



**«Центр генерації ключів» зі складу
«Комплексу програмного
криптографічного захисту інформації
«QUANT»**

Настанова оператора
Версія 1/2018

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ	3
ВСТУП	4
СКЛАДОВІ КОМПОНЕТИ ЗАСОБУ	4
МІНІМАЛЬНІ ТЕХНІЧНІ ВИМОГИ	4
СУМІСНІСТЬ З ОПЕРАЦІЙНИМИ СИСТЕМАМИ	4
ВСТАНОВЛЕННЯ ЦГК	5
РОБОТА З ЦГК	7
Формування кореневого ключа (ключових даних) ЦГК	7
Робота з анкетами (профайлами) користувачів	11
Формування ключових даних та сертифікатів відкритих ключів за даними наперед сформованих анкет (профайлів)	20
Введення ключових документів в дію (активація)	31
Скасування / блокування сертифікатів відкритих ключів та ключових даних	34
Формування (випуск) списку відкликаних сертифікатів	44
Обробка запиту на сертифікат	47
Формування запиту на сертифікацію в АЦСК	51
Формування ключових даних сумісних із модулями «QUANT»	52

Пор. № зміни	Підпис відпов. особи	Дата внесення

ПЕРЕЛІК СКОРОЧЕНЬ

ЕОМ	Електронна обчислювальна машина
ЦГК	«Центр генерації ключів» зі складу «Комплексу програмного криптографічного захисту інформації «QUANT»
ОС	Операційна система
ДКЕ	Довгостроковий ключовий елемент
АЦСК	Акредитований центр сертифікації ключів

Пор. № зміни	Підпис відпов. особи	Дата внесення

ВСТУП

«Центр генерації ключів» зі складу «Комплексу програмного криптографічного захисту інформації «QUANT» (далі – ЦГК) призначений для забезпечення управління ключовими даними та ключовими документами, а саме формування ключових даних та ключових документів користувачів, адміністраторів, шлюзів, формування сертифікатів відкритих ключів ключових даних користувачів, адміністраторів, шлюзів, управління статусом ключових даних та сертифікатів відкритих ключів ключових даних, формування списків відкликаних сертифікатів.

Документ містить опис дій адміністратора безпеки (користувача), щодо постачання ключових даних та управління їх статусом.

Даний документ містить опис послідовності дій адміністратора безпеки стосовно розгортання, налаштування та використання ЦГК.

СКЛАДОВІ КОМПОНЕТИ ЗАСОБУ

ЦГК складається з наступних компонентів:

ЕТАЛОННІ ФАЙЛИ	
CGK.bin	Контроль цілісності ЦГК
CGK.exe	ЦГК
UACrypto.dll	Бібліотека криптографічних функцій
ФАЙЛИ КОРИСТУВАЧ ЦГК	
database_file.db	База даних ЦГК
CGK.ini	Файл налаштування ЦГК

МІНІМАЛЬНІ ТЕХНІЧНІ ВИМОГИ

Центральний процесор: Intel® Pentium® III 800Mhz

Графічний адаптер: в наявності

Оперативна пам'ять: 512 Mb

Вільне місце на жорсткому диску: 300 Mb

Мережева карта: 10 Мбіт/с (у разі роботи із системою управління)

Примітка: Зазначені технічні вимоги є мінімально необхідними для функціонування ЦГК.

СУМІСНІСТЬ З ОПЕРАЦІЙНИМИ СИСТЕМАМИ

32- бітні ОС: Microsoft® Windows® XP/2003/7/8/8.1/2008/10

64-бітні ОС: Microsoft® Windows® XP/2003/7/8/8.1/2008 R2/2012/2012 R2/10

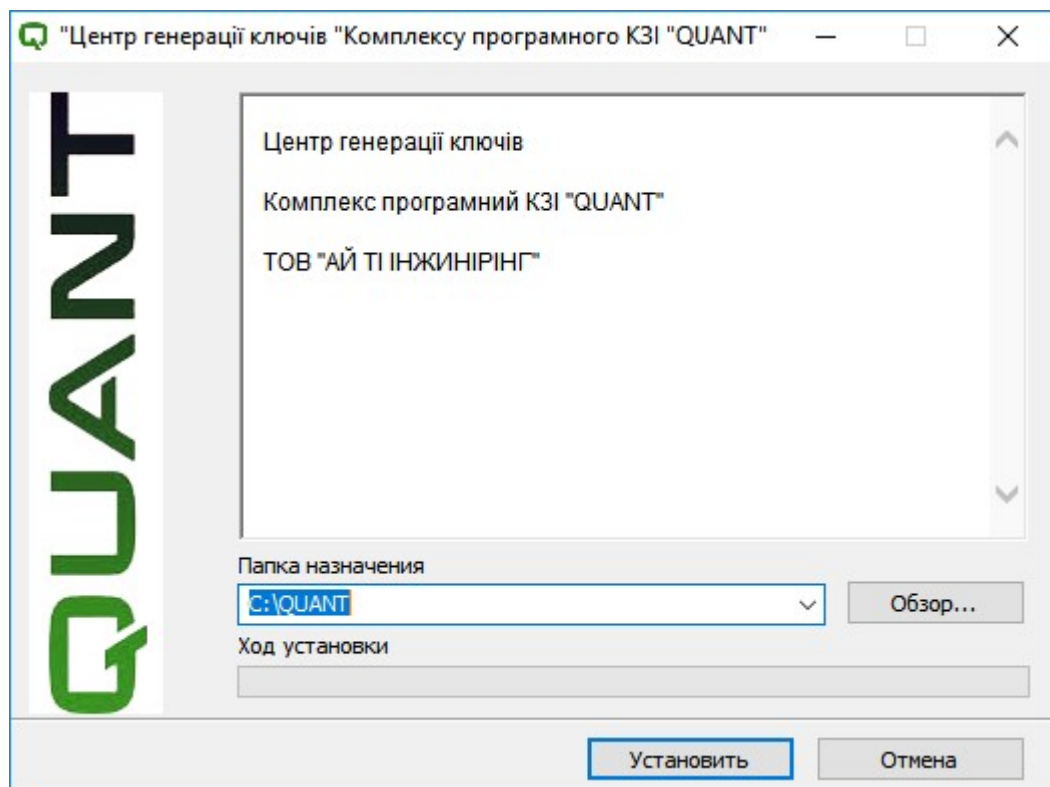
Пор. № зміни	Підпис відпов. особи	Дата внесення

ВСТАНОВЛЕННЯ ЦГК

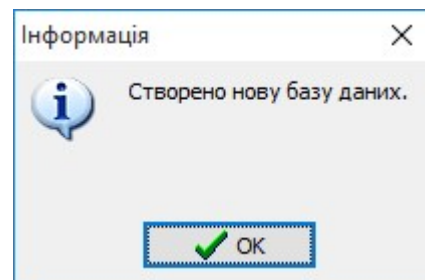
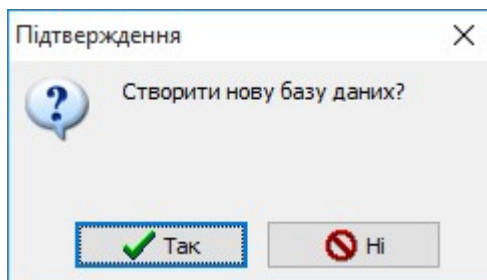
Для встановлення ЦГК необхідно запустити виконуючий файл CGK-QUANT.exe інсталяційного пакету через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої кнопки миші.



У вікні, що відкрилось необхідно вказати шлях до каталогу, в який буде встановлено програмне забезпечення. Для цього натисніть на кнопку «Обзор» та в файловому менеджері операційної системи оберіть каталог. За замовчуванням програмне забезпечення встановлюється за шляхом C:\QUANT, рекомендуємо залишити його таким. Після цього натисніть кнопку «Установить»



Після запуску на екрані з'явиться вікно «Підтвердження» дозволу на створення нової бази даних, яке буде мати наступний вигляд:



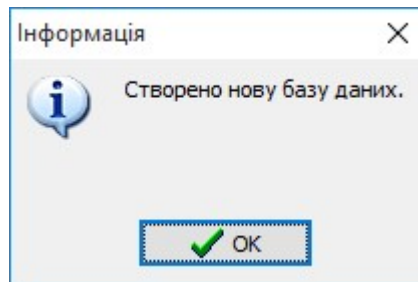
Примітка: У разі першого запуску ЦГК рекомендується натиснути кнопку «Так».

Пор. № зміни	Підпис відпов. особи	Дата внесення

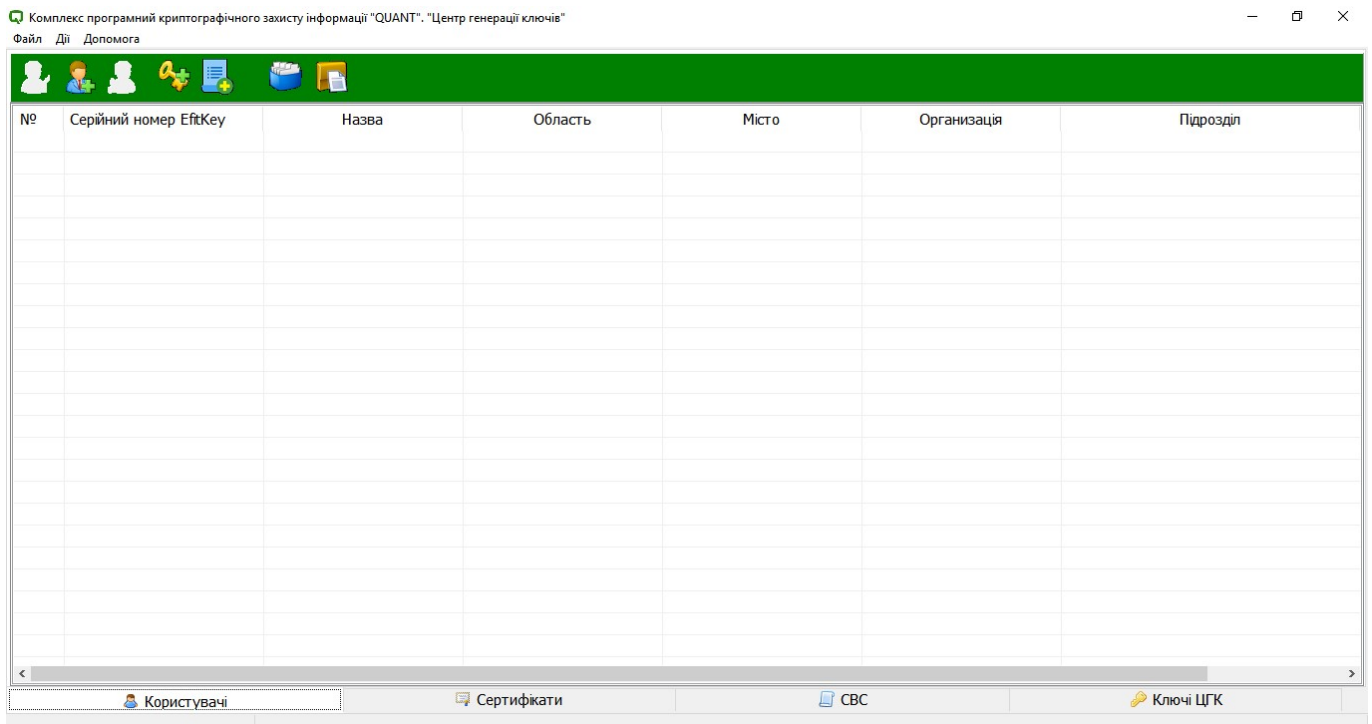
НАСТАНОВА ОПЕРАТОРА. ВЕРСІЯ 1

Примітка: Дане вікно може з'являтися при першому запуску програмного забезпечення та у разі відсутності створеної бази даних чи у випадку пошкодження бази даних.

У вікні «Інформація» необхідно натиснути кнопку «ОК», що засвідчує успішне виконання операції зі створення бази даних.



Відображення вікна «Центр генерації ключів» свідчить про успішний запуск ЦГК.



Після першого успішного запуску ЦГК автоматично буде створено наступні каталоги:

*\keys\	Каталог для збереження ключових даних, ключових документів, сертифікатів відкритих ключів, списків відкликаних сертифікатів
*\log\	Каталог для збереження файлів протоколу роботи програмного забезпечення

Пор. № зміни	Підпис відпов. особи	Дата внесення

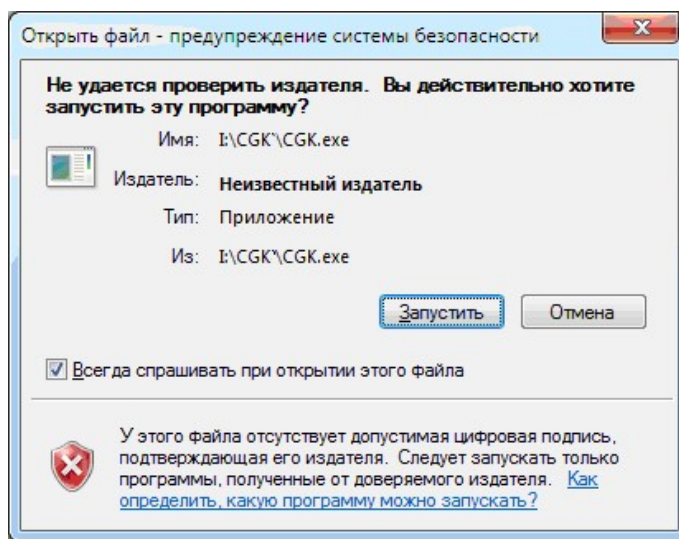
РОБОТА З ЦГК

Формування кореневого ключа (ключових даних) ЦГК

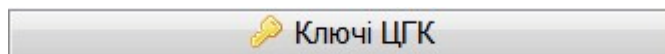
Для формування кореневого ключа ЦГК необхідно підключити з'ємний носій інформації до ЕОМ (у разі встановлення ЦГК на з'ємному носії інформації типу USB-накопичувача), що призначена для формування ключових даних та управління ключовими даними та запустити виконуючий файл CGK.exe через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої кнопки миші.

	CGK.bin	29.09.2017 17:02	Файл "BIN"	1 КБ
	CGK.exe	29.09.2017 16:48	Приложение	3 822 КБ
	CGK.ini	13.05.2016 15:50	Параметры конф...	1 КБ

У вікні попередження системи безпеки ОС необхідно натиснути кнопку «Запустити».



Після запуску на екрані з'явиться вікно «Центр генерації ключів» у якому необхідно обрати вкладку «Ключі ЦГК».



Для формування кореневого ключа ЦГК необхідно натиснути лівою кнопкою миші на кнопку «Генерація ключів...».

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

Файл Дії Допомога

Генерація ключів...				
№	Статус	Початок дії	Завершення дії	

У вікні «Генерація ключів ЦГК» необхідно заповнити реквізити, які будуть занесені до кореневого сертифіката відкритого ключа ЦГК та натиснути кнопку «ОК».

