ

ВВЕДЕННЯ

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

Шифр виробу: “ІІТ Електронний ключ Алмаз-1К”.

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 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(ширина)х(висота), мм, не більше	52 х 17 х 9
Маса, кг, не більше	0,010
Споживана потужність від блоку електроживлення ЕОМ +5В±10%., Вт, не більше:	0,5

1.3 Склад виробу

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.

1.4.2 Конструктивно ЕК виконаний на двошаровій друкованій платі, яка залита компаундом, що формує захисний шар та встановлена в пластмасовий чи металевий 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 умовної позначки "Almaz" та заводського номера з шести цифр.

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 пакується у чохол з прозорої поліетиленової плівки, до якого вкладається паспорт, поєднаний з етикеткою, яка видна знизу пакування та захищена плівкою.

1.7.2 У разі поставки партії ЕК, усі вироби, які входять до складу партії пакуються згідно 1.7.1 та складаються у ящик з гофрованого картону. До цього ящика вкладаються один носій інформації з інсталяційним пакетом програм ЄААД.00153-01 97 01-1та один екземпляр настанови з експлуатації ЄААД.469535.153 РЭ.

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/7/8/2012 Server.

Пристрій використовує стандартний драйвер ОС Microsoft Windows usbccid.sys.

2.4.2 Драйвери пристрою

2.4.2.1 Призначення

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.

Драйвери CCID-пристроїв, яким є 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.

2.4.2.2 Інсталяція

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. 2.1), розгорнути пункт "Smart card readers" та у списку пристроїв знайти пристрій "Microsoft Usbccid Smartcard Reader (WUDF)". Значок поряд з пристроєм повинен мати вигляд, наведений на рис. 2.1.

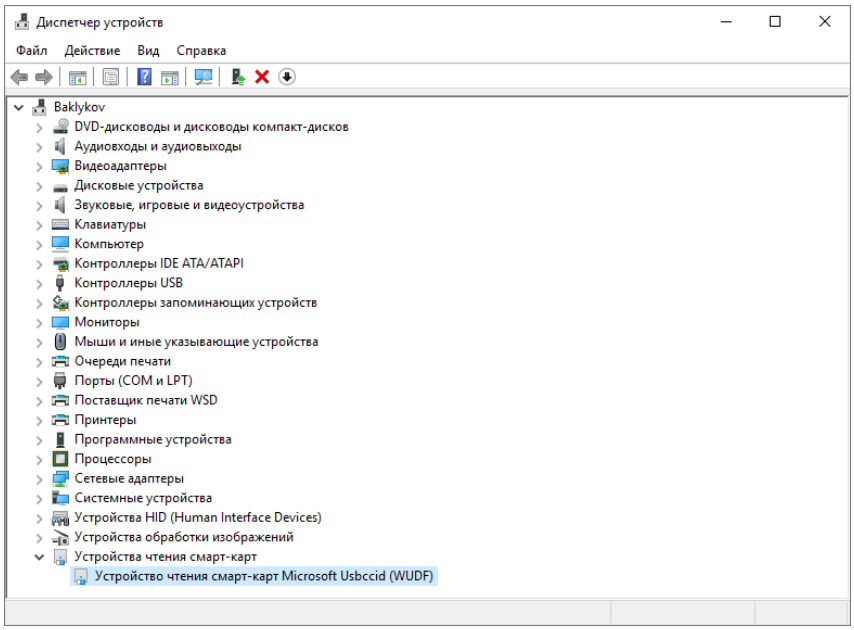

Рисунок 2.1

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;
- зміну паролю доступу до електронного ключа;
- ініціалізація електронного ключа в якості PKCS#11-пристрою.

2.4.3.2 Інсталяція

Для інсталяції програми необхідно запустити програму інсталяції (майстер інсталяції) EKAlmaz1CInstall.exe з інсталяційного носія (оптичного диску чи ін.).

Після запуску програми інсталяції на першій сторінці (рис. 2.2) виводиться інформація про початок інсталяції. Для продовження інсталяції необхідно натиснути кнопку “Далі”, а для завершення - “Відміна”.

