Прим. №1

ПОГОДЖЕНО
Перший заступник Голови
Держспецзв'язку

_____ **О.Г. Цуркан**

«15» 05 **2013 р.**

ЗАТВЕРДЖУЮ
Директор
ТОВ «АВТОР»

_____ **В.В. Татьянін**

«___» _____ **2013 р.**

ПТК АЦСК «CryptoKDC»

ІНСТРУКЦІЯ
ЩОДО ПОРЯДКУ ГЕНЕРАЦІЇ КЛЮЧОВИХ ДАНИХ ТА ПОВОДЖЕННЯ З КЛЮЧОВИМИ ДОКУМЕНТАМИ

АЧСА.466459.010 Д10

РОЗРОБЛЕНО

Директор департаменту
ТОВ «АВТОР»

_____ **Д. І. Пархотик**

«12» 05 **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 комплексу програмно-технічних засобів, які виконують регламентні процедури та функції щодо генерації власних ключів АЦСК та ключів користувачів, керування сертифікатами та користувачами, ведення реєстрів користувачів, сертифікатів, запитів, надання послуги фіксування часу та отримання статусу сертифікатів в режимі реального часу тощо.

ПТК «АЦСК CryptoKDC», в цілому, відноситься до програмних засобів криптографічного захисту інформації (КЗІ) виду Б, категорії «К», класу Б2. Окремі засоби, що входять до його складу та керуються ПТК, відносяться до типів програмних засобів КЗІ, категорії «К», «Ш», «П», «Р» класу Б2 або нижче, відповідно до «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації», затвердженого наказом від 20.07.2007 №141 Адміністрації ДССЗЗІ України.

ПТК «АЦСК CryptoKDC» призначений для оброблення інформації з обмеженим доступом (крім службової та інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом.

В якості носіїв ключових даних ПТК «АЦСК CryptoKDC» використовуються наступні засоби КЗІ:

- мікропроцесорна картка «CryptoCard-337» (ТУ У 30.0-32248356-016:2011, експертний висновок ДССЗЗІ України №05/02/02-810 від 11.03.2013 р.);
- мікропроцесорна картка «CryptoCard-318» (АЧСА.467649.028, експертний висновок ДССЗЗІ України № 5/1-8324 від 30.12.2009 р.);

- електронний ключ «Secure Token-337» (ТУ У 30.0-32248356-017:2011, експертний висновок ДССЗЗІ України №05/02/02-809 від 11.03.2013 р.);
- електронний ключ «Secure Token-318» (АЧСА.467369.004, експертний висновок ДССЗЗІ України № 5/1-8325 від 30.12.2009 р.);
- апаратно-програмні модулі захисту (HSM) «CryptoLine 3x8» (ТУ У 30.0-32248356-005:2006, експертний висновок ДССЗЗІ України № 5/1-8323 від 30.12.2009 р.).

Даний документ може бути використаний для створення інструкції користувача по роботі з апаратними засобами КЗІ зі складу ПТК «АЦСК CryptoKDC»: мікропроцесорними картками «CryptoCard-318» з операційною системою (ОС) «УкрКОС 2.0», мікропроцесорними картками «CryptoCard-337» з ОС «УкрКОС v.3.0», електронними ключами «Secure Token-318» з ОС «УкрКОС 2.0», електронними ключами «Secure Token-337» з ОС «УкрКОС v.3.0», апаратно-програмними модулями захисту (HSM) «CryptoLine 3x8», в конкретній системі.

Відповідальними особами (обслуговуючим персоналом) ПТК «АЦСК CryptoKDC» можуть бути:

- адміністратор безпеки;
- адміністратор реєстрації;
- адміністратор сертифікації;
- системний адміністратор.