Пор. № зміни	Підпис відпов. особи	Дата внесення

Поле	Значення
Реквізити	
Назва	ROOT
Область	Київська
Місто	Київ
Організація	ІнфоБезпека
Підрозділ	ІТ-безпеки
Сертифікат	
Серійний №	00000001
Дата початку дії	12.10.2017 11:15:58
Термін дії	5

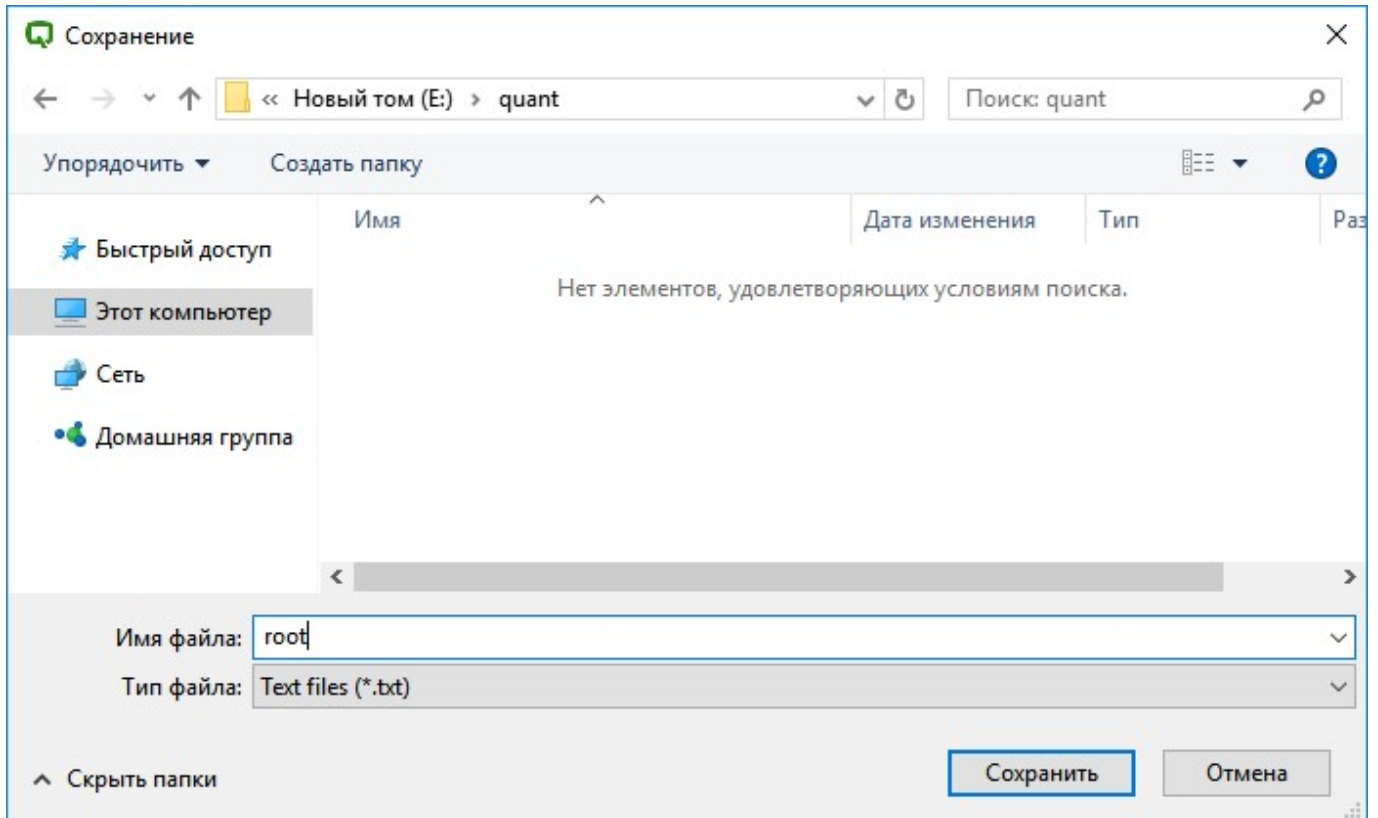
У вікні «Генерацію ключів виконано» необхідно обрати спосіб збереження відомостей про кореневий ключ ЦГК та ПІН-код доступу до використання ключа ЦГК.

Серед запропонованих варіантів збереження доступний друк інформації на папері через підключені до ЕОМ засоби друку або збереження такої інформації у текстовому файлі.

Генерацію ключів виконано	
Відомості про ключі	
Сертифікат	
Серійний номер: 01	
Ідентифікатор ключа: 1965e884aac63ccb42df6f3d77b2691c3440314dc5	
Ідентифікатор ключа ЦСК: 1965e884aac63ccb42df6f3d77b2691c3440314dc5	
Початок терміну дії: 12.10.2017 11:15:58	
Завершення терміну дії: 12.10.2022 11:15:58	
Відомості щодо власника	
Серійний номер: 1	
Назва: ROOT	
Друкують:	<input type="button" value="Зберегти у файл"/> <input type="button" value="HP LaserJet M2727 MFP Series PCL 6"/> <input type="button" value="HP LaserJet M2727 MFP Series Fax"/> <input type="button" value="HP LaserJet Enterprise 600 M601 M602 M603 PCL6 Clas"/>

У разі обрання «Зберегти у файл» у вікні «Сохранение» необхідно обрати каталог для збереження текстової інформації.

Пор. № зміни	Підпис відпов. особи	Дата внесення



У разі успішного створення кореневого ключа ЦГК у списку буде відображено наявність активного для використання ключа, а також термін його дії.

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

№	Статус	Початок дії	Завершення дії
1	Активний	12.10.2017 11:15:58	12.10.2022 11:15:58

Для перегляду детальної інформації про кореневий ключ ЦГК необхідно виділити ключ лівою кнопкою миші та натиснути кнопку «Переглянути...» або обрати «Перегляд відомостей про ключі ЦГК» в контекстному меню.

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

№	Статус	Початок дії	Завершення дії
1	Активний	12.10.2017 11:15:58	12.10.2022 11:15:58

Пор. № зміни	Підпис відпов. особи	Дата внесення

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

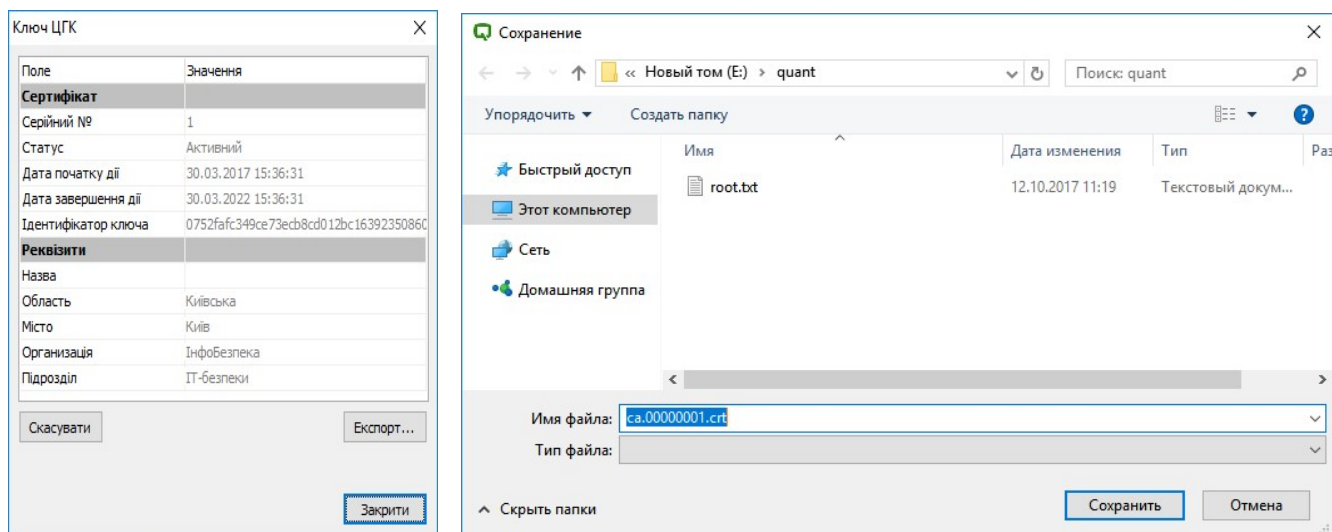
Файл Дії Допомога

№	Статус	Початок дії	Завершення дії
1	Активний	12.10.2017 11:15:58	12.10.2022 11:15:58

Перегляд відомостей про ключі ЦГК

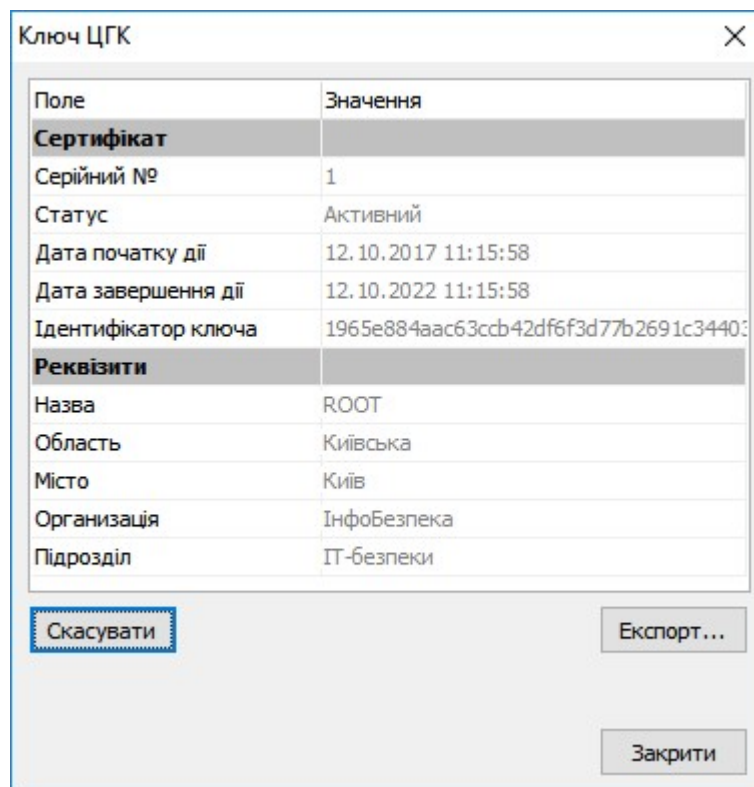
Генерація нових ключів та формування сертифікату ЦГК

У разі необхідності експорту кореневого сертифіката відкритого ключа ЦГК необхідно натиснути кнопку «Експорт...» та обрати каталог для збереження.



Для скасування кореневого сертифіката відкритого ключа ЦГК, а також припинення використання корневих ключових даних ЦГК необхідно натиснути кнопку «Скасувати».

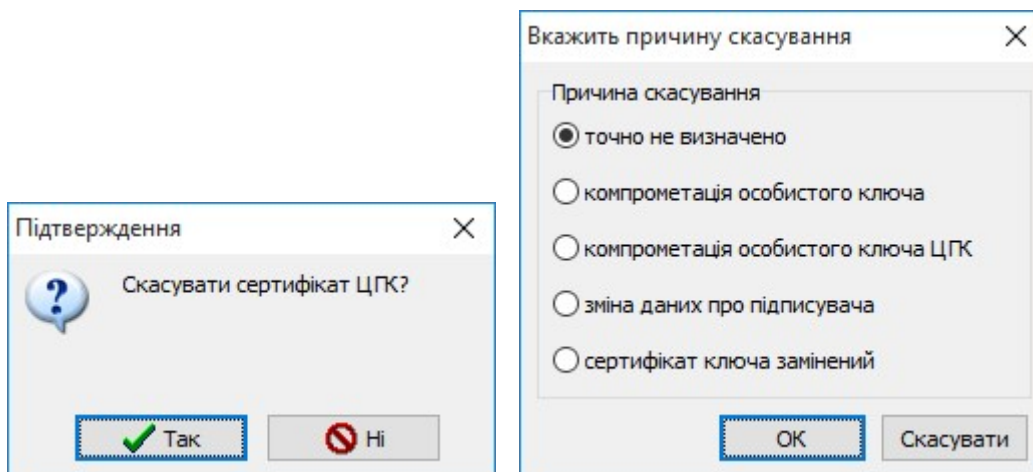
Пор. № зміни	Підпис відпов. особи	Дата внесення



Поле	Значення
Сертифікат	
Серійний №	1
Статус	Активний
Дата початку дії	12.10.2017 11:15:58
Дата завершення дії	12.10.2022 11:15:58
Ідентифікатор ключа	1965e884aac63ccb42df6f3d77b2691c34403
Реквізити	
Назва	ROOT
Область	Київська
Місто	Київ
Організація	ІнфоБезпека
Підрозділ	ІТ-безпеки

Buttons: Скасувати, Експорт..., Закрити

У вікні «Підтвердження» необхідно натиснути кнопку «Так» для продовження скасування або кнопку «Ні» для відхилення виконання операції. Для остаточного скасування сертифіката відкритого ключа ЦГК, а також припинення використання кореневих ключових даних ЦГК у вікні «Вкажіть причину скасування» необхідно обрати одну з причин, на підставі якої здійснюється скасування.



Підтвердження

Скасувати сертифікат ЦГК?

Buttons: Так, Ні

Вкажіть причину скасування

Причина скасування

- ☒ точно не визначено
- ☐ компрометація особистого ключа
- ☐ компрометація особистого ключа ЦГК
- ☐ зміна даних про підписувача
- ☐ сертифікат ключа замінений

Buttons: ОК, Скасувати

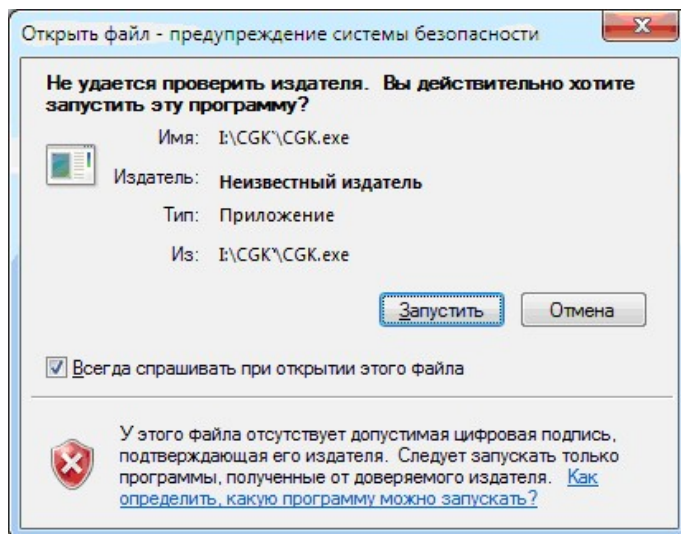
Робота з анкетами (профайлами) користувачів

Для створення, коригування, видалення анкет (профайлів) користувачів «Адміністратор» або «Користувач» необхідно запустити виконуючий файл CGK.exe через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої кнопки миші.