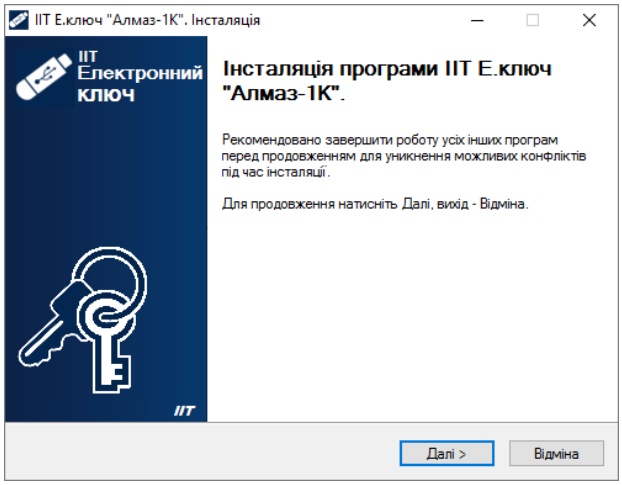

Рисунок 2.2

На наступній сторінці майстра (рис. 2.3) за необхідністю можна вказати каталог на диску до якого буде встановлено програму. Для продовження інсталяції необхідно натиснути кнопку “Далі”.

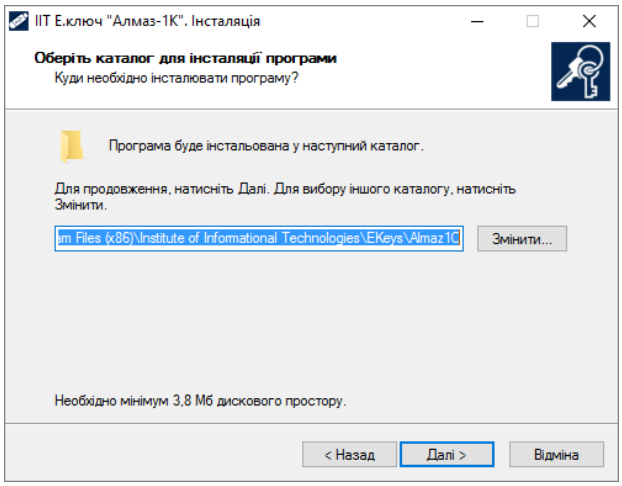

Рисунок 2.3

На наступній сторінці майстра (рис. 2.4) за необхідністю можна вказати розділ меню “Пуск” до якого буде встановлено значки запуску та деінсталяції програми. Для продовження інсталяції необхідно натиснути кнопку “Далі”.

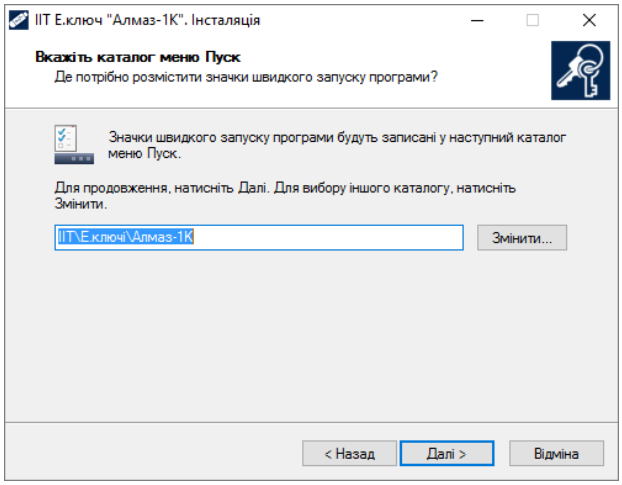

Рисунок 2.4

На наступній сторінці майстра (рис. 2.5) 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”.

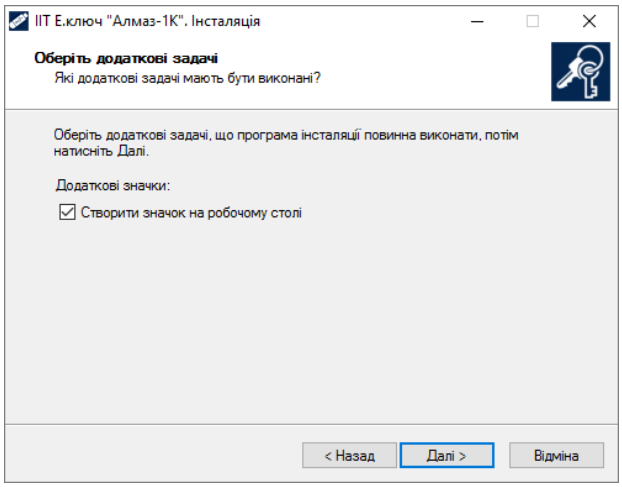

Рисунок 2.5

На наступній сторінці майстра (рис. 2.6) буде виведено інформацію про операції, що будуть виконані майстром. Для виконання інсталяції необхідно натиснути кнопку “Встановити”.

