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
ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕКСПЛУАТАЦІЇ

АЧСА.466459.010 И9

РОЗРОБЛЕНО

Директор департаменту
ТОВ «АВТОР»
_____ Д. І. Пархотик
«10» 04 2013 р.

2013

ЗМІСТ

АНОТАЦІЯ

Даний документ містить відомості про організаційно-технічні заходи по забезпеченню безпеки експлуатації 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 до захисту якої встановлена законом.

ПТК «АЦСК CryptoKDC» призначений для керування ключами електронного цифрового підпису та протоколів погодження ключів шифрування користувачів, реєстраційними даними користувачів, носіями ключової інформації та сертифікатами відкритих ключів (формування, поновлення, блокування та скасування сертифікатів відкритих ключів, розповсюдження сертифікатів, надання інформації про статус сертифікатів). ПТК має використовуватись в організаціях будь-якої форми власності для побудови інфраструктури відкритих ключів та її використання в прикладних системах.

ПТК «АЦСК CryptoKDC» складається з апаратної та програмної частин.

Апаратна частина в ПТК АЦСК може складатися з наступних засобів КЗІ[1] (використання в якості носіїв ключової інформації для виконання криптографічних перетворень та/або роботи із форматами даних), які мають позитивний експертний висновок за результатами державної експертизи у сфері 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.).

До складу програмної частини ПТК «АЦСК CryptoKDC» можуть входити:

- програмне забезпечення (ПЗ) серверних додатків у складі:
  - ПЗ ЦСК-сервер;
  - ПЗ OCSP-сервер;
  - ПЗ TSP-сервер;
  - ПЗ WEB-сервер;
- клієнтські додатки;
- засоби ЕЦП «CryptoLibV2»;
- допоміжне програмне забезпечення (ДПЗ), до якого можуть входити компоненти, склад яких може змінюватись під час експлуатації ПТК «АЦСК CryptoKDC». Склад ДПЗ визначається відповідно до договору на поставку.

1 – для виконання криптографічних перетворень та/або роботи із форматами даних в ПТК АЦСК можуть бути задіяні інші засоби КЗІ, що мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту.

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
TSP	Time Stamp (позначка часу)
OCSP	Online Certificate Status Protocol (Онлайновий протокол визначення статусу сертифікату)
СВС	Список відкликаних сертифікатів
ІТС	Інформаційно-телекомунікаційна система
НКІ	Носій ключової інформації
ПІН	Персональний ідентифікаційний номер
КЗІ	Криптографічний захист інформації
СЗІ	Система захисту інформації
АРМ	Автоматизоване робоче місце
НСД	Несанкціонований доступ
Ключові дані (ключ)	Конкретний стан деяких параметрів криптографічного алгоритму, які забезпечують вибір одного криптографічного перетворення із сукупності усіх можливих для цього криптографічного алгоритму

Ключовий документ	Матеріальний носій із зафіксованими відповідним чином ключовими даними
Службовий ключовий документ	Матеріальний носій із зафіксованими відповідним чином особистими ключами АЦСК та його сервісів
Апаратні засоби КЗІ	мікропроцесорна картка «CryptoCard-337»; мікропроцесорна картка «CryptoCard-318»; електронний ключ «Secure Token-337»; електронний ключ «Secure Token-318»; апаратно-програмні модулі захисту (HSM) «CryptoLine 3x8»
ПІН-код доступу	Персональний ідентифікаційний номер доступу до носія ключових даних
ПІН-код розблокування	Персональний ідентифікаційний номер розблокування носія ключових даних
Гаряче резервування	Резервування даних в режимі реального часу

2. Права та обов'язки осіб, відповідальних за забезпечення безпеки експлуатації ПТК «АЦСК CryptoKDC»

Відповідальні особи (адміністратори безпеки), які відповідають за забезпечення безпеки експлуатації ПТК «АЦСК CryptoKDC» зобов'язані:

- організовувати проектування, розроблення, експлуатацію, обслуговування та модернізацію СЗІ ПТК «АЦСК CryptoKDC»;
- забезпечувати створення резервних копій сертифікатів, СВС та журналів аудиту ПТК «АЦСК CryptoKDC» та їх зберігання;
- своєчасно реагувати на спроби несанкціонованого доступу до ресурсів ПТК «АЦСК CryptoKDC», порушення правил експлуатації апаратних та програмних засобів захисту інформації;