1. Визначення термінів та скорочень

В даному документі використовуються терміни та скорочення у наступному значенні:

АЦСК	Акредитований центр сертифікації ключів
ПТК	Програмно-технічний комплекс
ЕЦП	Електронний цифровий підпис
ПІН	Персональний ідентифікаційний номер
КЗІ	Криптографічний захист інформації
АРМ	Автоматизоване робоче місце
ОС	Операційна система

2. Ключовий документ

2.1 Ключовий документ - носій ключових даних. Ключовим документом, або апаратним засобом, КЗІ ПТК «АЦСК CryptoKDC» можуть виступати:

- мікропроцесорні картки «CryptoCard-318» з ОС «УкрКОС 2.0»;
- мікропроцесорні картки «CryptoCard-337» з ОС «УкрКОС v.3.0»;
- електронні ключі «Secure Token-318» з ОС «УкрКОС 2.0»;
- електронні ключі «Secure Token-337» з ОС «УкрКОС v.3.0»;
- апаратно-програмні модулі захисту (HSM) «CryptoLine 328»;
- апаратно-програмні модулі захисту (HSM) «CryptoLine 358»,

які є ініціалізованими засобами в цілому.

2.2 До складу ключових даних входять:

- особистий ключ ЕЦП;
- відкритий ключ ЕЦП;
- ПІН-код

- код розблокування
- ключі захисту процесу резервування та обміну даними

2.3 Ключові дані окрім відкритого ключа ЕЦП не можуть бути зчитаними через зовнішній інтерфейс ключового документа.

3. Ініціалізація ключових документів

3.1 Ініціалізація ключового документа виконується у Центрі ініціалізації ПТК «АЦСК CryptoKDC» відповідно до положень наведених в документі «Программно-технический комплекс центра сертификации ключей «CryptoKDC». Центр инициализации. Описание применения» АЧСА. 32248356.00086 01 33 01.

3.2 Під час ініціалізації записуються наступні дані:

- початковій ПІН-код та коди розблокування носія ключових даних;
- додаткові ключові дані, якщо це передбачено системою (наприклад, ключі захисту процесу резервування та обміну даними);
- допоміжні дані;
- код розблокування;
- ключі захисту процесу резервування та обміну даними.

3.3 Кожен носій ключових даних має унікальний серійний номер, за яким здійснюється облік у Центрі ініціалізації ПТК «АЦСК CryptoKDC».

4. Отримання ключових документів

4.1 Ініціалізований носій ключових даних та початковий ПІН-код доставляються користувачеві.

4.2 Отримання ключового документу користувачем повинно бути зареєстровано в журналі.

4.3 Якщо для первинної ідентифікації користувача використовується тільки тимчасовий (стартовий) сертифікат, початковий ПІН-код повинен передаватися користувачеві тільки після отримання носія ключових даних.

4.4 Користувач повинен змінити початковий ПІН-код носія ключових даних та код розблокування, якщо такий використовується.

4.5 Рекомендована довжина ПІН-кодів має становити не менш ніж 4 символи.

4.6 Користувач повинен згенерувати особистий та відкритий ключ ЕЦП (див. розділ 5. Генерація нового особистого ключа).

5. Генерація нового особистого ключа

5.1 Користувач генерує особистий ключ ЕЦП за допомогою сервісного або прикладного програмного забезпечення, визначеного правилами ПТК «АЦСК CryptoKDC», в якому застосовуються визначені в даній інструкції носії ключових даних відповідно до положень наведених в документах:

- «Программно-технический комплекс центра сертификации ключей «CryptoKDC». Центр сертификации ключей. Описание применения» АЧСА. 32248356.00088 01 33 01;
- «Программно-технический комплекс центра сертификации ключей «CryptoKDC». Центр сертификации ключей. Руководство оператора» АЧСА. 32248356.00088 01 34 01.

5.2 Строк дії ключових даних визначається регламентом роботи АЦСК, але не може перевищувати встановлений нормативно-правовими документами України термін.

5.3 Операція генерації особистого ключа потребує знання ПІН-коду носія ключових даних.

5.4 Користувач повинен відправити запит на сертифікацію особистого ключа способом, передбаченим ПТК «АЦСК CryptoKDC», в якому застосовуються дані носії ключових даних.