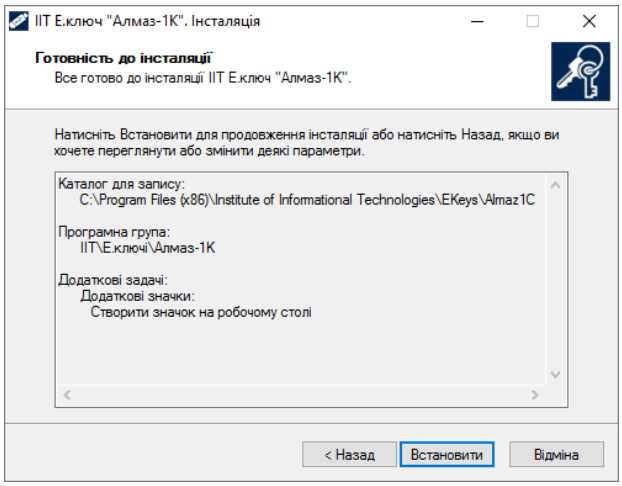

Рисунок 2.6

Після інсталяції програми, майстер завершує свою роботу (рис. 2.7).

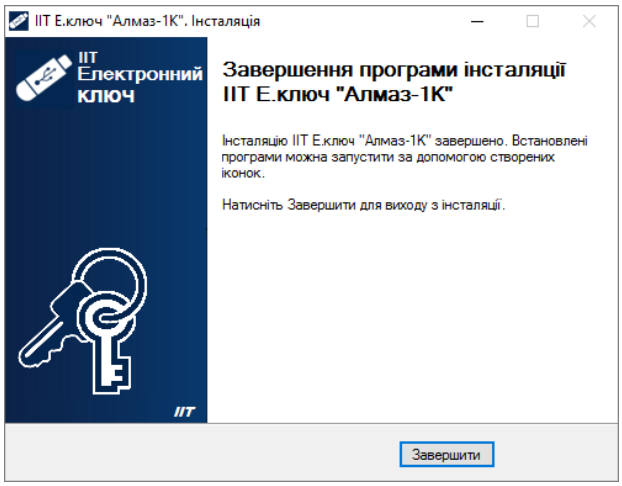

Рисунок 2.7

2.4.3.3 Порядок роботи

2.4.3.3.1 Завантаження програми

Для завантаження програми необхідно запустити модуль, що виконується EKeyCrystal1CConfiguration.exe через файловий менеджер ОС. Після запуску на екрані буде відображене вікно, що наведене на рис. 2.8.

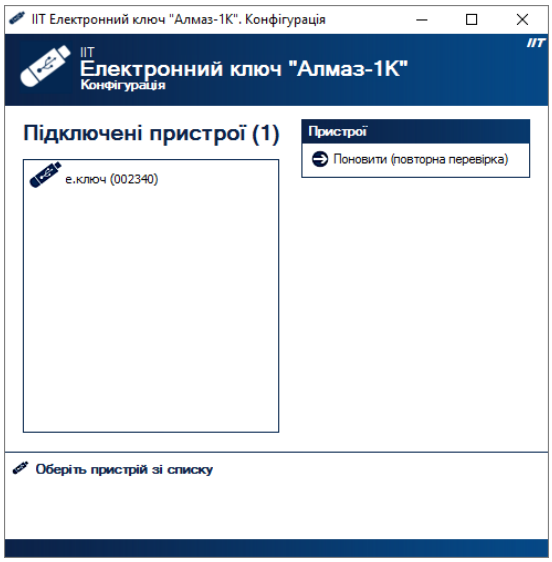

Рисунок 2.8

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. 2.9. У ніжній частині вікна буде виведено інформацію про параметри електронного ключа (пристрою).

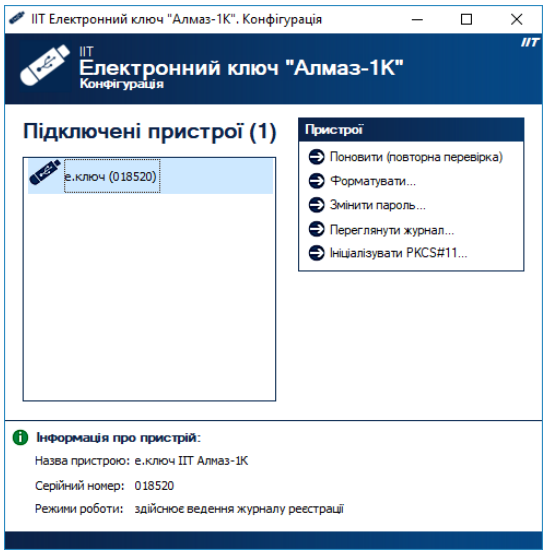

Рисунок 2.9

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.