- організовувати розмежування доступу до ресурсів ПТК «АЦСК CryptoKDC», зокрема розподілення між обслуговуючим персоналом паролів, ключів, сертифікатів тощо;
- знати перелік та призначення усіх апаратних та програмних засобів зі складу ПТК «АЦСК CryptoKDC»;
- забезпечувати суворе виконання вимог щодо забезпечення безпеки інформації при організації технічного обслуговування апаратних та програмних засобів і передачі їх у ремонт;
- забезпечувати ініціалізацію апаратних засобів КЗІ зі складу ПТК «АЦСК CryptoKDC»;
- забезпечувати контроль за виконанням процедур введення в експлуатацію апаратних та програмних засобів КЗІ зі складу ПТК «АЦСК CryptoKDC»;
- забезпечувати контроль за виконанням процедур генерації та резервування ключових документів ПТК «АЦСК CryptoKDC»;
- забезпечувати контроль за виконанням процедур знищення ключових документів ПТК «АЦСК CryptoKDC»;
- забезпечувати контроль за виконанням процедур збереженням апаратних засобів КЗІ ПТК «АЦСК CryptoKDC»;
- проводити службові розслідування у разі виникнення позаштатних ситуацій під час ініціалізації апаратних засобів КЗІ зі складу ПТК «АЦСК CryptoKDC», генерації, резервування або використання ключових документів;
- забезпечувати контроль за цілісністю операційного середовища, в якому використовуються апаратні та програмні засоби зі складу ПТК «АЦСК CryptoKDC».

Адміністратори безпеки, які відповідають за забезпечення безпеки експлуатації ПТК ЦСК мають право:

- доступу до приміщень, в яких розташовано ПТК «АЦСК CryptoKDC»;
- обмежувати доступ обслуговуючого персоналу до апаратних та програмних засобів із складу ПТК «АЦСК CryptoKDC»;
- вимагати від обслуговуючого персоналу виконання встановлених технологій обробки інформації та виконання встановленою даною інструкцією заходів із забезпечення безпеки експлуатації ПТК «АЦСК CryptoKDC»;
- ініціювати проведення службових розслідувань щодо фактів порушення встановлених даною інструкцією вимог щодо забезпечення безпеки експлуатації ПТК «АЦСК CryptoKDC»;
- призупиняти роботу всього ПТК «АЦСК CryptoKDC» в цілому та його окремих складових частин при порушенні встановленої технології обробки інформації та невиконанні вимог з безпеки експлуатації ПТК «АЦСК CryptoKDC»;
- встановлювати програмну частину ПТК «АЦСК CryptoKDC» разом із системним адміністратором.

3. Права та обов'язки користувачів ПТК «АЦСК CryptoKDC»

Користувачі (адміністратор реєстрації, адміністратор сертифікації, системний адміністратор), що використовують апаратні або програмні компоненти, які входять до складу ПТК «АЦСК CryptoKDC» зобов'язані:

- дотримуватися вимог інструкцій та вказівок адміністраторів безпеки, що відповідають за безпеку експлуатації ПТК «АЦСК CryptoKDC»;
- перед використанням програмних та апаратних засобів із складу ПТК «АЦСК CryptoKDC» ознайомитись з відповідними інструкціями по експлуатації;

- зберігати значення ПІН-коду доступу та розблокування до апаратних засобів КЗІ із складу ПТК «АЦСК CryptoKDC» у таємниці;
- не зберігати разом апаратні засоби КЗІ із складу ПТК «АЦСК CryptoKDC» та ПІН-коди доступу до них;
- періодично, або в разі потреби, змінювати ПІН-код доступу до апаратних засобів КЗІ із складу ПТК «АЦСК CryptoKDC»;
- не допускати використання апаратних засобів КЗІ із складу ПТК «АЦСК CryptoKDC» іншими особами, що не мають відповідних повноважень;
- доповідати адміністратору безпеки про факти порушення встановлених вимог забезпечення безпеки експлуатації, НСД, втрати, пошкодження інформації та апаратних засобів ПТК «АЦСК CryptoKDC»;
- у разі виникнення позаштатних ситуацій припинити використання апаратних та/або програмних засобів із складу ПТК «АЦСК CryptoKDC» та звернутися до адміністратора безпеки;
- використовувати програмні та апаратні засоби із складу ПТК «АЦСК CryptoKDC» лише за їх функціональним призначенням.

