

**ПРОЕКТ**

**Стенд**  
**тестування функціональної сумісності**  
**електронного цифрового підпису**  
(шифр – "Стенд ЕЦП")

**Технічні вимоги**

на 11 аркушах

Київ - 2014

## ЗМІСТ

<b>ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ.....</b>	<b>3</b>
<b>1 ЗАГАЛЬНІ ВІДОМОСТІ.....</b>	<b>4</b>
1.1 ВІДОМОСТІ ЩОДО ОБ'ЄКТА РОЗРОБКИ.....	4
1.2 МЕТА І ПРИЗНАЧЕННЯ РОБОТИ.....	4
<b>2 ОПИС ОБ'ЄКТУ РОЗРОБКИ .....</b>	<b>5</b>
2.1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТА РОЗРОБКИ .....	5
2.2 ОСНОВНІ ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ОБ'ЄКТА РОЗРОБКИ .....	5
2.2.1 Основні функціональні можливості забезпечення безпеки.....	5
2.2.1.1 Списки доступу.....	5
2.2.1.2 Групи безпеки .....	5
2.2.1.3 Керування та збереження облікових даних користувачів .....	5
2.2.1.4 Аудит подій безпеки.....	6
2.2.1.5 Групові політики.....	6
2.2.2 Конфіденційність персональних даних .....	6
2.3 ЗАГАЛЬНА АРХІТЕКТУРА ОБ'ЄКТА РОЗРОБКИ.....	6
2.3.1 Технічне обладнання.....	6
2.3.2 Додаткове технічне обладнання .....	7
2.4 СЕРЕДОВИЩЕ ФУНКЦІОНУВАННЯ І ОБМЕЖЕННЯ ОБ'ЄКТА РОЗРОБКИ.....	8
2.4.1 Середовище функціонування об'єкта розробки .....	8
2.4.2 Етапи побудови середовища об'єкта розробки.....	8
2.4.2.1 Стенд тестування технологічної сумісності засобів ЕЦП, відповідно до етапів побудови, має забезпечити: .....	8
2.4.2.1.1 на першому етапі побудови Стенду: .....	8
2.4.2.1.2 На другому етапі побудови Стенду: .....	8
2.4.2.1.3 На третьому етапі побудови Стенду: .....	8
2.4.3 Обмеження об'єкта розробки .....	10
2.4.3.1 Апаратні обмеження функціонування об'єкта розробки.....	10
2.4.3.2 Програмні обмеження функціонування об'єкта розробки .....	10
<b>3 СПЕЦИФІКАЦІЯ ОБ'ЄКТА РОЗРОБКИ ЩОДО РЕАЛІЗАЦІЇ ВИМОГ НОРМАТИВНИХ ДОКУМЕНТІВ..</b>	<b>11</b>

**ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ**

<b>ЕЦП</b>	- електронний цифровий підпис
<b>ЦСК</b>	- центр сертифікації ключів
<b>АЦСК</b>	- акредитований центр сертифікації ключів
<b>ПТК</b>	- програмно-технічний комплекс
<b>КЗІ</b>	- криптографічний захист інформації
<b>ЦЗО</b>	- центральний засвідчувальний орган
<b>НЖМД</b>	- накопичувач на жорстких магнітних дисках
<b>ОС</b>	- операційна система
<b>ТВ</b>	- технічні вимоги
<b>ПЗ</b>	- програмне забезпечення
<b>ПБ</b>	- політика безпеки
<b>ЗЦ</b>	- засвідчувальний центр
<b>ПЕОМ</b>	- персональна обчислювальна машина

## 1 ЗАГАЛЬНІ ВІДОМОСТІ

### 1.1 Відомості щодо об'єкта розробки

Повне найменування об'єкта розробки – «Стенд тестування функціональної сумісності електронного цифрового підпису».

Повним найменуванням роботи є: «Створення Стенду тестування функціональної сумісності електронного цифрового підпису».

Шифр робіт – «Стенд ЕЦП».

Координатор робіт – Управління функціонування центрального засвідчувального органу Міністерства юстиції України (далі - ЦЗО).

### 1.2 Мета і призначення роботи

Метою проведення робіт є досягнення повної інтероперабельності засобів ЕЦП, виготовлених розробниками ПТК ЦСК України, шляхом здійснення заходів щодо практичної перевірки.