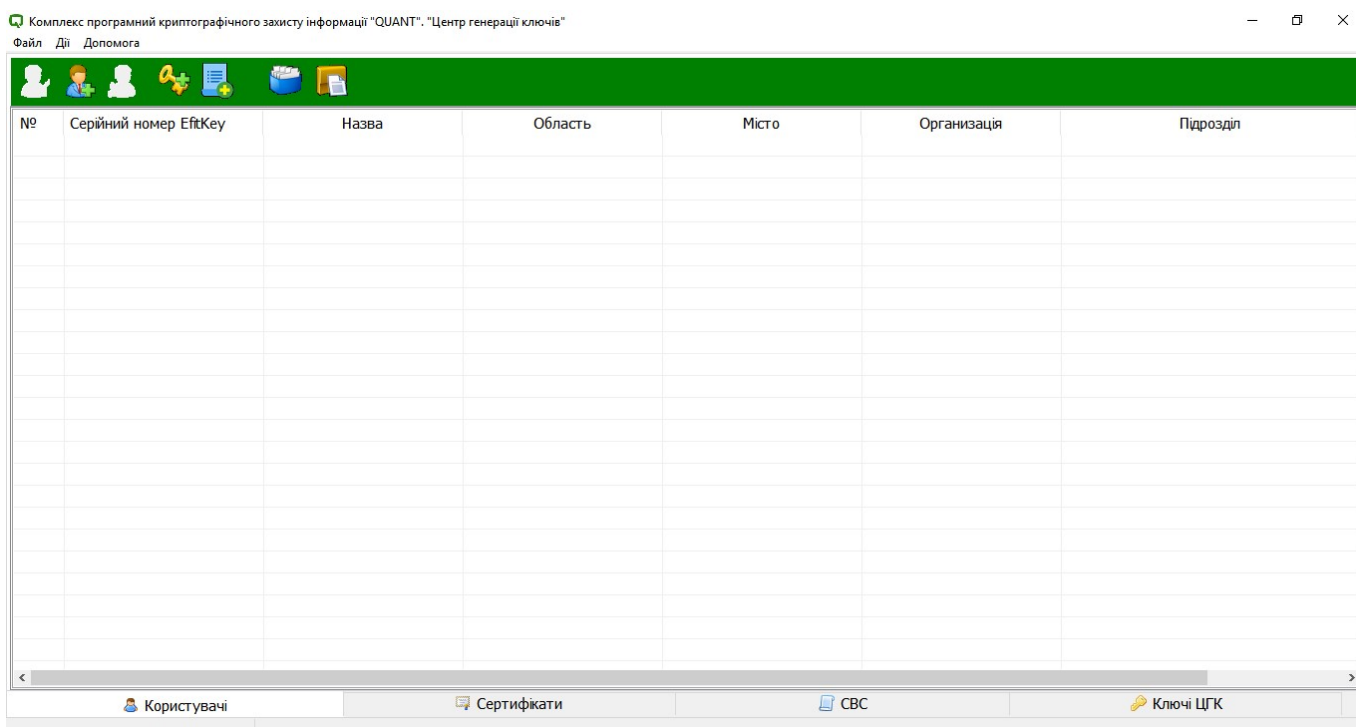
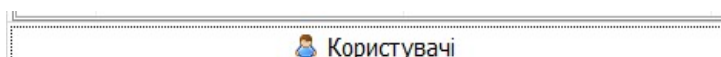
 CGK.bin	29.09.2017 17:02	Файл "BIN"	1 КБ
 CGK.exe	29.09.2017 16:48	Приложение	3 822 КБ
 CGK.ini	13.05.2016 15:50	Параметры конф...	1 КБ

Пор. № зміни	Підпис відпов. особи	Дата внесення

У вікні попередження системи безпеки ОС необхідно натиснути кнопку «Запустити».



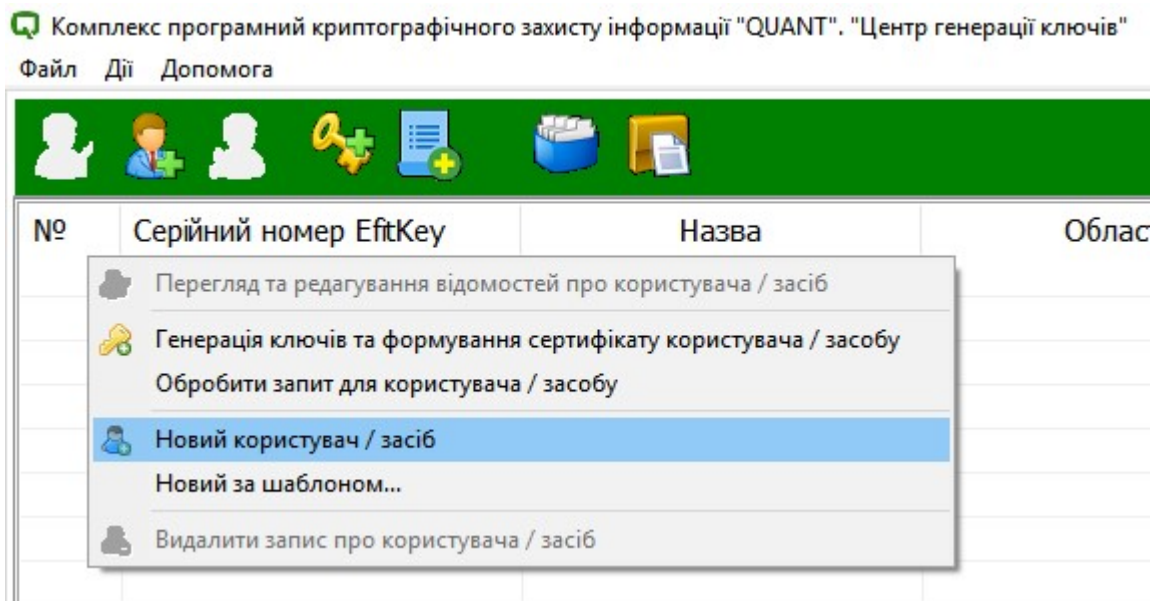
Після запуску, знизу на екрані необхідно натиснути на пункт меню «Користувачі».



Після запуску на екрані з'явиться вікно «Центр генерації ключів» у якому необхідно натиснути кнопку «Новий...» або обрати в контекстному меню «Новий користувач / засіб».



Пор. № зміни	Підпис відпов. особи	Дата внесення



У вікні «Користувач» необхідно зазначити інформацію, яка буде у подальшому вноситися до сертифіката відкритого ключа «Користувача» або «Адміністратора».

Поле	Значення
Серійний №	1001
Серійний № EfitKey	
Назва	Центральний шлюз
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки
Тип	Адміністратор

OK Скасувати

В процесі заповнення анкети обов'язково необхідно обрати тип «Адміністратор» або «Користувач»

Тип: Адміністратор

OK Скасувати

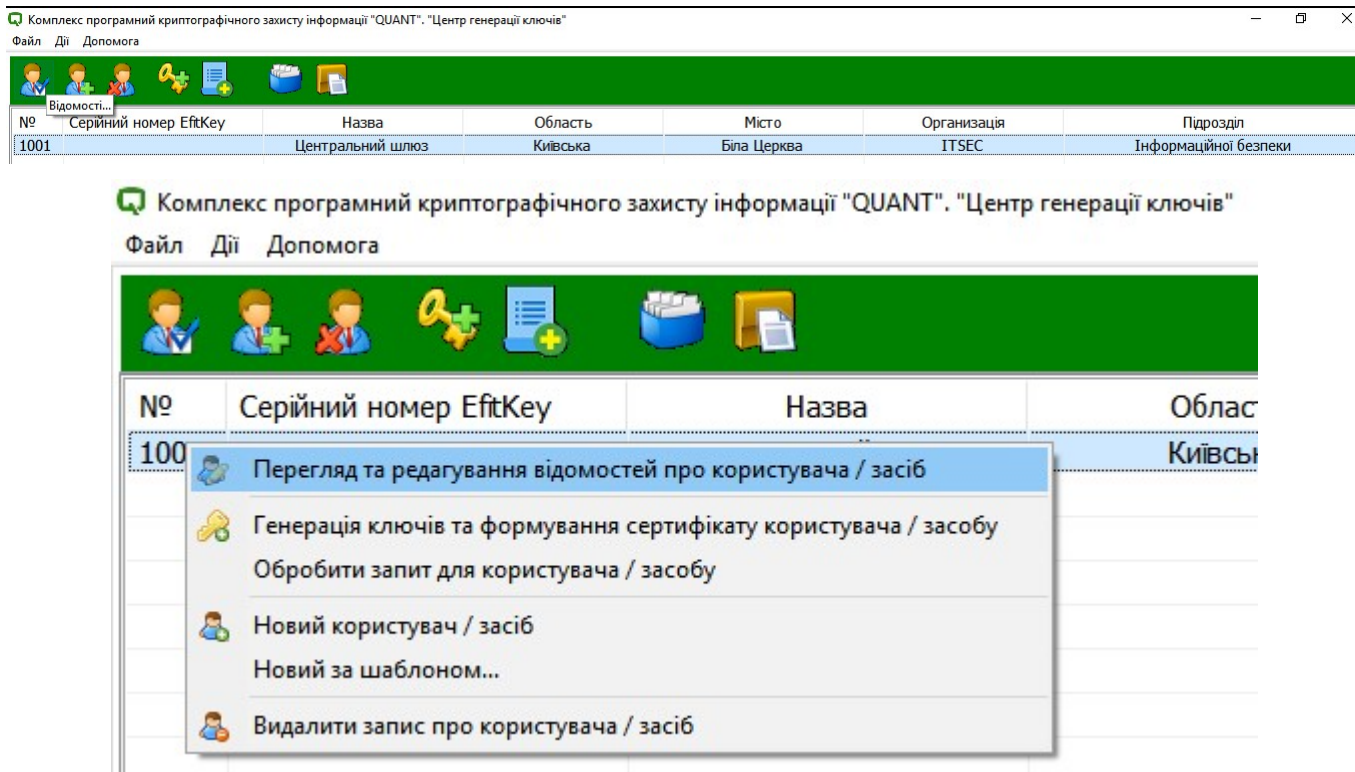
Для збереження анкети необхідно натиснути кнопку «ОК», або кнопку «Скасувати» для відхилення операції збереження.

Фактом успішного створення анкети є її наявність у списку.

№	Серійний номер EfitKey	Назва	Область	Місто	Організація	Підрозділ
1001		Центральний шлюз	Київська	Біла Церква	ITSEC	Інформаційної безпеки

Пор. № зміни	Підпис відпов. особи	Дата внесення

У разі необхідності внесення змін до створеної анкети потрібно її обрати та натиснути кнопку «Відомості...» або обрати в контекстному меню «Перегляд та редагування відомостей про користувача / засіб».



Після внесення змін до анкети для їх збереження необхідно натиснути кнопку «ОК» або «Скасувати» для відхилення операції.

Користувач

Реквізити

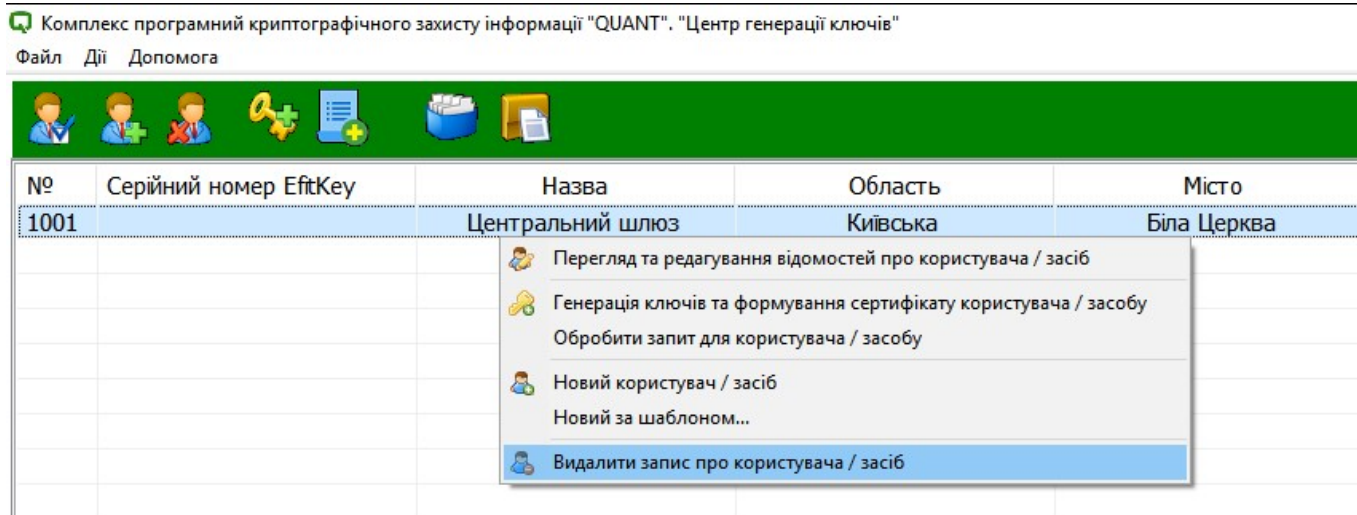
Поле	Значення
Серійний №	1001
Серійний № EfitKey	
Назва	Центральний шлюз
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки
Тип	Адміністратор

OK Скасувати

Для здійснення видалення створеної анкети потрібно її обрати та натиснути кнопку «Видалити» або обрати в контекстному меню «Видалити запис про користувача / засіб».

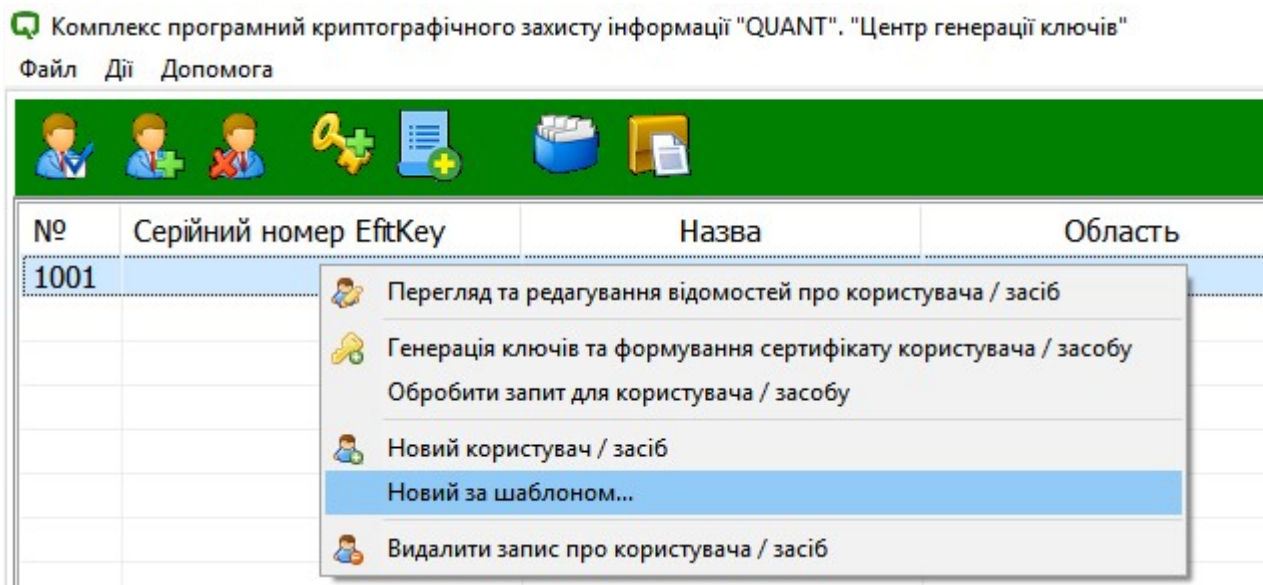


Пор. № зміни	Підпис відпов. особи	Дата внесення



З метою прискорення та оптимізації процесу створення анкет наявна можливість створення анкет за шаблоном.

Для створення анкети за шаблоном необхідно обрати вже створену анкету та обрати пункт «Новий за шаблоном...» в контекстному меню.



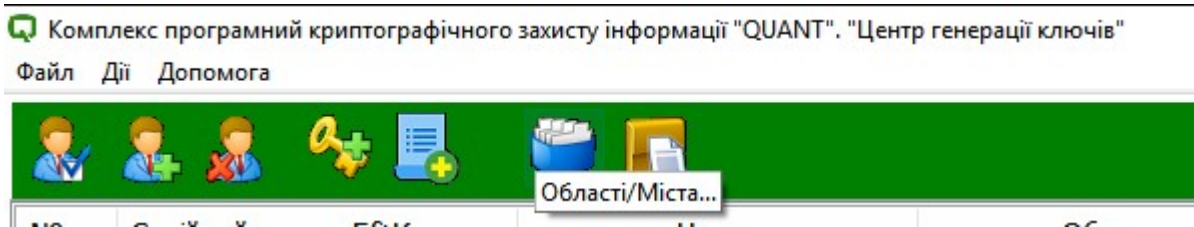
У вікні «Користувач» необхідно заповнити лише реквізит «Назва» оскільки усі інші реквізити будуть автоматично заповнені на підставі інформації з обраної анкети.


Пор. № зміни	Підпис відпов. особи	Дата внесення

Поле	Значення
Серійний №	1002
Серійний № EfitKey	
Назва	
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки
Тип	Адміністратор

З метою прискорення та оптимізації процесу заповнення реквізитів «Область» та «Місто» анкет наявна можливість створення наперед заповнених позицій.