Користувачі, що використовують апаратні і програмні компоненти, які входять до складу ПТК «АЦСК CryptoKDC» мають право:

- надавати свої пропозиції адміністраторам безпеки щодо вдосконалення заходів з безпеки експлуатації ПТК «АЦСК CryptoKDC»;
- звертатися до адміністраторів безпеки для отримання необхідної технічної та методологічної допомоги у своїй роботі.

4. Забезпечення безпеки ПТК «АЦСК CryptoKDC» під час його встановлення

Під час встановлення ПТК «АЦСК CryptoKDC» необхідно дотримуватись наступних вимог та положень:

- встановлення програмної частини ПТК «АЦСК CryptoKDC» відбувається лише з еталонної копії, яка надана розробником. Встановлення програмної частини виконується системним адміністратором та адміністратором безпеки. При встановленні ПЗ «ЦСК-сервер», програмної частини ПТК «АЦСК CryptoKDC», необхідно унеможливити доступ сторонніх осіб до серверного приміщення;

- при створенні та введені ПІН-кодів доступу до апаратних та програмних засобів із складу ПТК «АЦСК CryptoKDC» необхідно унеможливити виявлення паролів сторонніми особами. Забороняється записувати ПІН-коди до окремих апаратних та програмних засобів, та зберігати їх у письмовій формі;

- у разі, якщо встановлення програмної частини ПТК «АЦСК CryptoKDC» не було вдалим, внаслідок перебою живлення, зависання серверу або АРМ, інсталяція виконується наново (з попереднім видаленням невдало або не повністю встановленої програмної частини);

- рекомендована мінімальна довжина ПІН-кодів доступу до апаратних та програмних засобів із складу ПТК «АЦСК CryptoKDC» має становити не менш ніж 4 символи;

- у випадку якщо ІТС, що використовує апаратні засоби зі складу ПТК «АЦСК CryptoKDC», не надає змоги змінити ПІН-код розблокування – не активуйте ПІН-код розблокування під час ініціалізації;

- забороняється залишати ПІН-коди доступу до апаратних та програмних засобів із складу ПТК «АЦСК CryptoKDC», які були встановлені виробником, без зміни;

- у разі виникнення позаштатних ситуацій в процесі встановлення ПТК «АЦСК CryptoKDC» необхідно припинити даний процесі і звернутися до розробника.

Загальна схема встановлення ПТК «АЦСК CryptoKDC» в інформаційно-телекомунікаційну систему наведена в Додатку 1.

5. Забезпечення безпеки ПТК «АЦСК CryptoKDC» під час його експлуатації

Під час експлуатації ПТК «АЦСК CryptoKDC» необхідно дотримуватись наступних вимог та положень:

- експлуатація серверної частини ПТК «АЦСК CryptoKDC» повинна здійснюватись у спеціальному приміщені, яке обладнане замками, засобами охоронної та пожежної сигналізації та постійно знаходиться під охороною або наглядом;
- повинні бути створені умови, що виключають можливість безконтрольного проникнення у приміщення сторонніх осіб та забезпечують фізичну збереженість ресурсів ПТК «АЦСК CryptoKDC». Розміщення та установка технічних засобів ПТК «АЦСК CryptoKDC» повинні виключати можливість візуального перегляду оброблюваної інформації сторонніми особами;
- генерація ключових документів ПТК «АЦСК CryptoKDC» повинна виконуватись лише відповідальною особою, що має на це повноваження;
- процедуру генерації ключових документів ПТК «АЦСК CryptoKDC» необхідно проводити комісійно за участю адміністратора безпеки;
- в разі дублювання засобів КЗІ, під час генерації ключових документів, дублікати повинні зберігатися у надійному місці, що виключає можливість НСД до них сторонніми особами.

Заборонено використовувати за призначенням апаратні засоби КЗІ зі складу ПТК «АЦСК CryptoKDC», які мають ознаки порушення функціонування.