5.5 Дублювання ключових даних можливе лише для ключових документів, які були ініціалізовані з відповідними ключами захисту процесу резервування та обміну даними.

5.6 Дублювання особистого ключа здійснюється одразу після генерації ключа за допомогою утиліт «CSPKeyUtil» (мікропроцесорні картки «CryptoCard-337» та електронні ключі «Secure Token-337»), «CL3x8Service» (апаратно-програмні модулі захисту (HSM) «CryptoLine 328» та «CryptoLine 358»). Дублювання особистого ключа для карток мікропроцесорних «CryptoCard-318» та електронних ключів «Secure Token-318» не можливе.

6. Використання ключових документів

6.1 Користувач несе персональну відповідальність за зберігання носія ключових даних. Рекомендовано зберігати носії ключових даних у сейфі.

6.2 Користувач повинен не допускати використання носіїв ключових даних іншими особами, що не мають відповідних повноважень.

6.3 Користувач повинен зберігати значення ПІН-коду доступу до ключових документів та значення коду їх розблокування у таємниці. Рекомендовано запам'ятати ПІН-код та не записувати його.

6.4 Забороняється зберігати носії ключових даних та ПІН-коди до них в одному місці.

6.5 Користувач повинен періодично, відповідно до встановленого адміністратором безпеки терміну, або в разі потреби (наприклад, при підозрі, що ПІН-код став відомим іншім особам), змінювати ПІН-код доступу до ключових документів.

6.6 Користувач повинен використовувати носії ключових даних виключно за призначенням.

6.7 У разі, якщо носій ключових даних було загублено, або у випадку іншої підозри щодо компрометації особистого ключа, необхідно негайно сповістити адміністратора безпеки ПТК «АЦСК CryptoKDC».

6.8 Операція постановки ЕЦП потребує знання ПІН-коду носія ключових даних.

7. Робота з ПІН-кодами носіїв ключових даних

7.1 Більшість операцій з носієм ключових даних потребує введення ПІН-коду.

7.2 Вводити ПІН-код дозволяється тільки у випадках, якщо користувач дійсно ініціював роботу з носієм ключових даних.

7.3 Зміна ПІН-коду виконується за допомогою сервісних утиліт, що постачаються розробником носія ключових даних.

7.4 Кількість спроб введення помилкового ПІН-коду є обмеженою і фіксується лічильником. При перевищенні допустимої кількості спроб носій ключових даних блокується.

7.5 У разі блокування носія ключових даних можливе застосування наступних механізмів розблокування:

- за допомогою коду розблокування;
- механізму «запит/відповідь».

7.6 Розблокування носія ключових даних може бути заборонено згідно з регламентом роботи АЦСК.

7.7 Якщо причину блокування не виявлено, користувач повинен негайно сповістити адміністратора безпеки ПТК «АЦСК CryptoKDC».

8. Знищення ключових даних

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

8.2 Ключові дані повинні бути знищені у наступних випадках:

- планова заміна ключів;
- зміна реквізитів користувача;

- компрометація ключів;
- вихід з ладу носіїв ключових даних;
- закінчення повноважень користувача.

8.3 У разі необхідності ключові дані повинні бути знищені одним із наступних способів:

- знищення за допомогою сервісних утиліт;
- генерація нового ключа замість поточного;
- повторна ініціалізація носіїв ключових даних;
- блокування ПІН-коду та коду розблокування носія ключових даних;
- механічне пошкодження носія ключових даних.

8.4 Навмисне знищення ключових даних носія повинно бути зареєстровано в журналі.

8.5 Для ключових документів, які спроможні мати одночасно більше одного дійсного особистого ключа (мікропроцесорні картки «CryptoCard-337» та електронні ключі «Secure Token-337»), при знищенні рівно одного з особистих ключів, повинен застосовуватись механізм знищення за допомогою сервісної утиліти «CSPKeyUtil».