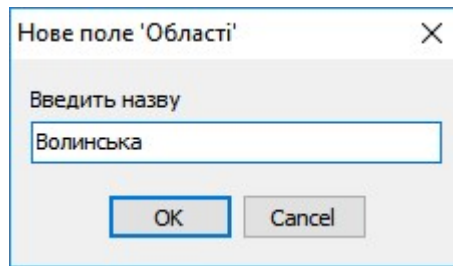
Необхідно натиснути кнопку «Області / Міста...».




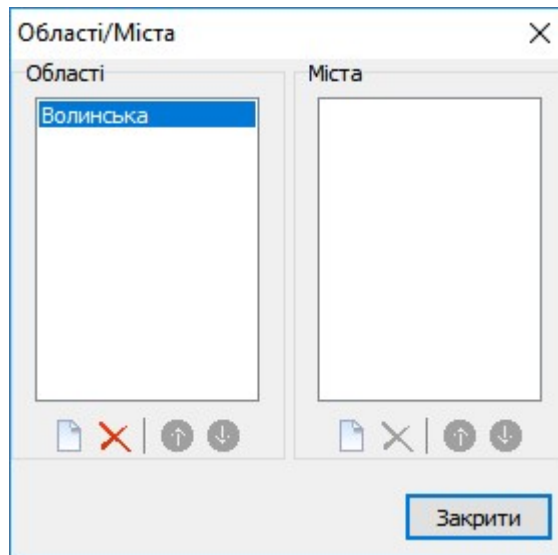
У вікні «Області / Міста» в розділі «Області» необхідно натиснути .

У вікні «Області» потрібно зазначити назву області та натиснути кнопку «ОК» для застосування або «Cancel» для відхилення операції.

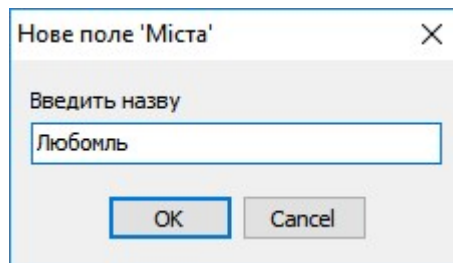
Пор. № зміни	Підпис відпов. особи	Дата внесення



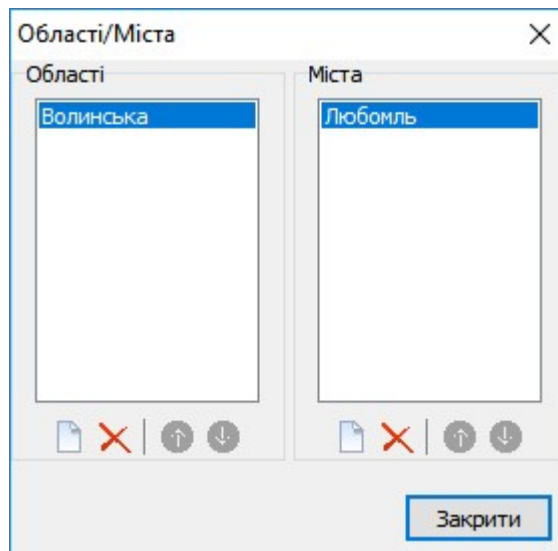
У вікні «Області / Міста» в розділі «Міста» необхідно натиснути .



У вікні «Нове поле `Міста`» потрібно зазначити назву міста наперед зазначеної області та натиснути кнопку «OK» для застосування або «Cancel» для відхилення операції.



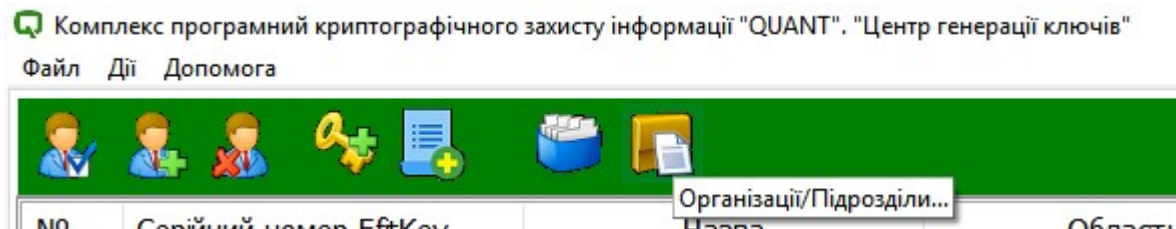
Після внесення інформації стосовно областей та міст таких областей необхідно у вікні «Області / Міста» натиснути кнопку «Закрити».




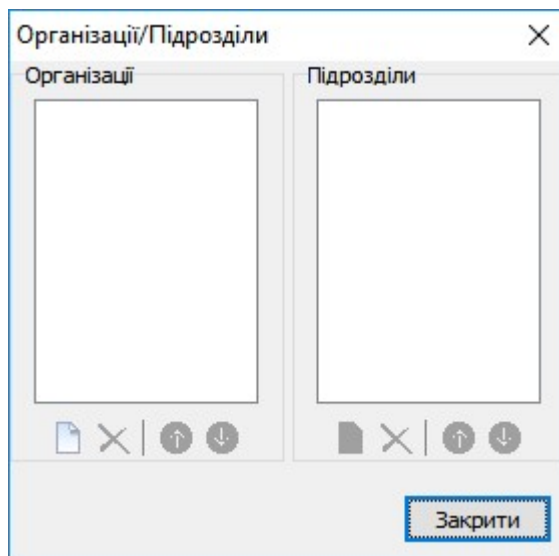
Пор. № зміни	Підпис відпов. особи	Дата внесення

З метою прискорення та оптимізації процесу заповнення реквізитів «Організація» та «Підрозділ» анкет наявна можливість створення наперед заповнених позицій.

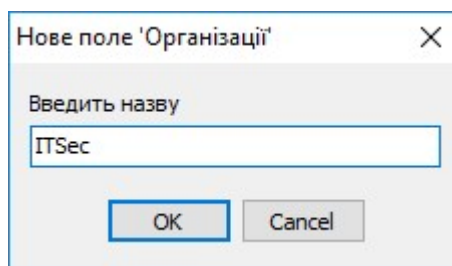
Необхідно натиснути кнопку «Організації / Підрозділи...».



У вікні «Організації / Підрозділи» в розділі «Організації» необхідно натиснути .

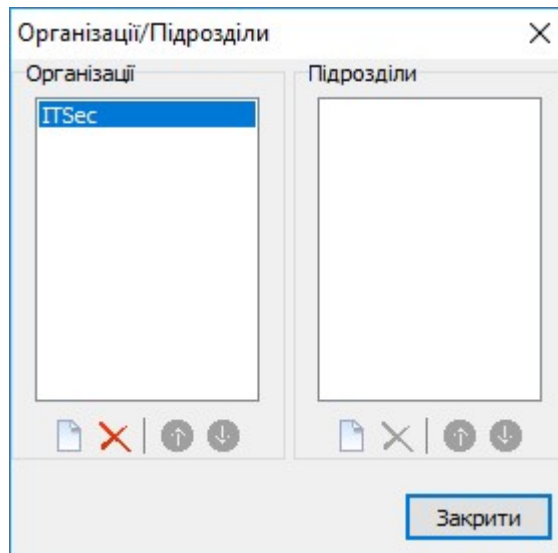


У вікні «Нове поле `Організації`» потрібно зазначити назву підприємства, установи, організації та натиснути кнопку «ОК» для застосування або «Cancel» для відхилення операції.

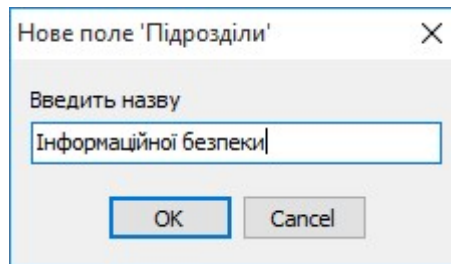


У вікні «Організації / Підрозділи» в розділі «Підрозділи» необхідно натиснути .

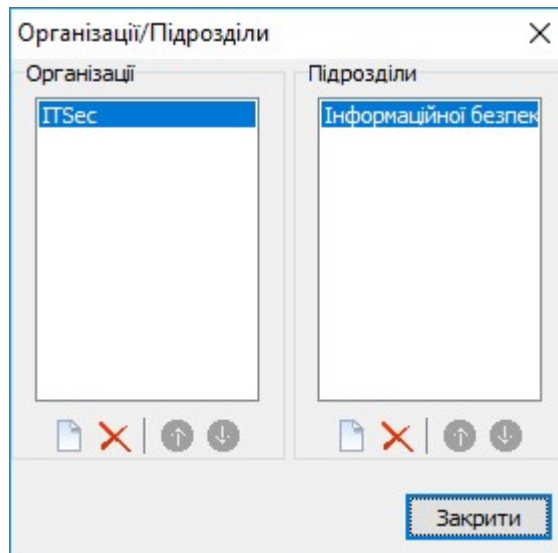
Пор. № зміни	Підпис відпов. особи	Дата внесення



У вікні «Нове поле 'Підрозділ'» потрібно зазначити назву підрозділу підприємства, установи, організації та натиснути кнопку «ОК» для застосування або «Cancel» для відхилення операції.



Після внесення інформації стосовно підприємств, установ, організацій та структурних підрозділів необхідно у вікні «Організації / Підрозділи» натиснути кнопку «Закрити».



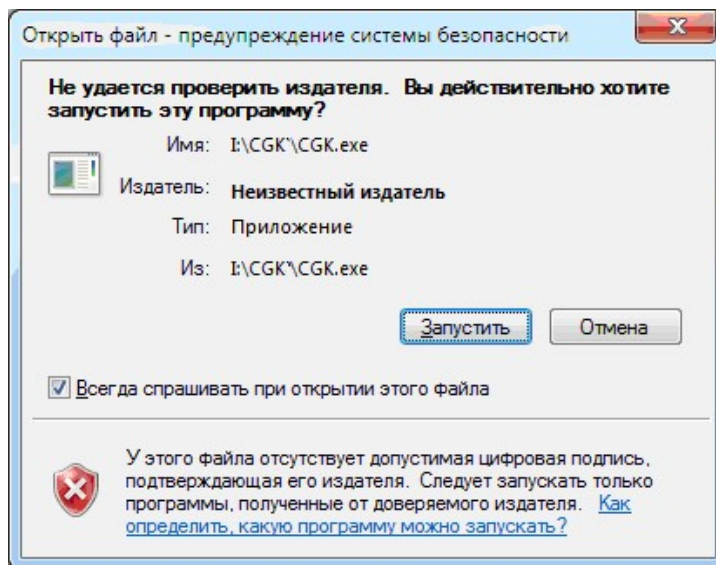
Пор. № зміни	Підпис відпов. особи	Дата внесення

Формування ключових даних та сертифікатів відкритих ключів за даними наперед сформованих анкет (профайлів)

Для формування ключових даних та сертифікатів відкритих ключів «Адміністратор» або «Користувач» необхідно запустити виконуючий файл CGK.exe через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої кнопки миші.

	CGK.bin	29.09.2017 17:02	Файл "BIN"	1 КБ
	CGK.exe	29.09.2017 16:48	Приложение	3 822 КБ
	CGK.ini	13.05.2016 15:50	Параметры конф...	1 КБ

У вікні попередження системи безпеки ОС необхідно натиснути кнопку «Запустити».



Після запуску на екрані з'явиться вікно «Центр генерації ключів» у якому необхідно обрати анкету (звертайте уваги на «Тип» - «Користувач / Адміністратор») за якою необхідно сформувати ключові дані та сертифікат відкритого ключа ключових даних.

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

Файл Дії Допомога

№	Серійний номер EfitKey	Назва	Область	Місто	Організація	Підрозділ
1001		Центральний шлюз	Київська	Біла Церква	ITSEC	Інформаційної безпеки
1002		Центральний шлюз	Київська	Київ	InfoSafe	ІТ

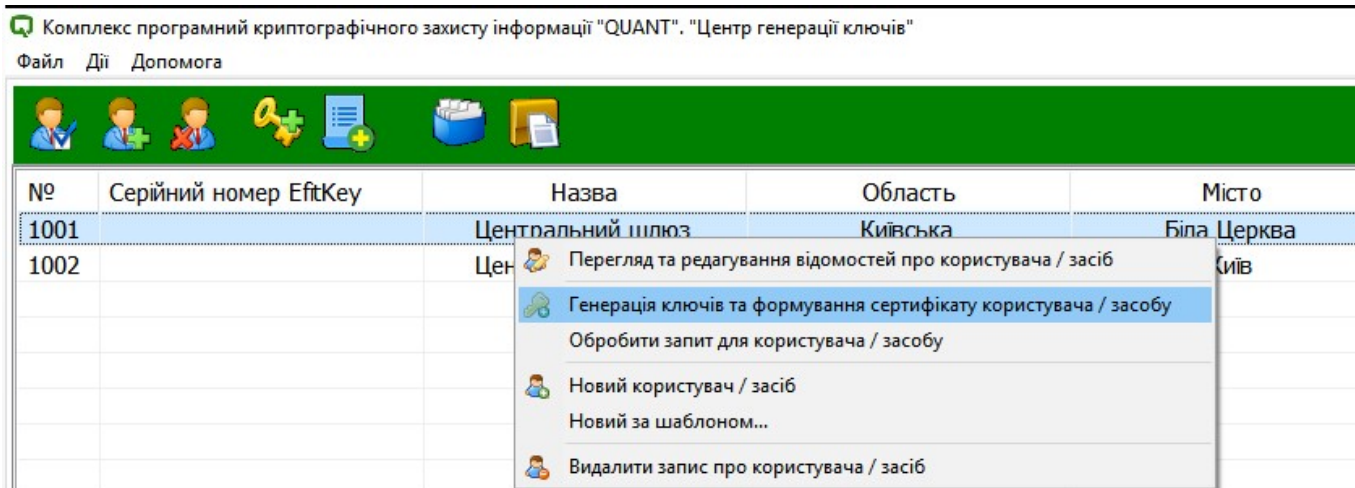
Для формування ключових даних та сертифіката відкритого ключа ключових даних після обрання анкети необхідно натиснути кнопку «Генерація ключів...» або обрати в контекстному меню «Генерація ключів та формування сертифіката користувача / засобу».

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

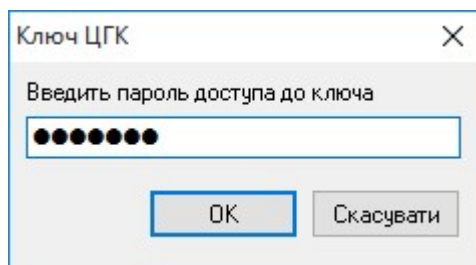
Файл Дії Допомога

№	Серійний номер EfitKey	Назва	Область	Місто	Організація	Підрозділ
1001		Центральний шлюз	Київська	Біла Церква	ITSEC	Інформаційної безпеки
1002		Центральний шлюз	Київська	Київ	InfoSafe	ІТ

Пор. № зміни	Підпис відпов. особи	Дата внесення



У вікні «Ключ ЦГК» необхідно зазначити пароль доступу до ключа ЦГК та натиснути кнопку «ОК» для виконання або кнопку «Скасувати» для відхилення виконання операції.



Примітка: Пароль доступу до ключа ЦГК було Вами надруковано або збережено у текстовий файл в процесі формування ключа ЦГК.