6. Забезпечення безпеки ПТК «АЦСК CryptoKDC» під час його виведення з експлуатації

Під час виведення з експлуатації ПТК «АЦСК CryptoKDC» необхідно дотримуватись наступних вимог та положень:

- для виведення з експлуатації окремої компоненти ПТК «АЦСК CryptoKDC», така компонента видаляється з серверу або АРМ, при цьому повинно бути забезпечене резервне копіювання сертифікатів користувачів, СВС, особистих ключів АЦСК, файлів журналу аудиту тощо;
- знищення ключових документів для засобів КЗІ зі складу ПТК «АЦСК CryptoKDC» повинне відбуватися у відповідності з інструкцією щодо поводження з ключовими документами, яка постачається із відповідним засобом КЗІ лише в тих випадках, якщо засіб КЗІ не буде використовуватись, або засіб може бути використаний в інший системі.

7. Забезпечення безпеки ПТК «АЦСК CryptoKDC» під час його ремонту

В разі, якщо технічний персонал, що експлуатує ПТК «АЦСК CryptoKDC» не може на місці відремонтувати обладнання, що вийшло з ладу, то таке обладнання передається для ремонту в спеціалізовані сервісні установи. В разі передачі обладнання до сервісних установ із серверів або АРМ виймаються накопичувачі на жорстких магнітних дисках та апаратні засоби КЗІ.

В разі виходу з ладу накопичувача на жорстких магнітних дисках такий накопичувач знищується у спосіб, що унеможливлює відтворення інформації на ньому та замінюється новим.

В разі заміни старого накопичувача на жорстких магнітних дисках на новий, дані зі старого повинні переноситися на новий шляхом прямого копіювання.

Пристрій зчитування смарт-карток (карткоприймач) не містить ключових документів, тому він може бути переданий до сервісу для ремонту без обмежень.

Перед звертанням до сервісу рекомендовано самостійно вжити заходів щодо поновлення функціонування апаратних засобів КЗІ наступним чином:

- видалити забруднення з контактних поверхонь чип-модуля картки у разі, якщо використовуються картки мікропроцесорні «CryptoCard-318» та «CryptoCard-337»;
- перевірити правильність підключення пристрою зчитування смарт-карток до комп'ютерної техніки.

Забороняється передавати до сервісної організації значення ПІН-коду або коду розблокування апаратного засобу КЗІ.

Перед передачею до сервісної організації апаратних засобів КЗІ поточні ключі користувача мають бути скасовані, а сертифікат відкликаний.

Апаратні засоби КЗІ зі складу ПТК «АЦСК CryptoKDC», що використовувались для роботи із службовими ключовими документами забороняється передавати до сервісної організації. Такі засоби КЗІ необхідно знищити встановленим порядком в ПТК «АЦСК CryptoKDC».

8. Забезпечення безпеки ПТК «АЦСК CryptoKDC» в разі порушення функціонування інформаційно-телекомунікаційної системи

В разі порушення цілісності інформаційно-телекомунікаційної системи адміністратор безпеки, оцінює загрозу безпеці інформації і безпеці функціонування ПТК «АЦСК CryptoKDC», та приймає невідкладні дії щодо відновлення працездатності інформаційно-телекомунікаційної системи.

В разі, якщо порушення функціонування ІТС не впливає на безпеку інформації, що оброблюється ПТК «АЦСК CryptoKDC», то ЦСК може продовжувати функціонування, а технічний персонал може починати налагоджувальні роботи. Якщо порушення функціонування ІТС має вплив на роботу окремого компоненту ПТК «АЦСК CryptoKDC», то такий компонент відключається від ІТС, та знову під'єднуєтсья до ІТС після ліквідації причини порушення функціонування сегменту ІТС.

9. Питання проведення тестування компонентів ПТК «АЦСК CryptoKDC» та їх резервування

Тестування апаратних засобів КЗІ із складу ПТК «АЦСК CryptoKDC» виконується автоматично після їх підключення. Якщо тестування закінчилося з помилкою, то робота з засобом буде неможлива (Див. розділ 7).

Тестування програмних засобів із складу ПТК «АЦСК CryptoKDC» виконується автоматично. Якщо тестування закінчилося з помилкою, то програмне забезпечення відобразить опис помилки та припинить функціонування (Див. розділ 7).

