Прим. №1

ПОГОДЖЕНО
Перший заступник Голови
Держспецзв'язку

_____ **О.Г. Цуркан**

«__15__» ____08_____2013 р.

ЗАТВЕРДЖУЮ
Директор
ТОВ «АВТОР»

_____ **В.В. Татьянін**

«__06__» ____08_____ 2013 р.

Засіб
електронного цифрового підпису
«CryptoLibV2»

ІНСТРУКЦІЯ
ЩОДО ПОРЯДКУ ГЕНЕРАЦІЇ КЛЮЧОВИХ ДАНИХ ТА ПОВОДЖЕННЯ З КЛЮЧОВИМИ ДОКУМЕНТАМИ

АЧСА.460709.007 Д10

РОЗРОБЛЕНО

Директор департаменту
ТОВ «АВТОР»

_____ **Д. І. Пархотик**

«__06__» ____08_____ 2013 р.

2013

АНОТАЦІЯ

Даний документ містить відомості про організаційно-технічні заходи по забезпеченню безпеки під час генерації ключових даних та правила поводження з ключовими документами засобу електронного цифрового підпису (ЕЦП) «CryptoLibV2».

Носіями ключових документів засобів ЕЦП «CryptoLibV2» є засоби криптографічного захисту інформації: мікропроцесорна картка «CryptoCard-337» (ТУ У 30.0-32248356-016:2011, експертний висновок ДССЗЗІ України №05/02/02-810 від 11.03.2013 р.), електронний ключ «SecureToken-337» (ТУ У 30.0-32248356-017:2011, експертний висновок ДССЗЗІ України №05/02/02-809 від 11.03.2013 р.) або інші засоби, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Засіб ЕЦП «CryptoLibV2» є засобом КЗІ і призначений для захисту конфіденційної інформації.

Засіб виконує функції постановки ЕЦП, перевірки ЕЦП та управління ключовими даними.

Даний документ може бути використаний для створення інструкції користувача по роботі з засобом КЗІ «CryptoLibV2» в конкретній системі.

1. Визначення термінів та скорочень

В даному документі використовуються терміни та скорочення у наступному значенні:

ЕЦП	Електронний цифровий підпис
ЦСК	Центр сертифікації ключів
КЗІ	Криптографічний захист інформації

2. Ключові документи

2.1 Засіб КЗІ «CryptoLibV2» використовує ключові документи двох типів:

2.1.1 ключові документи, які використовуються для накладання ЕЦП;

2.1.2 ключові документи, які використовуються для перевірки ЕЦП.

2.2 Ключові документи, які використовуються для накладання ЕЦП, зберігають особисті ключі користувача і розміщуються на носіях ключових даних: мікропроцесорна картка «CryptoCard-337», електронний ключ «SecureToken-337» або на інших засобах, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

2.3 Порядок генерації ключових даних та особливості поводження з ключовими документами, які використовуються для накладання ЕЦП, викладено в окремих інструкціях до відповідних засобів КЗІ.

2.4 Ключові документи, які використовуються для перевірки ЕЦП, зберігають один або декілька сертифікатів ЦСК і розміщуються на носіях ключових даних, файлах комп'ютерної системи або спеціалізованих сховищах сертифікатів.

3. Отримання засобів КЗІ

3.1 Порядок отримання засобів КЗІ, які використовуються для накладання ЕЦП, викладено в окремих інструкціях до відповідних засобів КЗІ.

3.2 Сертифікати ЦСК мають бути доставлені користувачеві у спосіб, який виключає їх модифікацію.

4. Генерація ключів

4.1 Користувач має змогу згенерувати особистий ключ ЕЦП за допомогою сервісного або прикладного програмного забезпечення, визначеного правилами системи, в якій застосовуються дані засоби.

4.2 Порядок генерації особистого ключа ЕЦП викладено в окремих інструкціях до відповідних засобів КЗІ.

4.3 Сертифікати ЦСК не генеруються даним засобом КЗІ.

5. Використання ключових документів

5.1 Користувач несе персональну відповідальність за зберігання носія ключових документів.

5.2 Користувач повинен не допускати використання засобу КЗІ іншими особами, що не мають відповідних повноважень.

5.3 Порядок використання особистого ключа ЕЦП викладено в окремих інструкціях до відповідних засобів КЗІ.

5.4 Сертифікати використовуються засобом КЗІ «CryptoLibV2» автоматично. Сертифікати ЦСК не є конфіденційними, але потребують заходів, що унеможливлюють їх навмисне пошкодження або несанкціоновану зміну кількості сертифікатів у сховищі.

6. Знищення ключових даних

6.1 Знищення поточного ключа під час переходу до використання нового особистого ключа, виконується за командою прикладного програмного забезпечення.

6.2 Порядок знищення особистого ключа ЕЦП викладено в окремих інструкціях до відповідних засобів КЗІ.

6.3 Сертифікати ЦСК не потрібують знищення після закінчення строку їх дії.

6.4 У разі компрометації ключів ЦСК, відповідний сертифікат має бути видалено із сховища сертифікатів, або перенесено у список заблокованих сертифікатів.