Сертифікат

Серійний номер: 01

Ідентифікатор ключа:

1965e884aас63сcb42df6f3d77b2691c3440314dc5930613e2dd9a9059a9504a

Ідентифікатор ключа ЦСК:

1965e884aас63сcb42df6f3d77b2691c3440314dc5930613e2dd9a9059a9504a

Початок терміну дії: 12.10.2017 11:15:58

Завершення терміну дії: 12.10.2022 11:15:58

Відомості щодо власника

Серійний номер: 1

Назва: ROOT

Область: Київська

Місто: Київ

Організація: ІнфоБезпека

Підрозділ: IT-безпеки

Секретний ключ

Пароль: *****

У вікні «Генерація ключів» необхідно натиснути кнопку «ОК» для виконання або кнопку «Скасувати» для відхилення виконання операції.

Пор. № зміни	Підпис відпов. особи	Дата внесення

Генерація ключів

Поле	Значення
Власник	
Серійний №	1001
Назва	Центральний шлюз
Ім'я	
Прізвище	
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки
Тип	Користувач
Сертифікат	
Серійний №	00000002
Дата початку дії	12.10.2017 11:49:12
Термін дії	12.10.2018 11:49:12
Шлях до НКІ	C:\QUANT\keys\admin\users\1001
Файл з ДКЕ	


☐ Генерація на EfitKey

OK Скасувати

Примітка: За замовчуванням ключові дані та сертифікат відкритого ключа ключових даних «Шлюзу» зберігається у створеному при першому запуску ЦГК каталогу «keys».

Для збереження ключових даних та сертифікат відкритого ключа ключових даних «Шлюзу» використовується каталог \keys\admin

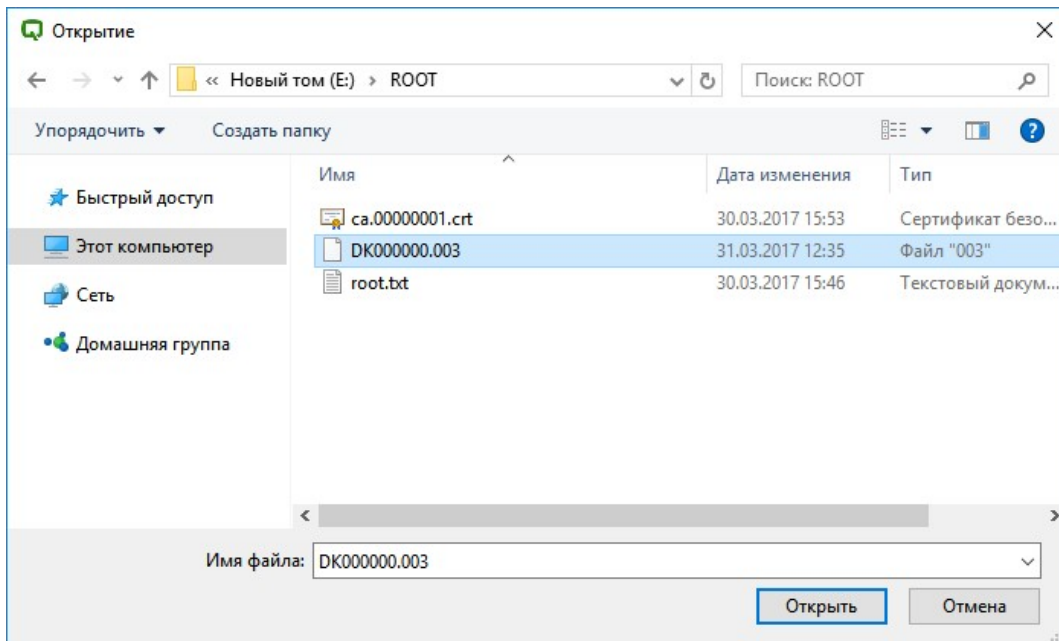
\keys\admin\ca	Каталог для збереження сертифіката відкритого ключа ключових даних ЦГК
\keys\admin\crl	Каталог для збереження списків відкликаних сертифікатів сформованих ЦГК
\keys\admin\users	Каталог для збереження ключових даних на ключовому документі та сертифікатів відкритого ключа ключових даних «Шлюзу» сформованих ЦГК

Важливо: У випадку використання довгострокового ключового елементу отриманого від органу державної влади у встановленому порядку або використання власного необхідно натиснути кнопку  у полі «Файл з ДКЕ» та обрати такий файл.

Файл з ДКЕ



Пор. № зміни	Підпис відпов. особи	Дата внесення

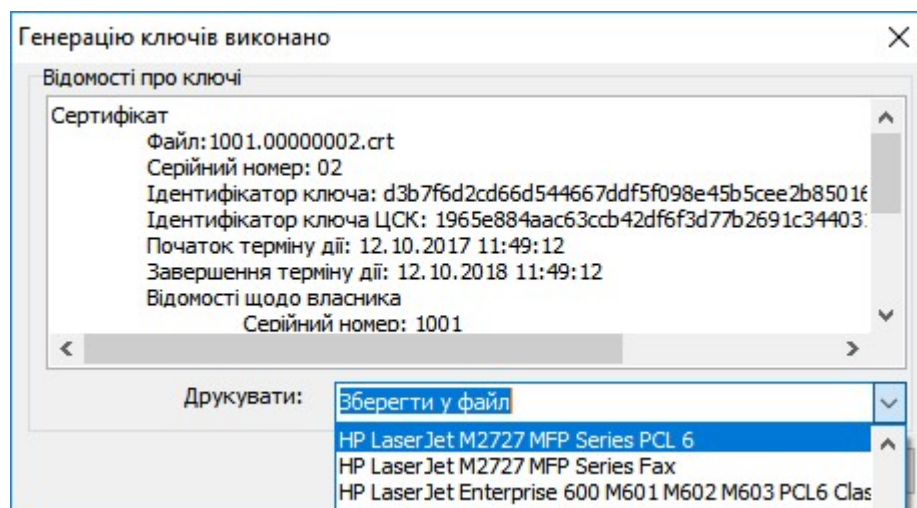


Важливо: У разі використання довгострокового ключового елементу необхідно кожного разу при формуванні ключових даних та сертифіката відкритого ключа ключових даних обов'язково обирати файл ДКЕ, що використовується.



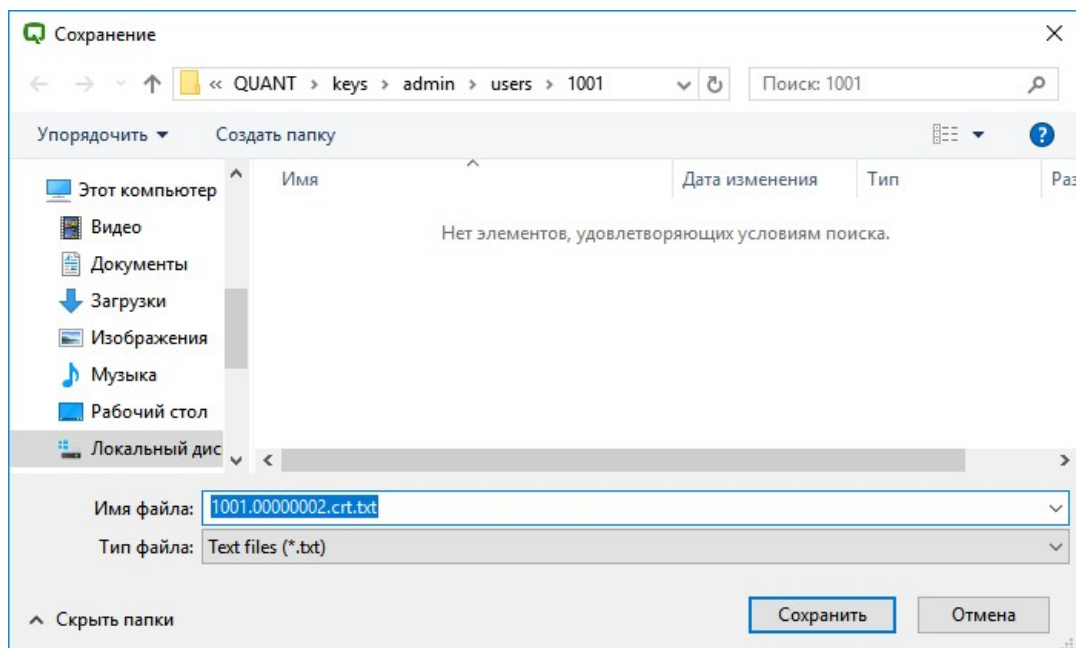
У вікні «Генерацію ключів виконано» необхідно обрати спосіб збереження відомостей про ключові дані та сертифіката відкритого ключа ключових даних «Шлюзу» та ПІН-код доступу до таких ключових даних.

Серед запропонованих варіантів збереження доступний друк інформації на папері через підключені до ЕОМ засоби друку або збереження такої інформації у текстовому файлі.

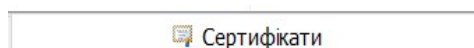


У разі обрання «Зберегти у файл» у вікні «Сохранение» необхідно обрати каталог для збереження текстової інформації.

Пор. № зміни	Підпис відпов. особи	Дата внесення



У разі успішного створення ключових даних та сертифіката відкритого ключа ключових даних «Адміністратора» на вкладці «Сертифікати» повинен бути доступний новостворений сертифікат відкритого ключа ключових даних «Адміністратора».



№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Сформований	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...

За результатом успішного виконання операції у каталогу 'keys\admin\users\' буде створено каталог для «Адміністратора» у якому буде збережено наступні файли:

1001.00000002.cnt	Ключові дані «Адміністратора»
1001.00000002.crt	Сертифікат відкритого ключа ключових даних «Адміністратора»
1001.00000002.dke	Довгостроковий ключовий елемент, що було використано у шифрованому вигляді на ключових даних «Адміністратора»
1001.00000002.crt.txt	Детальний опис

Для формування ключових даних та сертифіката відкритого ключа ключових даних «Користувач» (тип: «Користувач») необхідно натиснути кнопку «Генерація ключів...» або обрати «Генерація ключів та формування сертифікату користувача / засобу».

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

Файл Дії Допомога

№	Серійний номер EtkKey	Назва	Область	Місто	Організація	Підрозділ	Тип
1001		Центральний шлюз	Київська	Біла Церква	ITSEC	Інформаційної безпеки	Адміністратор
1002		Центральний шлюз	Київська	Київ	InfoSafe	ІТ	Користувач

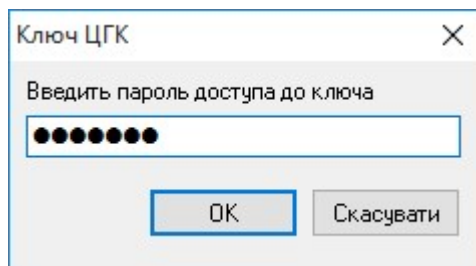
Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

Файл Дії Допомога

№	Серійний номер EtkKey	Назва	Область	Місто	Організація	Підрозділ	Тип
1001		Центральний шлюз	Київська	Біла Церква	ITSEC	Інформаційної безпеки	Адміністратор
1002		Центральний шлюз	Київська	Київ	InfoSafe	ІТ	Користувач

Пор. № зміни	Підпис відпов. особи	Дата внесення

У вікні «Ключ ЦГК» необхідно зазначити пароль доступу до ключа ЦГК та натиснути кнопку «ОК» для виконання або кнопку «Скасувати» для відхилення виконання операції.



Примітка: Пароль доступу до ключа ЦГК було Вами надруковано або збережено у текстовий файл в процесі формування ключа ЦГК.

Сертифікат

Серійний номер: 01

Ідентифікатор ключа:

1965e884aac63ccb42df6f3d77b2691c3440314dc5930613e2dd9a9059a9504a

Ідентифікатор ключа ЦСК:

1965e884aac63ccb42df6f3d77b2691c3440314dc5930613e2dd9a9059a9504a

Початок терміну дії: 12.10.2017 11:15:58

Завершення терміну дії: 12.10.2022 11:15:58

Відомості щодо власника

Серійний номер: 1

Назва: ROOT

Область: Київська

Місто: Київ

Організація: ІнфоБезпека

Підрозділ: IT-безпеки

Секретний ключ

Пароль *****

У вікні «Генерація ключів» необхідно натиснути кнопку «ОК» для виконання або кнопку «Скасувати» для відхилення виконання операції.

Пор. № зміни	Підпис відпов. особи	Дата внесення

Поле	Значення
Власник	
Серійний №	1002
Назва	Центральний шлюз
Ім'я	
Прізвище	
Область	Київська
Місто	Київ
Організація	InfoSafe
Підрозділ	ІТ
Тип	Користувач
Сертифікат	
Серійний №	00000003
Дата початку дії	12.10.2017 15:07:35
Термін дії	12.10.2018 15:07:35
Шлях до НКІ	C:\QUANT\keys\user\users\1002
Файл з ДКЕ	


☐ Генерація на EfitKey

OK Скасувати

Примітка: За замовчуванням ключові дані та сертифікат відкритого ключа ключових даних «Клієнта» зберігається у створеному при першому запуску ЦГК каталогу «keys».

Для збереження ключових даних та сертифіката відкритого ключа ключових даних «Шлюзу» використовується каталог \keys\user

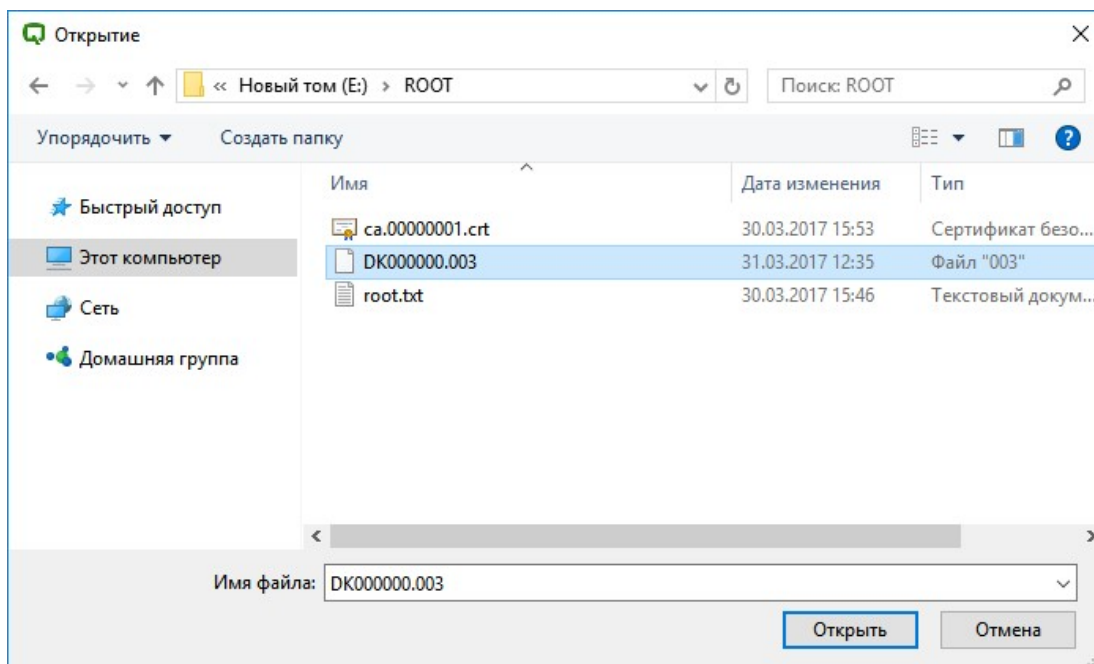
\keys\user\users\	Каталог для збереження ключових даних на ключовому документі та сертифікатів відкритого ключа ключових даних «Клієнта» сформованих ЦГК
-------------------	--

Важливо: У випадку використання довгострокового ключового елементу отриманого від органу державної влади у встановленому порядку або використання власного необхідно натиснути кнопку  у полі «Файл з ДКЕ» та обрати такий файл.