Спеціальні модифікації апаратних засобів КЗІ із складу ПТК «АЦСК CryptoKDC» мають можливість резервування. Якщо використовуються саме такі засоби, слід врахувати наступне:

- резервні (дубльовані) засоби мають ті самі ключові документи, що і оригінал. Резервні засоби повинні зберігатися з дотриманням вимог безпеки, що висуваються й до оригіналів;
- процедуру дублювання необхідно проводити комісійно за участю адміністратора безпеки;
- під час дублювання повинно бути створено визначену кількість апаратних засобів КЗІ. Кількість резервних апаратних засобів КЗІ повна бути зафіксована в протоколі комісії;
- рекомендовано проводити дублювання апаратних засобів КЗІ, які використовуються для службових ключових документів.

З метою швидкого відновлення працездатності ПТК «АЦСК CryptoKDC», в разі збою апаратного забезпечення, адміністратор безпеки може тримати в резерві налаштовані та підготовлені до роботи резервні сервери та АРМ, які, в разі виходу з ладу основного обладнання можуть бути в короткі строки встановлені на заміну серверам та АРМ, що вийшли з ладу.

З метою побудови системи гарячого резервування (резервування даних в режимі реального часу) дозволяється робота двох серверів ЦСК одночасно.

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

Ситуація, що виникає в результаті небажаного впливу на ІТС, та яка не може бути подолана засобами захисту, називається надзвичайною. Надзвичайна ситуація може виникнути в результаті навмисних дій або випадково (в результаті ненавмисних дій, аварій, стихійних лих тощо).

Під навмисним нападом розуміється надзвичайна ситуація, яка виникла в результаті виконання зловмисниками в певні моменти часу заздалегідь продуманих та спланованих дій.

Під випадковою (ненавмисною) надзвичайною ситуацією розуміється така ситуація, яка не була результатом заздалегідь продуманих дій та виникнення якої стало результатом об'єктивних причин випадкового характеру, халатності, необережності або випадкового збігу обставин.

Усі користувачі, робота яких може бути порушена в результаті виникнення надзвичайної ситуацій, повинні бути негайно поінформовані.

У разі надзвичайних ситуацій апаратні засоби КЗІ користувачів із складу ПТК «АЦСК CryptoKDC» необхідно відключити від АРМ. Допускається залишати їх в місці звичайного зберігання лише при умові зберігання ПІН-коду у таємниці.

У разі надзвичайних ситуацій апаратні засоби КЗІ, які використовуються для службових ключових документів необхідно відключити від серверів та/або завершити роботу серверного програмного забезпечення. Не рекомендується залишати їх в місці використання.

Для унеможливлення знищення основної та резервної копій апаратних засобів КЗІ їх слід зберігати в різних приміщеннях.

Подальші дії щодо знешкодження причин порушення працездатності ПТК «АЦСК CryptoKDC», поновленню обробки та відновленню пошкоджених (втрачених) ресурсів визначаються функціональними обов'язками відповідальних осіб.

Кожна надзвичайна ситуація повинна бути проаналізованою відповідальною особою за забезпечення безпеки експлуатації. За результатами такого аналізу повинні бути сформовані пропозиції, щодо зміни повноважень користувачів, атрибутів доступу до ресурсів, створенню додаткових резервів, зміни конфігурації системи або параметрів засобів захисту і т.і.

При розслідуванні наслідків надзвичайних ситуацій слід враховувати наступне:

- якщо картки мікропроцесорні «CryptoCard-318» та «CryptoCard-337» не функціонують в пристрої зчитування, це не гарантує неможливість їх використання;
- якщо електронні ключі «SecureToken 318» та «Secure Token-337» не функціонують після приєднання до комп'ютера, це не гарантує неможливості їх використання;
- ключові документи, що знаходяться на апаратних засобах КЗІ не можуть бути знищені водою, агресивними рідинами або електричним струмом;
- ключові документи гарантовано знищені, якщо кристал чип-модуля апаратного засобу КЗІ механічно пошкоджений, або його було піддано дії настільки високої температури, що захисна

смола кристала обвуглилася та контакти чип-модуля були розплавлені.

При розслідуванні наслідків надзвичайних ситуацій слід використовувати журнали аудиту програмного забезпечення.

