Прим.№1

ПОГОДЖЕНО
Перший заступник Голови
Держспецзв'язку

_____ **О.Г. Цуркан**

«15» 05 2013 р.

ЗАТВЕРДЖУЮ
Директор
ТОВ «АВТОР»

_____ **В.В. Татьянін**

«06» 05 2013 р.

Засіб
електронного цифрового підпису
«CryptoLibV2»

ІНСТРУКЦІЯ
ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕКСПЛУАТАЦІЇ

АЧСА.460709.007 И9

РОЗРОБЛЕНО

Директор департаменту
ТОВ «АВТОР»

_____ **Д. І. Пархотик**

«06» 05 2013 р.

2013

АЧСА.460709. 007 Д10

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.

Криптографічні алгоритми, що є державними стандартами України використовуються для захисту конфіденційної інформації.

Алгоритми: PKCS#1 v2.1 RSA Cryptography Standard, ISO/IEC 10116:2006 (алгоритми DES, TDES, AES), PKCS#1 v2.1 RSA Cryptography Standard, ГОСТ 34.311-95 можуть використовуватися виключно для міжнародного обміну, а також в банківський системі України, за погодженням Національного банку України.

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. Обов'язки осіб, відповідальних за забезпечення безпеки експлуатації засобів КЗІ

2.1 Ініціалізація засобів КЗІ.

2.2 Контроль за виконанням процедур введення в експлуатацію засобів КЗІ.

2.3 Контроль за виконанням процедур знищення ключових даних засобів КЗІ.

2.4 Проведення службового розслідування у разі виникнення позаштатних ситуацій під час ініціалізації засобів КЗІ, генерації або використання ключових даних.

2.5 Видалення сертифікатів ЦСК у разі компрометації ключів ЦСК.

2.6 Контроль за цілісністю операційного середовища.

3. Обов'язки користувачів засобів КЗІ

3.1 Генерація ключових даних.

3.2 Перехід на використання нових ключових даних.

3.3 Знищення ключових даних.

3.4 Використовувати засіб КЗІ виключно за призначенням.

3.5 Зберігання значення кодів доступу до засобу КЗІ у таємниці.

3.6 Зберігання значення кодів розблокування засобу КЗІ у таємниці.

3.7 Періодична зміна, або в разі потреби, коду доступу до засобу КЗІ.

3.8 Не допускання зберігання разом засобів КЗІ та кодів доступу до них.

3.9 Не допускання використання засобу КЗІ іншими особами, що не мають відповідних повноважень.

3.10 У разі, якщо засіб КЗІ був загублений, або іншій підозрі щодо компрометації особистого ключа, негайно сповістити особу, відповідальну за забезпечення безпеки.

3.11 У разі блокування засобу КЗІ негайно сповістити особу, відповідальну за забезпечення безпеки.

3.12 У разі виявлення порушення роботи засобу КЗІ негайно сповістити особу, відповідальну за забезпечення безпеки.

3.13 Виконувати інші положення інструкції щодо поводження з ключовими документами.

4. Забезпечення безпеки засобу КЗІ під час його вводу в експлуатацію

4.1 Програмне забезпечення засобу КЗІ «CryptoLibV2» повинно бути отримано із надійного джерела.

4.2 Перед встановленням на комп'ютерну систему користувача, рекомендовано виконати перевірку цілісності засобу наступним чином:

4.2.1 Перевірити цілісність утиліти CheckCryptoLibPackage.exe, яка входить до комплекту засобу, за електронним цифровим підписом файлу. Підпис повинен бути дійсним. Постачальник файлу повинен бути «AVTOR Ltd.».

4.2.2 Для перевірки цілісності утиліти CheckCryptoLibPackage.exe скористайтесь пунктом меню «Свойства», вкладка «Цифрові Підписи».

4.2.3 Якщо цілісність утиліти перевірено успішно, запустить утиліту.

4.2.4 Утиліта відображає список знайдених та перевірених компонент.

4.3 Забороняється використання засобу КЗІ, якщо під час перевірки було отримане повідомлення про пошкодження будь якого з компонентів засобу.

4.4 При необхідності, перевірку цілісності засобу можливо повторити в будь-який час після встановлення.