Файл з ДКЕ



Пор. № зміни	Підпис відпов. особи	Дата внесення

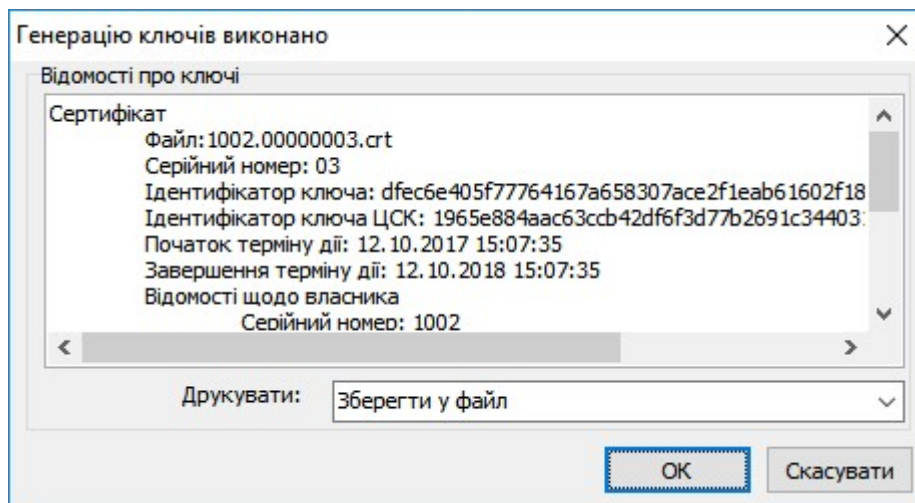


Важливо: У разі використання довгострокового ключового елементу необхідно кожного разу при формуванні ключових даних та сертифіката відкритого ключа ключових даних обов'язково обирати файл ДКЕ, що використовується.



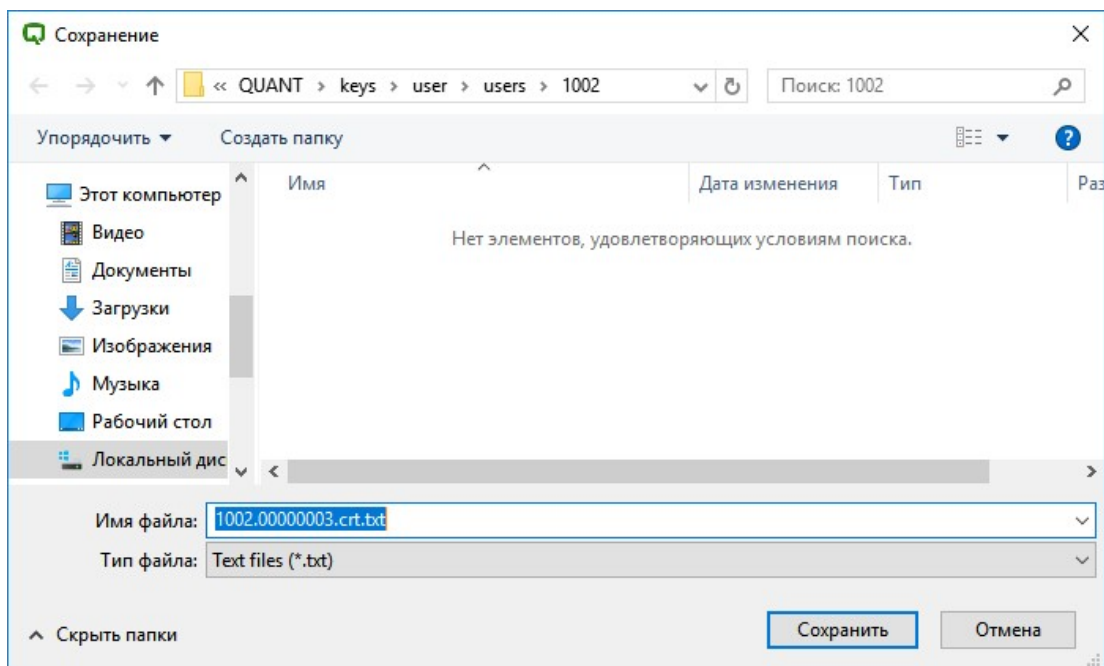
У вікні «Генерацію ключів виконано» необхідно обрати спосіб збереження відомостей про ключові дані та сертифіката відкритого ключа ключових даних «Клієнта» та ПІН-код доступу до таких ключових даних.

Серед запропонованих варіантів збереження доступний друк інформації на папері через підключені до ЕОМ засоби друку або збереження такої інформації у текстовому файлі.

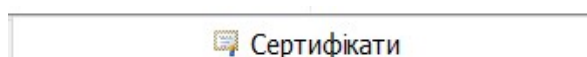


У разі обрання «Зберегти у файл» у вікні «Сохранение» необхідно обрати каталог для збереження текстової інформації.

Пор. № зміни	Підпис відпов. особи	Дата внесення



У разі успішного створення ключових даних та сертифіката відкритого ключа ключових даних «Клієнт» на вкладці «Сертифікати» повинен бути доступний новостворений сертифікат відкритого ключа ключових даних «Клієнта».



Комплекс программный криптографический зашиту информации "QUANT". "Центр генерации ключей"

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Сформований	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63cb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Сформований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63cb42df6f3d77b2691c344...

За результатом успішного виконання операції у каталогу \keys\user\users\ буде створено каталог для «Користувача» у якому буде збережено наступні файли:

1002.00000003.cnt	Ключові дані «Користувач»
1002.00000003.crt	Сертифікат відкритого ключа ключових даних «Користувач»
1002.00000003.dke	Довгостроковий ключовий елемент, що було використано у шифрованому вигляді на ключових даних «Користувач»
1002.00000003.crt.txt	Детальний опис
CN.TXT	Значення поля «Назва» користувача

Для формування ключових даних та сертифікатів відкритих ключів «Адміністратор» або «Користувач» на захищений носій Efit Key, необхідно інсталиювати програмне забезпечення EfitKeysTool для EfitKey згідно інструкції користувача EfitKeysTool_UserHelp_v.1.pdf.

Потім у вікні «Генерація ключів» обрати пункт «Генерація на EfitKey» та натиснути «ОК».

Пор. № зміни	Підпис відпов. особи	Дата внесення

Поле	Значення
Власник	
Серійний №	1002
Назва	Центральний шлюз
Ім'я	
Прізвище	
Область	Київська
Місто	Київ
Організація	InfoSafe
Підрозділ	ІТ
Тип	Користувач
Сертифікат	
Серійний №	00000004
Дата початку дії	12.10.2017 15:12:19
Термін дії	12.10.2018 15:12:19
Шлях до НКІ	C:\QUANT\keys\user\users\1002
Файл з ДКЕ	

☒ Генерація на EfitKey

ОК Скасувати

У наступному вікні необхідно ввести власний пароль до захищеного носія EfitKey, за замовчуванням від виробника це «12345678».

Введіть пароль доступу до ключа

●●●●●●●●●●●●

ОК Скасувати

У вікні «Генерацію ключів виконано» обрати збереження у файл або друк на принтері.

Відомості про ключі

Сертифікат

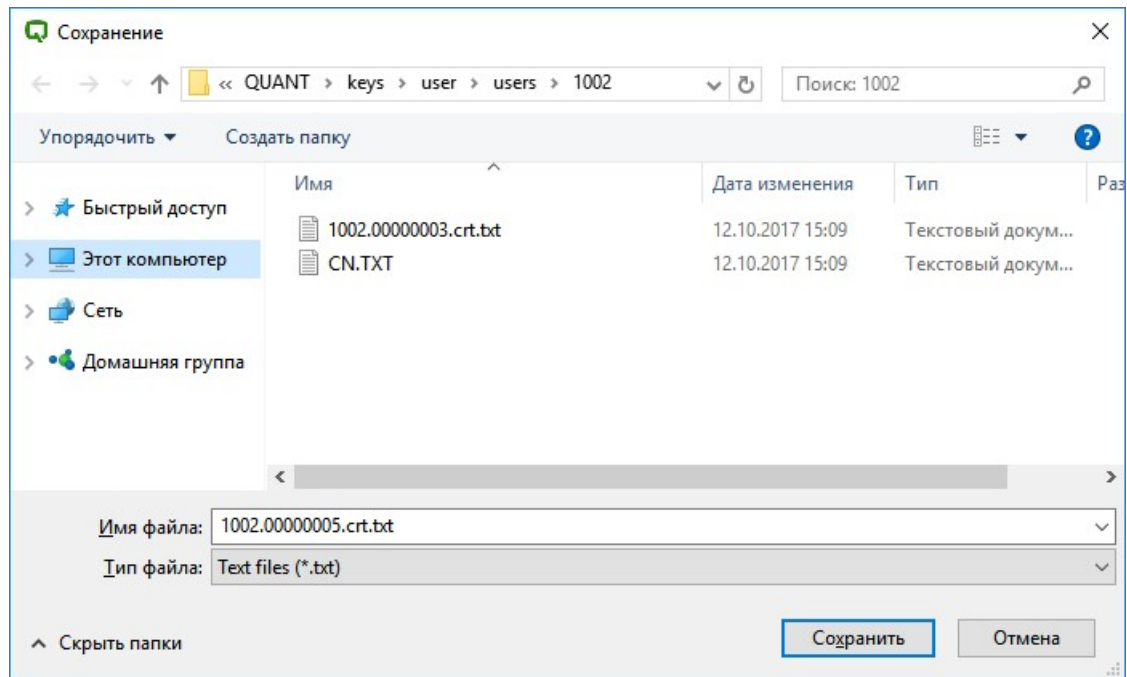
- Файл: 1002.00000005.crt
- Серійний номер: 05
- Ідентифікатор ключа: 91d6a8af630699f5c5c8e7d6c68018de8c772b3889
- Ідентифікатор ключа ЦСК: 1965e884aac63ccb42df6f3d77b2691c34403
- Початок терміну дії: 13.10.2017 13:27:30
- Завершення терміну дії: 13.10.2018 13:27:30
- Відомості щодо власника
- Серійний номер: 1002

Друкувати: Зберегти у файл

ОК Скасувати

У вікні «Сохранение» натиснути «ОК».

Пор. № зміни	Підпис відпов. особи	Дата внесення






Пор. № зміни	Підпис відпов. особи	Дата внесення

Введення ключових документів в дію (активація)

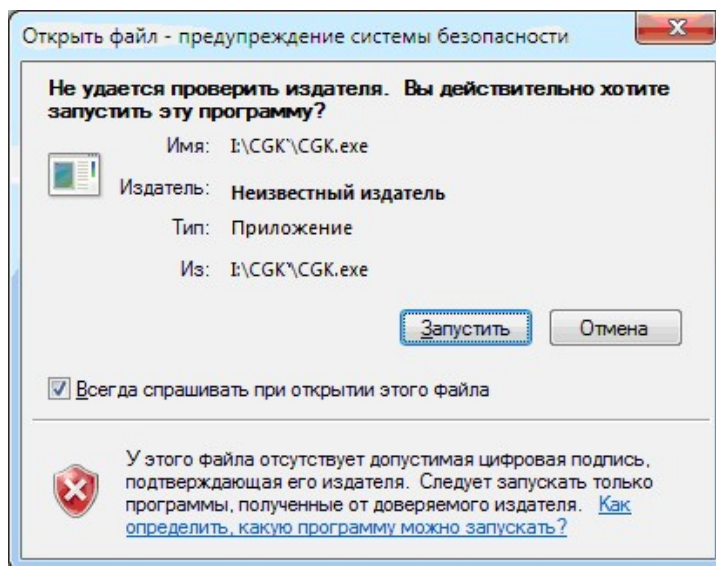
Ключові дані «Адміністратор» та «Користувач» обов'язково потрібно ввести в експлуатацію (активізувати).

Важливо: Тільки після активації такі ключові дані будуть сприйматися системою.

Для активації ключових даних та сертифікатів відкритих ключів «Користувача» або «Адміністратора» необхідно запустити виконуючий файл CGK.exe через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої кнопки миші.

	CGK.bin	29.09.2017 17:02	Файл "BIN"	1 КБ
	CGK.exe	29.09.2017 16:48	Приложение	3 822 КБ
	CGK.ini	13.05.2016 15:50	Параметры конф...	1 КБ

У вікні попередження системи безпеки ОС необхідно натиснути кнопку «Запустити».



Після запуску на екрані з'явиться вікно «Центр генерації ключів» у якому необхідно обрати вкладку «Сертифікати».

Сертифікати

Для активації ключових даних та сертифіката відкритого ключа необхідно обрати сертифікат відкритого ключа з переліку та натиснути лівою кнопкою миші на кнопку «Властивості...» або обрати в контекстному меню пункт «Властивості сертифікату».

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"
Файл Дії Допомога

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Сформований	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Сформований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"
Файл Дії Допомога

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Сформований	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Сформований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...


У вікні «Сертифікат» необхідно натиснути кнопку «Активізувати».

Пор. № зміни	Підпис відпов. особи	Дата внесення

Поле	Значення
Загальні	
Серійний №	2
Статус	Сформований
Дата початку дії	12.10.2017 11:49:12
Дата завершення дії	12.10.2018 11:49:12
Ідентифікатор ключа	d3b7f6d2cd66d544667ddf5f098e45b5cee2b
Ідентифікатор ключа ЦПК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	2
Назва	Центральний шлюз
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки

Зміна статусу

Для підтвердження дій з активації сертифіката відкритого ключа та ключових даних необхідно натиснути кнопку «Так» або кнопку «Ні» для відхилення такої операції.

Підтвердження	
 Активізувати сертифікат?	
<input checked="" type="button" value="Так"/>	<input type="button" value="Ні"/>

Про факт успішної активації сертифіката відкритого ключа свідчить зміна статусу «Активний» у полі «Статус».

Пор. № зміни	Підпис відпов. особи	Дата внесення

Сертифікат

Поле	Значення
Загальні	
Серійний №	2
Статус	Активний
Дата початку дії	12.10.2017 11:49:12
Дата завершення дії	12.10.2018 11:49:12
Ідентифікатор ключа	d3b7f6d2cd66d544667ddf5f098e45b5cee2b
Ідентифікатор ключа ЦГК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	2
Назва	Центральний шлюз
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки

Зміна статусу

Блокувати

Активізувати

Скасувати

Закрити

В загальному списку сертифікатів викритих ключів у позиції «Статусу» буде відображено «активні», «скасовані», «сформовані», «блоковані» сертифікати відкритих ключів ключових даних.

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

Файл Дії Допомога

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Сформований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...

Важливо: Усі ключові дані, що використовуються в системі повинні бути активовані.

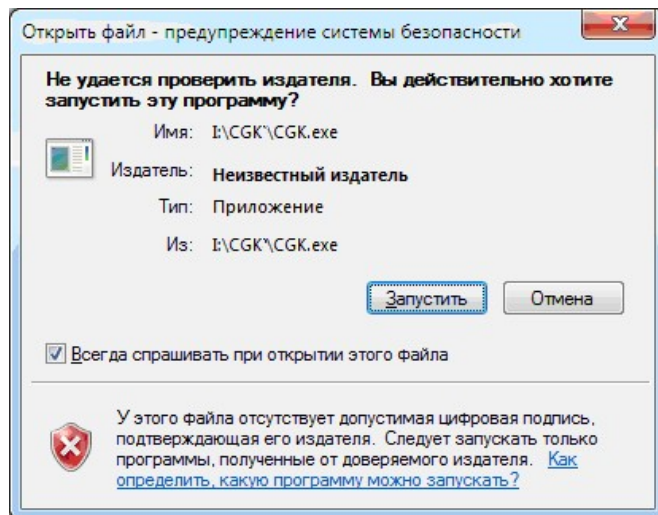
Пор. № зміни	Підпис відпов. особи	Дата внесення

Скасування / блокування сертифікатів відкритих ключів та ключових даних

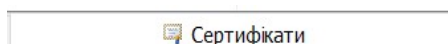
Для скасування сертифікатів відкритих ключів та ключових даних необхідно запустити виконуючий файл CGK.exe через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої кнопки миші.