11. Порядок проведення контролю за станом забезпечення безпеки ПТК «АЦСК CryptoKDC»

Контроль за станом безпеки ПТК «АЦСК CryptoKDC» здійснюється шляхом проведення періодичного нагляду та профілактичних робіт. Користувачі ПТК «АЦСК CryptoKDC» періодично (не менше ніж раз на місяць) здійснюють перевірку стану безпеки інформаційних ресурсів та апаратних засобів ПТК «АЦСК CryptoKDC».

Перевірка включає в себе:

- контроль за наявністю вільного місця на накопичувачах на жорстких магнітних дисках серверів та АРМ;
- перегляд журналів аудиту ПТК «АЦСК CryptoKDC», що ведуться в автоматичному режимі, а також журналів, що ведуться засобами операційного середовища;
- перевірка актуальності програмного забезпечення, що забезпечує антивірусний захист;
- перевірка налаштувань, що встановлюють права доступу до ресурсів ПТК «АЦСК CryptoKDC».

У разі, якщо підчас перевірки були виявлені відхилення від встановленого раніше рівня безпеки, то особи, що проводять перевірку повинні повідомити про такі відхилення адміністратора безпеки, та приступити до з'ясування та усунення причин, що призвели до відхилення від встановленого рівня безпеки.

У разі, якщо відхилення від встановленого рівня безпеки можуть загрожувати безпеці захисту особистого ключа ПТК «АЦСК CryptoKDC», то ПТК АЦСК має бути негайно відключений від мережі Інтернет, до з'ясування та усунення обставин, що призвели до таких відхилень від встановленого рівня безпеки.

У разі вимкнення основного серверу ПТК «АЦСК CryptoKDC» необхідно забезпечити такі умови, щоб було надано вільний доступ клієнтів АЦСК до переліку сертифікатів та СВС.

12. Порядок допуску в приміщення, в яких встановлено ПТК «АЦСК CryptoKDC»

Контроль за виконанням порядку допуску до приміщень, у яких встановлено ПТК «АЦСК CryptoKDC», здійснюється адміністратором безпеки.

Серед приміщень, що використовуються для роботи ПТК «АЦСК CryptoKDC», виділяють наступні типи приміщень:

- для клієнтів;
- для користувачів;
- серверне приміщення.

Апаратні засоби КЗІ не накладають спеціальних обмежень на присутність осіб, що не є користувачами цих засобів, але при формуванні порядку допуску в приміщення слід врахувати наступне:

- апаратні засоби КЗІ у вигляді мікропроцесорних карт «CryptoCard-318», «CryptoCard-337» та електронних ключів «Secure Token-318» і «Secure Token-337» є компактними пристроями, які можуть бути легко сховані;
- якщо для вводу ПІН-коду використовується звичайна клавіатура, ПІН-код може бути викритий іншими особами, які знаходяться поряд з клавіатурою

Доступ до приміщень для клієнтів в робочі часи не обмежується. В неробочі часи доступ до приміщення мають особи, які здійснюють чергування, а також відповідальних осіб ПТК «АЦСК CryptoKDC».

Доступ до приміщень для користувачів має лише обслуговуючий персонал ПТК «АЦСК CryptoKDC». Інші особи можуть бути допущені до приміщення користувачів лише з дозволу адміністратора безпеки ПТК «АЦСК CryptoKDC» та у його супроводі. Приміщення користувачів має бути відокремлене від приміщення для клієнтів.

Серверна зона ЦСК є об'єктом особливого контролю щодо виконання режиму безпеки під час зберігання і обробки інформації.

Розкриття та закриття серверного приміщення має проводиться адміністратором безпеки та системним адміністратором. Факт розкриття та закриття приміщення фіксується у відповідному журналі.

Право розкриття та закриття серверного приміщення має лише адміністратор безпеки ПТК «АЦСК CryptoKDC».

Перед розкриттям приміщення, особи, які розкривають приміщення, пересвідчуються, що печатки на дверях приміщення не пошкоджено. В разі виявлення пошкоджень, необхідно терміново повідомити адміністратора безпеки та утриматись від розкриття приміщення до подальшого розпорядження.

Закриття приміщення має виконуватись у зворотному порядку. Факт закриття приміщення має фіксуватися у відповідному журналі.

Додаток 1

Загальна схема встановлення ПТК «АЦСК CryptoKDC» в інформаційно-телекомунікаційну систему