4.5 Сертифікати ЦСК мають бути доставлені користувачеві у спосіб, який виключає їх модифікацію. Спосіб доставки і перевірки сертифікатів визначається ЦСК.

4.6 Якщо для збереження сертифікатів ЦСК використовується папка файлового сховища комп'ютерної системи, доступ на запис в папку повинен бути обмежений.

4.7 Перевірити точність налаштування часу комп'ютерної системи.

4.8 Введення в експлуатацію носіїв особистих ключів підпису користувачів викладено в окремих інструкціях до відповідних засобів КЗІ.

5. Забезпечення безпеки засобу КЗІ під час його виведення з експлуатації

5.1 Якщо засіб КЗІ більше не буде використовуватись, або засіб має бути використаний в інший системі, слід знищити ключові дані наступним чином:

5.1.1 Виконайте знищення особистих ключів користувачів за допомогою прикладного програмного забезпечення. Докладніше, правила виведення з експлуатації носіїв особистих ключів підпису користувачів викладено в окремих інструкціях до відповідних засобів КЗІ.

6. Забезпечення безпеки засобу КЗІ у разі порушення функціонування

6.1 Використовувати за призначенням засіб КЗІ, який має ознаки порушення функціонування, заборонено.

6.2 Перед зверненням до сервісу рекомендовано самостійно вжити заходи щодо поновлення функціонування засобу КЗІ наступним чином:

– виконати перевірку складу та цілісності компонентів засобу КЗІ «CryptoLibV2» за допомогою утиліти CheckCryptoLibPackage.exe.

Якщо необхідні компоненти засобу відсутні або пошкоджені, сповістить особу, відповідальну за забезпечення безпеки;

– програмні компоненти засобу КЗІ можуть бути встановлено повторно без втрати особистих ключів користувача;

– виконати перевірку правильності налаштування часу комп'ютерної системи;

– виконати інші заходи, викладені в інструкції до носія особистих ключів користувача.

6.3 Забороняється передавати до сервісної організації значення кодів доступу або коду розблокування носіїв особистих ключів.

6.4 Якщо немає впевненості, що коди доступу засобу змінені, поточні ключі користувача мають бути скасовані, сертифікат відкликаний. Після цього засіб КЗІ може бути переданий до сервісної організації.

6.5 Після проведення сервісного обслуговування комп'ютерної системи з встановленим засобом КЗІ необхідно перевірити цілісність компонентів засобу та перевірити цілісність сертифікатів ЦСК.

6.6 Цей порядок може бути змінений за погодженням із розробником засобу КЗІ.

7. Тестування засобів КЗІ та їх резервування в системі

7.1 Перевірку складу та цілісності компонентів засобу КЗІ «CryptoLibV2» можливо виконати за допомогою утиліти CheckCryptoLibPackage.exe (Див. пункт 4.2).

7.2 Резервування програмних компонент засобу КЗІ не відрізняється від резервування іншого програмного забезпечення. Після відновлення засобу КЗІ рекомендовано перевірити цілісність за допомогою утиліти CheckCryptoLibPackage.exe.

7.3 Порядок тестування і резервування носіїв особистих ключів підпису користувачів викладено в окремих інструкціях до відповідних засобів КЗІ.

8. Дії персоналу в умовах надзвичайних ситуацій, стихійного лиха та підозри компрометації ключів

8.1 У разі надзвичайних ситуацій засоби КЗІ можливо залишати в місці їх звичайного використання при умові зберігання кодів доступу у таємниці.

8.2 Якщо використовуються змінні носії особистих ключів, рекомендовано від'єднати носій від комп'ютерної системи.

8.3 Рекомендовано завершити роботу програмного забезпечення, яке використовує носії особистих ключів, або від'єднати електроживлення комп'ютерної системи.

8.4 Інші особливості дій персоналу відносно поводження з носіями особистих ключів викладено в окремих інструкціях до відповідних засобів КЗІ.

9. Порядок проведення контролю за станом забезпечення безпеки засобів КЗІ

9.1 Визначається правилами безпеки системи, що використовує засоби КЗІ.

10. Порядок допуску в приміщення, в яких встановлені засоби КЗІ

10.1 Порядок доступу визначається носіями особистих ключів, що застосовуються та наводиться в окремих інструкціях до відповідних засобів КЗІ.