	CGK.bin	29.09.2017 17:02	Файл "BIN"	1 КБ
	CGK.exe	29.09.2017 16:48	Приложение	3 822 КБ
	CGK.ini	13.05.2016 15:50	Параметры конф...	1 КБ

У вікні попередження системи безпеки ОС необхідно натиснути кнопку «Запустить».



Після запуску на екрані з'явиться вікно «Центр генерації ключів» у якому необхідно обрати вкладку «Сертифікати».



Для управління статусом сертифіката відкритого ключа та ключовими даними необхідно обрати сертифікат відкритого ключа з переліку та натиснути лівою кнопкою миші на кнопку «Властивості...» або обрати в контекстному меню пункт «Властивості сертифікату».

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Сформований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Сформований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...

У вікні «Сертифікат» необхідно перевірити серійний номер сертифіката відкритого ключа ключових даних, що підлягає зміні статусу та інформацію про власника.

Пор. № зміни	Підпис відпов. особи	Дата внесення

Поле	Значення
Загальні	
Серійний №	2
Статус	Сформований
Дата початку дії	12.10.2017 11:49:12
Дата завершення дії	12.10.2018 11:49:12
Ідентифікатор ключа	d3b7f6d2cd66d544667ddf5f098e45b5cee2b
Ідентифікатор ключа ЦГК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	2
Назва	Центральний шлюз
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки

Зміна статусу

Блокувати Активізувати Скасувати

Закрити

Для виконання зміни статусу сертифіката відкритого ключа ключових даних необхідно обрати кнопку:

	Кнопка «Скасувати» - використовується для виведення з експлуатації ключових даних без можливості відновлення (у випадку компрометації ключових даних або звільнення користувача).
	Кнопка «Блокувати» - використовується для виведення з експлуатації ключових даних з можливістю їх у подальшому відновлення (у випадку відпустки, відрядження, хвороби користувача).
	Кнопка «Активізувати» - використовується для вводу ключових даних у промислову експлуатацію.

З метою скасування сертифіката відкритого ключа ключових даних необхідно натиснути кнопку «Скасувати».

Пор. № зміни	Підпис відпов. особи	Дата внесення

Поле	Значення
Загальні	
Серійний №	3
Статус	Активний
Дата початку дії	12.10.2017 15:07:35
Дата завершення дії	12.10.2018 15:07:35
Ідентифікатор ключа	dfec6e405f77764167a658307ace2f1eab616
Ідентифікатор ключа ЦПК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	3
Назва	Центральний шлюз
Область	Київська
Місто	Київ
Організація	InfoSafe
Підрозділ	ІТ

Зміна статусу

Блокувати Поновити **Скасувати**

Закрити

У вікні «Підтвердження» необхідно натиснути кнопку «Так» для виконання або кнопку «Ні» для відхилення виконання операції скасування.

Підтвердження

Скасувати сертифікат?

☒ Так ☐ Ні

У вікні «Вкажіть причину скасування» необхідно обрати з переліку причин підставу для скасування сертифіката відкритого ключа ключових даних та натиснути кнопку «Ок» для виконання або кнопку «Скасувати» для відхилення виконання операції.

Вкажіть причину скасування

Причина скасування

☒ точно не визначено

☐ компрометація особистого ключа

☐ компрометація особистого ключа ЦПК

☐ зміна даних про підписувача

☐ сертифікат ключа замінений

ОК Скасувати

Про факт успішного скасування сертифіката відкритого ключа свідчить зміна статусу «Скасований» у вікні «Сертифікат».

Пор. № зміни	Підпис відпов. особи	Дата внесення

Сертифікат

Поле	Значення
Загальні	
Серійний №	3
Статус	Скасований
Дата початку дії	12.10.2017 15:07:35
Дата завершення дії	12.10.2018 15:07:35
Ідентифікатор ключа	dfec6e405f77764167a658307ace2f1eab616
Ідентифікатор ключа ЦГК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	3
Назва	Центральний шлюз
Область	Київська
Місто	Київ
Організація	InfoSafe
Підрозділ	ІТ

Зміна статусу

Блокувати Поновити Скасувати

Закрити

В загальному списку сертифікатів викритих ключів у позиції «Статусу» буде відображено «активні» та «скасовані» сертифікати відкритих ключів ключових даних.

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Скасований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...

Важливо: Після успішного скасування сертифіката відкритого ключа ключових даних обов'язково необхідно здійснити випуск списку відкликаних сертифікатів.

Для тимчасового призупинення терміну дії сертифіката відкритого ключа та призупинення використання ключових даних необхідно обрати сертифікат відкритого ключа з переліку та натиснути лівою кнопкою миші на кнопку «Властивості...» або обрати в контекстному меню пункт «Властивості сертифікату».

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Скасований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Скасований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...

У вікні «Сертифікат» необхідно перевірити серійний номер сертифіката відкритого ключа ключових даних, що підлягає зміні статусу та інформацію про власника.

Пор. № зміни	Підпис відпов. особи	Дата внесення

Сертифікат

Поле	Значення
Загальні	
Серійний №	2
Статус	Сформований
Дата початку дії	12. 10. 2017 11:49:12
Дата завершення дії	12. 10. 2018 11:49:12
Ідентифікатор ключа	d3b7f6d2cd66d544667ddf5f098e45b5cee2b
Ідентифікатор ключа ЦГК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	2
Назва	Центральний шлюз
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки

Зміна статусу

Блокувати

Активізувати

Скасувати

Закрити

Для виконання зміни статусу сертифіката відкритого ключа ключових даних необхідно обрати кнопку:

<div>Скасувати</div>	Кнопка «Скасувати» - використовується для виведення з експлуатації ключових даних без можливості відновлення (у випадку компрометації ключових даних або звільнення користувача).
<div>Блокувати</div>	Кнопка «Блокувати» - використовується для виведення з експлуатації ключових даних з можливістю їх у подальшому відновлення (у випадку відпустки, відрядження, хвороби користувача).


З метою тимчасового призупинення терміну дії сертифіката відкритого ключа ключових даних необхідно натиснути кнопку «Блокувати».

Пор. № зміни	Підпис відпов. особи	Дата внесення

Поле	Значення
Загальні	
Серійний №	2
Статус	Активний
Дата початку дії	12.10.2017 11:49:12
Дата завершення дії	12.10.2018 11:49:12
Ідентифікатор ключа	d3b7f6d2cd66d544667ddf5f098e45b5cee2b
Ідентифікатор ключа ЦГК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	2
Назва	Центральний шлюз
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки

Зміна статусу

У вікні «Підтвердження» необхідно натиснути кнопку «Так» для виконання або кнопку «Ні» для відхилення виконання операції блокування.

Підтвердження	
 Блокувати сертифікат?	
<input checked="" type="button" value="Так"/>	<input type="button" value="Ні"/>

Про факт успішного блокування сертифіката відкритого ключа свідчить зміна статусу «Блокований» у вікні «Сертифікат».

Пор. № зміни	Підпис відпов. особи	Дата внесення

Сертифікат

Поле	Значення
Загальні	
Серійний №	2
Статус	Блокований
Дата початку дії	12.10.2017 11:49:12
Дата завершення дії	12.10.2018 11:49:12
Ідентифікатор ключа	d3b7f6d2cd66d544667ddf5f098e45b5cee2b
Ідентифікатор ключа ЦГК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	2
Назва	Центральний шлюз
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки

Зміна статусу

Блокувати

Поновити

Скасувати

Закрити

В загальному списку сертифікатів викритих ключів у позиції «Статусу» буде відображено «активні», «блоковані» та «скасовані» сертифікати відкритих ключів ключових даних.

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Блокований	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Скасований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...

Важливо: Після успішного блокування сертифіката відкритого ключа ключових даних обов'язково необхідно здійснити випуск списку відкликаних сертифікатів.

Для поновлення терміну дії сертифіката відкритого ключа та поновлення використання ключових даних необхідно обрати блокований сертифікат відкритого ключа з переліку та натиснути лівою кнопкою миші на кнопку «Властивості...» або «Властивості сертифікату» в контекстному меню.

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Скасований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Скасований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...

У вікні «Сертифікат» необхідно перевірити серійний номер сертифіката відкритого ключа ключових даних, що підлягає зміні статусу та інформацію про власника.

Пор. № зміни	Підпис відпов. особи	Дата внесення

Сертифікат

Поле	Значення
Загальні	
Серійний №	2
Статус	Блокований
Дата початку дії	12. 10. 2017 11:49:12
Дата завершення дії	12. 10. 2018 11:49:12
Ідентифікатор ключа	d3b7f6d2cd66d544667ddf5f098e45b5cee2b
Ідентифікатор ключа ЦПК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	2
Назва	Центральний шлюз
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки

Зміна статусу

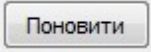
Блокувати

Поновити

Скасувати

Закрити

Для виконання зміни статусу сертифіката відкритого ключа ключових даних необхідно обрати кнопку:

	Кнопка «Поновити» - використовується для відновлення чинності (дії) раніше блокованих ключових даних
---	--


З метою поновлення терміну дії сертифіката відкритого ключа ключових даних необхідно натиснути кнопку «Поновити».

Пор. № зміни	Підпис відпов. особи	Дата внесення

Поле	Значення
Загальні	
Серійний №	2
Статус	Блокований
Дата початку дії	12.10.2017 11:49:12
Дата завершення дії	12.10.2018 11:49:12
Ідентифікатор ключа	d3b7f6d2cd66d544667ddf5f098e45b5cee2b
Ідентифікатор ключа ЦПК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	2
Назва	Центральний шлюз
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки

Зміна статусу

У вікні «Підтвердження» необхідно натиснути кнопку «Так» для виконання або кнопку «Ні» для відхилення виконання операції поновлення.

Підтвердження	
<div>  Активізувати сертифікат? </div>	
<input checked="" type="button" value="Так"/>	<input type="button" value="Ні"/>

Про факт поновлення дії сертифіката відкритого ключа свідчить зміна статусу «Активний» у вікні «Сертифікат».

Пор. № зміни	Підпис відпов. особи	Дата внесення

Сертифікат

Поле	Значення
Загальні	
Серійний №	2
Статус	Активний
Дата початку дії	12.10.2017 11:49:12
Дата завершення дії	12.10.2018 11:49:12
Ідентифікатор ключа	d3b7f6d2cd66d544667ddf5f098e45b5cee2b
Ідентифікатор ключа ЦГК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	2
Назва	Центральний шлюз
Область	Київська
Місто	Біла Церква
Організація	ITSEC
Підрозділ	Інформаційної безпеки

Зміна статусу

Блокувати

Поновити

Скасувати

Закрити

В загальному списку сертифікатів викритих ключів у позиції «Статусу» буде відображено «активні», «скасовані», «блоковані» сертифікати відкритих ключів ключових даних.

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

Файл Дії Допомога

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Скасований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...

Важливо: Після успішного поновлення сертифіката відкритого ключа ключових даних обов'язково необхідно здійснити випуск списку відкликаних сертифікатів.

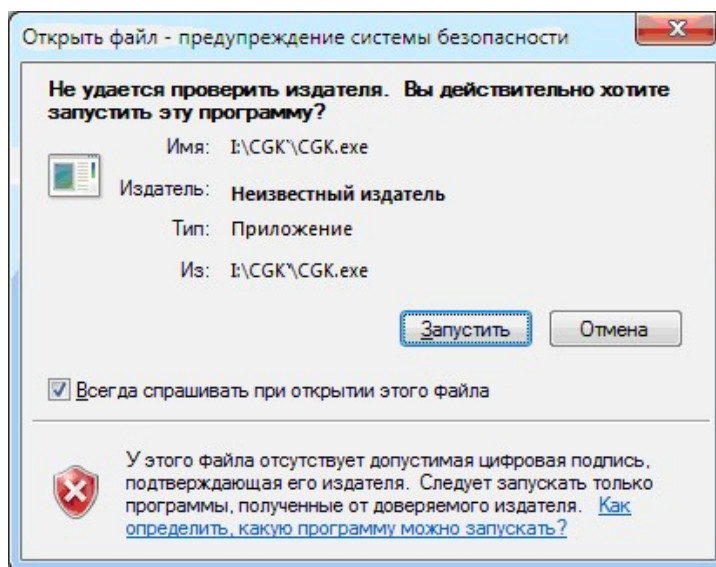
Пор. № зміни	Підпис відпов. особи	Дата внесення

Формування (випуск) списку відкликаних сертифікатів

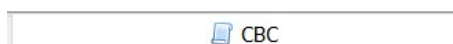
Для формування списку відкликаних сертифікатів необхідно запустити виконуючий файл CGK.exe через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої кнопки миші.

	CGK.bin	29.09.2017 17:02	Файл "BIN"	1 КБ
	CGK.exe	29.09.2017 16:48	Приложение	3 822 КБ
	CGK.ini	13.05.2016 15:50	Параметры конф...	1 КБ

У вікні попередження системи безпеки ОС необхідно натиснути кнопку «Запустить».



Після запуску на екрані з'явиться вікно «Центр генерації ключів» у якому необхідно обрати вкладку «СВС».



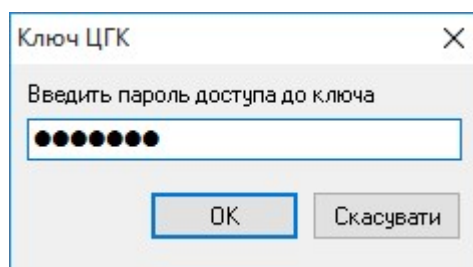
З метою формування списку відкликаних сертифікатів на вкладці «СВС» необхідно натиснути кнопку «Новий...».

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

Файл Дії Допомога



У вікні «Ключ ЦГК» необхідно зазначити пароль доступу до ключа ЦГК та натиснути кнопку «ОК» для виконання або кнопку «Скасувати» для відхилення виконання операції.



Пор. № зміни	Підпис відпов. особи	Дата внесення

НАСТАНОВА ОПЕРАТОРА. ВЕРСІЯ 1

Примітка: Пароль доступу до ключа ЦГК було Вами надруковано або збережено у текстовий файл в процесі формування ключа ЦГК.

Сертифікат

Серійний номер: 01

Ідентифікатор ключа:

1965e884aас63сsb42df6f3d77b2691c3440314dc5930613e2dd9a9059a9504a

Ідентифікатор ключа ЦСК:

1965e884aас63сsb42df6f3d77b2691c3440314dc5930613e2dd9a9059a9504a

Початок терміну дії: 12.10.2017 11:15:58

Завершення терміну дії: 12.10.2022 11:15:58

Відомості щодо власника

Серійний номер: 1

Назва: ROOT

Область: Київська

Місто: Київ

Організація: ІнфоБезпека

Підрозділ: IT-безпеки

Секретний ключ

Пароль *****

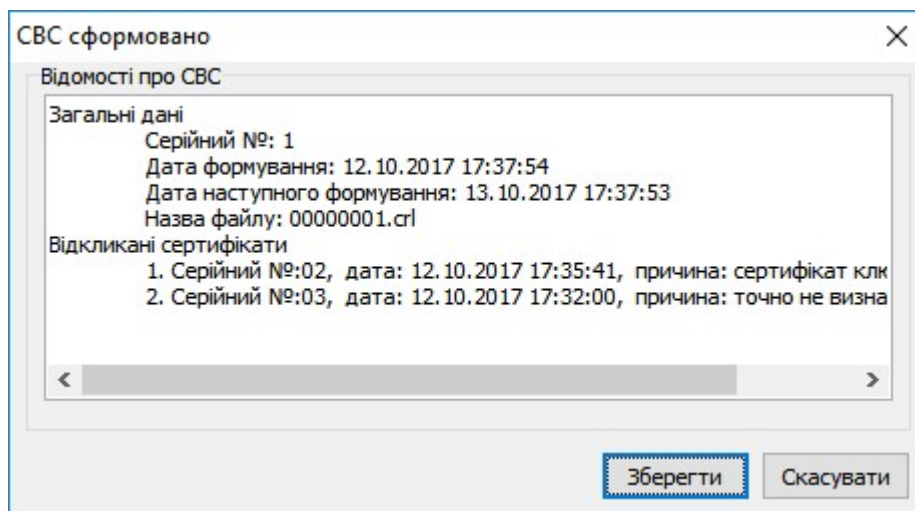
У вікні «Створення СВС» необхідно натиснути кнопку «ОК» для формування списку відкликаних сертифікатів або кнопку «Скасувати» для відхилення виконання такої операції.