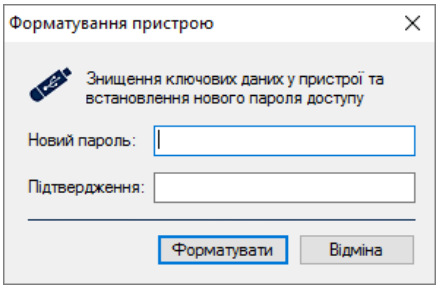

Рисунок 2.10

Після форматування необхідно задати новий пароль доступу до електронного ключа. Пароль задається у вікні що наведене на рис. 2.10.

2.4.3.3.4 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. 2.11. У вікні необхідно вказати старий пароль доступу та новий пароль із підтвердженням.

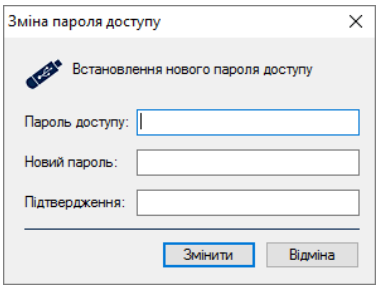

Рисунок 2.11

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.

2.4.3.3.5 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. 2.12.

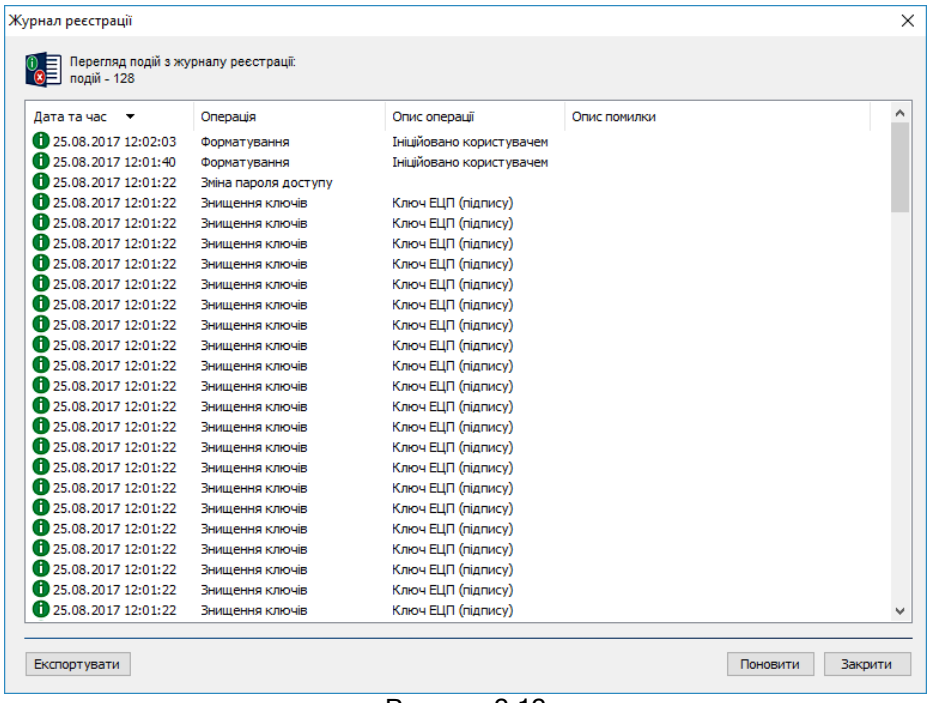

Рисунок 2.12

Для збереження подій до файлу необхідно натиснути "Експортувати". Опис операції форматування “Ініційовано пристроєм” означає, що було перевищено кількість можливих неуспішних уведень паролю доступу до пристрою і пристрій виконав знищення даних (форматування).

2.4.3.3.6 Перегляд інформації про пристрій

Для перегляду інформації про пристрій необхідно обрати потрібний пристрій та натиснути посилання "Інформація про пристрій". Вікно із інформацією про пристрій наведене на рис. 2.13.