Поле	Значення
Серійний №	00000001
Дата формування	12.10.2017 17:37:53
Дата наступного формування	13.10.2017 17:37:53
Назва файлу	00000001.crl

ОК Скасувати

У вікні «СВС сформовано» необхідно натиснути кнопку «Зберегти» для збереження сформованого списку відкликаних сертифікатів або кнопку «Скасувати» для відхилення виконання такої операції.

Пор. № зміни	Підпис відпов. особи	Дата внесення



В загальному списку CBC буде відображено сформований список відкликаних сертифікатів.

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

Файл Дії Допомога

№	Дата создания	Файл
2	12.10.2017 18:01:39	00000002.crl
1	12.10.2017 17:37:54	00000001.crl

Файл списку відкликаних сертифікатів зберігається у наступних каталогах (файл з розширенням *.crl):

\keys\admin\crl

\keys\user\crl

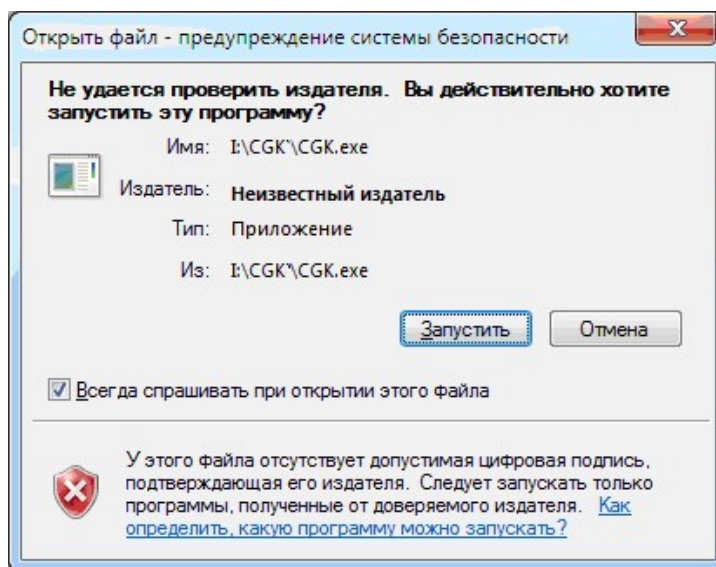
Пор. № зміни	Підпис відпов. особи	Дата внесення

Обробка запиту на сертифікат

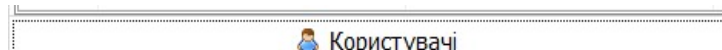
Для обробки запиту на сертифікат стандартизованого формату *.p10 необхідно запустити виконуючий файл CGK.exe через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої кнопки миші.

	CGK.bin	29.09.2017 17:02	Файл "BIN"	1 КБ
	CGK.exe	29.09.2017 16:48	Приложение	3 822 КБ
	CGK.ini	13.05.2016 15:50	Параметры конф...	1 КБ

У вікні попередження системи безпеки ОС необхідно натиснути кнопку «Запустити».



Після запуску на екрані з'явиться вікно «Центр генерації ключів» у якому необхідно обрати вкладку «Користувачі».



Оберіть користувача для якого бажаєте сформувати сертифікат та натисніть «Обробка запиту».

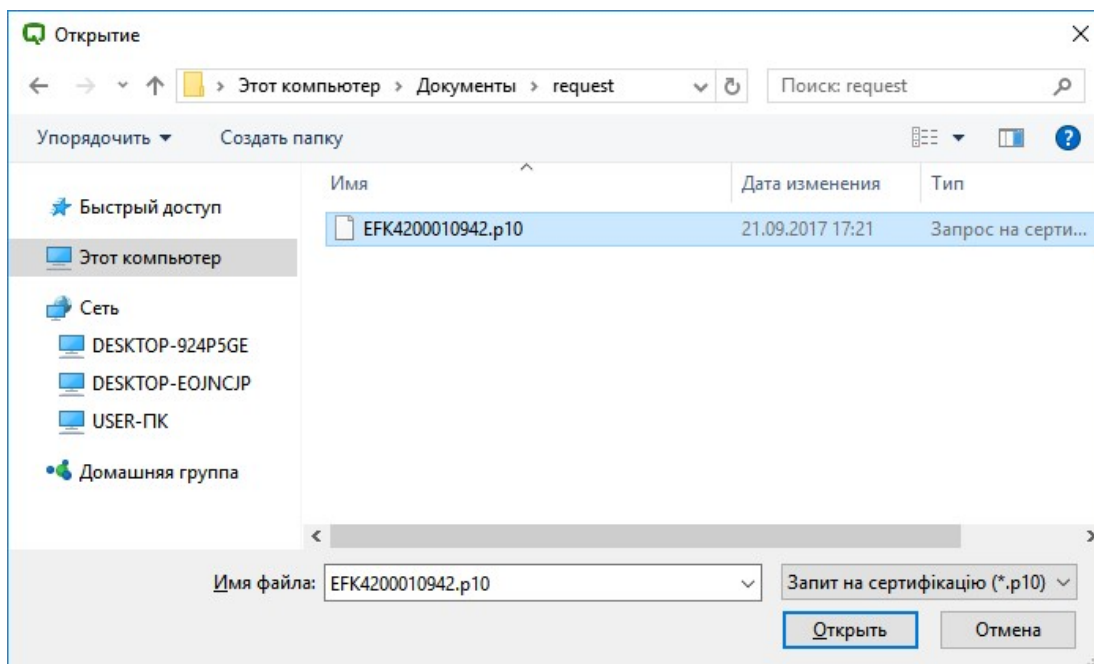
Комплекс програмний криптографічного захисту інформації "QUANT", "Центр генерації ключів"

Файл Дії Допомога

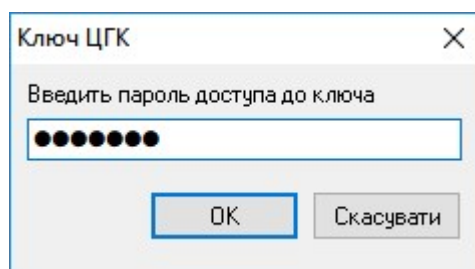
№	Серійний номер EfitKey	Обробка запиту...	Назва	Область	Місто	Організація	Підрозділ
1001			Центральний шлюз	Київська	Біла Церква	ITSEC	Інформаційної безпеки
1002			Центральний шлюз	Київська	Київ	InfoSafe	ІТ

У вікні, що відкрилось та зображене нижче, за допомогою файлового провідника перейдіть до каталогу, в якому збережено файл запиту. Оберіть файл та натисніть «Открьть».

Пор. № зміни	Підпис відпов. особи	Дата внесення



У вікні «Ключ ЦГК» необхідно зазначити пароль доступу до ключа ЦГК та натиснути кнопку «ОК» для виконання або кнопку «Скасувати» для відхилення виконання операції.



У вікні, що відкрилось та зображене нижче, перегляньте реквізити та за потреби змініть дату початку дії сертифіката та його термін дії. Після цього натисніть «ОК».

Поле	Значення
Власник	
Серійний №	1002
Назва	Центральний шлюз
Ім'я	
Прізвище	
Область	Київська
Місто	Київ
Організація	InfoSafe
Підрозділ	ІТ
Тип	Користувач
Серійний № EfitKey	
Сертифікат	
Серійний №	00000004
Дата початку дії	12.10.2017 18:09:37
Термін дії	12.10.2018 18:09:37

ОК Скасувати

Пор. № зміни	Підпис відпов. особи	Дата внесення

Після успішного створення сертифіката, перейдіть на вкладку «Сертифікати» для перегляду властивостей сертифіката.

 Сертифікати

Для перегляду властивостей сертифіката, оберіть його з переліку сертифікатів, натисканням лівої клавіші миші, та натисніть «Властивості», або натисніть правою клавішею миші та в контекстному меню оберіть «Властивості».

Комплекс програмний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

Файл Дії Допомога

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Скасований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Скасований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...
4	SN=1002 CN=Центральн...	Сформований	12.10.2017 18:09:37	12.10.2018 18:09:37	1965e884aac63ccb42df6f3d77b2691c344...
4	SN=1002 CN=Центральн...	Сформований	12.10.2017 18:09:37	12.10.2018 18:09:37	1965e884aac63ccb42df6f3d77b2691c344...

У вікні, що відкрилось і зображене нижче, перегляньте властивості сертифіката та за потреби блокуйте, активуйте чи скасуйте сертифікат.

Сертифікат

Поле	Значення
Загальні	
Серійний №	4
Статус	Сформований
Дата початку дії	12.10.2017 18:09:37
Дата завершення дії	12.10.2018 18:09:37
Ідентифікатор ключа	a012951b55fd746e0b776bb1bc2b36267a53
Ідентифікатор ключа ЦГК	1965e884aac63ccb42df6f3d77b2691c34403
Власник	
Серійний №	4
Назва	Центральний шлюз
Область	Київська
Місто	Київ
Організація	InfoSafe
Підрозділ	ІТ

Зміна статусу

Блокувати

Активізувати

Скасувати

Закрити

Для експорту сертифіката у файл формату *.crt оберіть сертифікат з переліку, натисніть правою клавішею миші та в контекстному меню натисніть «Експорт».

Пор. № зміни	Підпис відпов. особи	Дата внесення

Комплекс программний криптографічного захисту інформації "QUANT". "Центр генерації ключів"

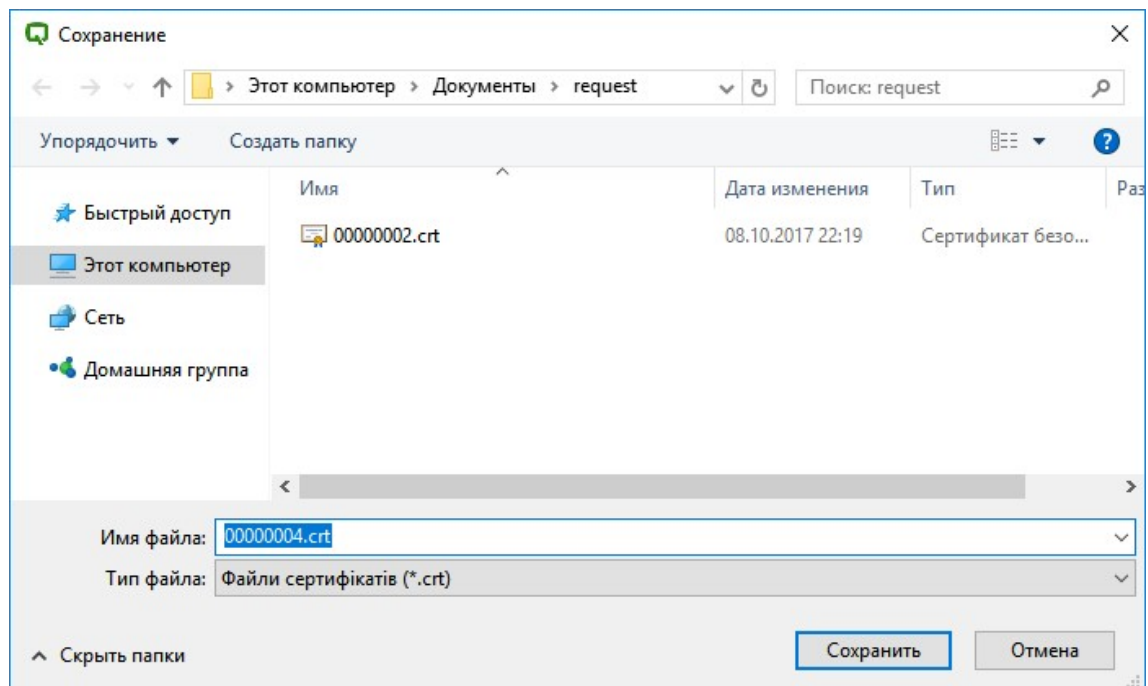
Файл Дії Допомога

№	Користувач / засіб	Статус	Початок дії	Завершення дії	Ключ ЦГК
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
2	SN=1001 CN=Центральн...	Активний	12.10.2017 11:49:12	12.10.2018 11:49:12	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Скасований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...
3	SN=1002 CN=Центральн...	Скасований	12.10.2017 15:07:35	12.10.2018 15:07:35	1965e884aac63ccb42df6f3d77b2691c344...
4	SN=1002 CN=Центральн...	Сформований	12.10.2017 18:09:37	12.10.2018 18:09:37	1965e884aac63ccb42df6f3d77b2691c344...

Властивості сертифікату

Експорт...

У вікні провідника, що відкрилось, змініть за потреби назву файлу та каталог для збереження.



Пор. № зміни	Підпис відпов. особи	Дата внесення

Формування запиту на сертифікацію в АЦСК

З метою формування запиту на сертифікацію відкритого ключа до АЦСК та отриманні від АЦСК посиленого сертифіката відкритого ключа необхідно у файлі налаштування CGK.ini встановити у секції [Common] параметр SavePCSK10 рівним значенню 0 (нуль)






Приклад:

[Common]

SavePCSK10=0

 CGK.bin	29.09.2017 17:02	Файл "BIN"	1 КБ
 CGK.exe	29.09.2017 16:48	Приложение	3 822 КБ
 CGK.ini	13.05.2016 15:50	Параметры конф...	1 КБ

Після формування ключових даних із встановленим параметром SavePCSK10=0 у каталог із ключовим документом буде збережено файл запиту із розширенням *.p10, який необхідно передати до АЦСК.

 1002.00000003.cnt	24.05.2016 16:57	Файл "CNT"	1 КБ
 1002.00000003.crt.txt	24.05.2016 16:57	Текстовый докум...	1 КБ
 1002.00000003.dke	24.05.2016 16:57	Файл "DKE"	1 КБ
 1002.00000003.p10	24.05.2016 16:57	Запрос на серти...	1 КБ
 CN.TXT	24.05.2016 16:57	Текстовый докум...	1 КБ

Пор. № зміни	Підпис відпов. особи	Дата внесення

Формування ключових даних сумісних із модулями «QUANT»

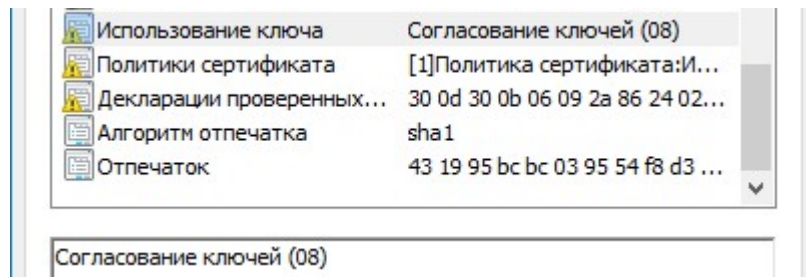
З метою формування ключових даних призначених для використання із модулями «Комплексу програмного криптографічного захисту інформації «QUANT» необхідно у файлі налаштування CGK.ini встановити у секції [Common] параметр KeyAgreement рівним значенню 1 (одиниці)

Приклад:

[Common]

KeyAgreement=1

Після формування ключових даних із встановленим параметром KeyAgreement=1 сертифікат відкритого ключа буде мати параметр використання «Узгодження ключів».



Пор. № зміни	Підпис відпов. особи	Дата внесення