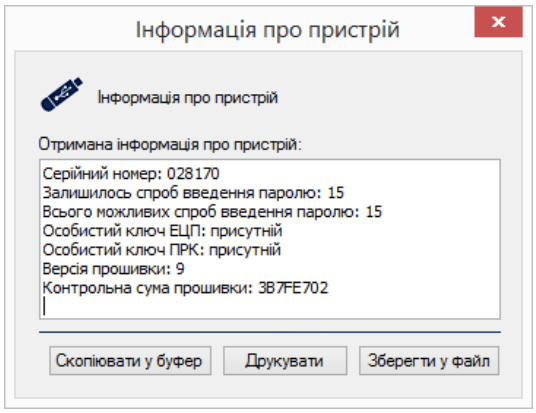

Рисунок 2.13

До складу інформації про пристрій входить інформація про кількість спроб введення паролю доступу до пристрою, що залишилися до знищення даних (форматування) пристрою. Якщо особисті ключі не присутні у пристрої, це може означати, що знищення даних (форматування) пристрою вже виконане і отримане значення кількості спроб введення паролю вже не має значення.

Отриману інформацію можливо "Скопіювати у буфер", "Роздрукувати" та "Зберегти у файл".

2.4.3.3.7 Ініціалізація електронного ключа в якості PKCS#11-пристрою

Для здійснення ініціалізації електронного ключа в якості PKCS#11-сумісного пристрою необхідно обрати потрібний 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. 2.14. У вікні необхідно вказати новий пароль доступу із підтвердженням.

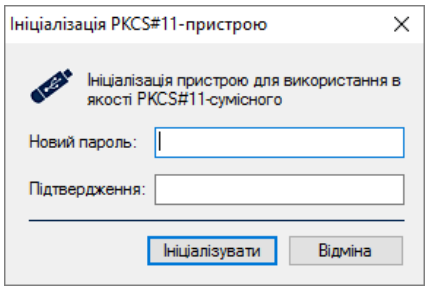

Рисунок 2.14

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 нового пароля доступу та об'єм вільної пам'яті на пристрої (рис. 2.15).

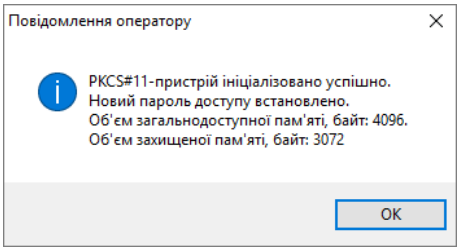

Рисунок 2.15

2.5 Порядок роботи у ОС Linux

2.5.1 Умови інсталяції програм

Бібліотеки та програмні компоненти конфігурування функціонують у ОС сімейства Linux.

Для роботи в 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>0x9324</string>

В кінець підрозділу ifdFriendlyName необхідно додати запис

<string>IIT E.Key Almaz-1C</string>

Внести інформацію про CCID-пристрій до відповідних файлів також можна шляхом виконання командного скрипту eka1c.register.sh з інсталяційного архіву eka1ci.tar. Для інсталяції програми конфігурування пристрою необхідно розпакувати архів eka1ci.tar до будь-якого каталогу файлової системи.

2.5.2 Порядок роботи з програмами

Для завантаження програми конфігурування необхідно запустити модуль, що виконується eka1cc через файловий менеджер ОС. Після запуску на екрані буде відображено наступні дані:

EKey Almaz-1C Configuration: Bad command line parameters

EKey Almaz-1C Configuration: Command line parameters next

Enum attached ekeys:	enum
Format ekey:	format <SN> <Password>
Change ekey password:	changepassword <SN> <OldPassword> <NewPassword>
Chek ekey:	check <SN> <Password>

EKey SN format – 000000..999999

EKey password length – 1..31 symbols

2.5.2.1 Перелік доступних електронних ключів

Для здійснення перегляду доступних електронних ключів необхідно запустити програму із наступними аргументами командної строки

eka1cc enum

Результатом виконання команди буде виведений перелік електронних ключів що доступні у ОС.

2.5.2.2 Форматування електронного ключа

Для здійснення форматування електронного ключа необхідно набрати команду

eka1cc format <SN> <Password>,

де <SN> <Password> відповідно серійний номер та пароль доступу до пристрою.

2.5.2.3 Зміна паролю доступу до електронного ключа

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

eka1cc changepassword <SN> <OldPassword> <NewPassword>,

де <SN> <OldPassword> <NewPassword> відповідно серійний номер, старий пароль доступу до пристрою та новий пароль доступу до пристрою.

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.

2.5.2.4 Перевірка роботи електронного ключа

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

eka1cc check <SN> <Password>,

де <SN> <Password> відповідно серійний номер та пароль доступу до пристрою.

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 роботопроможності виробу здійснюється за допомогою програмного комплексу користувача ЦСК ("ІІТ. Користувач ЦСК-1"). Порядок перевірки складається з генерації особистого ключа на пристрій та наступного зчитування цього особистого ключа.

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.