Оцінка спроможності виконання та забезпечення умов інтероперабельності здійснюється у контексті національних нормативних документів в сфері ЕЦП, зокрема Закону України «Про електронний цифровий підпис», наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 27 грудня 2013 року № 2782/5/689 «Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису», наказу Адміністрації державної служби спеціального зв'язку та захисту інформації України від «Про затвердження вимог до форматів криптографічних повідомлень» від 18 грудня 2012 року № 739, Державного стандарту України «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка» - ДСТУ 4145-2002, нормативного документу системи технічного захисту інформації «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (НД ТЗІ 2.5-004-99), далі – Національні критерії (НК) та інших нормативних документів.

Згідно з цими документами інтероперабельність розглядається як здатність взаємодіяти та функціонувати між собою програмних, програмно-апаратних засобів різних виробників.

Функція інтероперабельності може бути реалізована одним або декількома механізмами. Для реалізації функцій інтероперабельності можуть використовуватись різні програмні засоби, у тому числі і такі, що містять криптографічні перетворення.

Оцінка виконання вимог до форматів та протоколів, що реалізуються у надійних засобах ЕЦП ПТК ЦСК, АЦСК та ЗЦ є предметом дослідження, яке здійснюється в установленому порядку.

Результатом проведених робіт є оцінка спроможності виконання та забезпечення ЦСК, АЦСК та ЗЦ технічної сумісності (інтероперабельності) в частині забезпечення застосування вимог до форматів та протоколів, що реалізуються у надійних засобах ЕЦП ПТК. Замовник готує відповідне «Рішення» щодо відповідності вказаним критеріям.

## 2 ОПИС ОБ'ЄКТА РОЗРОБКИ

### 2.1 Загальна характеристика об'єкта розробки

Стенд ЕЦП повинен мати можливість тестування сертифікатів ЕЦП в ПТК, побудованих на базі Microsoft Windows XP, Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8, Apple iOS, Apple OS X Mountain Lion.

Стенд ЕЦП - це сервер та клієнтські ПЕОМ, які є членом родини клієнтських і серверних ОС різних фірм-виробників, які розроблені для взаємодії через обчислювальну мережу і можуть бути організовані в домен. Стенд ЕЦП, який діє в межах домену, може бути підпорядкований єдиній політиці безпеки і використовувати спільну базу даних.

Комплекс засобів захисту (КЗЗ) Стенду ЕЦП може забезпечувати послуги захисту в умовах функціонування одиночної обчислювальної машини (клас АС 1), при функціонуванні у складі локальної обчислювальної мережі (клас АС 2) або у складі локальної обчислювальної мережі з виходом у глобальну обчислювальну мережу (клас АС 3).

Стенд ЕЦП підтримує інсталяцію на робочій станції та призначений для настільних комп'ютерів і ноутбуків.

### 2.2 Основні функціональні можливості об'єкта розробки

Функціональні можливості Стенду ЕЦП розглядаються з позиції визначення наданих функцій технічного захисту інформації.

#### 2.2.1 Основні функціональні можливості забезпечення безпеки

##### 2.2.1.1 Списки доступу

Стенд ЕЦП надає доступ до ресурсів Стенду ЕЦП тільки авторизованим користувачам. Модель захисту включає компоненти, які реалізують контроль доступу суб'єктів і аудит подій.

Системний список доступу служить для забезпечення аудиту. Список доступу включає перелік користувачів, яким дозволено доступ до об'єкта, а також набір дозволених над об'єктом дій.

##### 2.2.1.2 Групи безпеки

Групи безпеки дозволяють спростити керування доступом до ресурсів, дозволяючи призначати дозволи і права для групи користувачів, а не окремому обліковому запису користувача. Таким чином, для надання доступу до нових ресурсів, обліковий запис може бути просто доданий або видалений з групи користувачів.

Крім користувачів в групу можна додавати комп'ютери та інші групи. Шляхом додавання комп'ютера до групи спрощується надання доступу системної задачі одного комп'ютера до ресурсів іншого.

##### 2.2.1.3 Керування та збереження облікових даних користувачів

Функція керування обліковими даними гарантує безпечне збереження облікових даних користувача, включаючи сертифікати X.509. Користувачам в домені надається можливість погодженої однократної реєстрації. При здійсненні першої спроби доступу до застосування в мережі потрібно виконати перевірку дійсності, у ході якої користувачу буде запропоновано ввести свої облікові дані. Після введення ці дані зв'язуються із запитаним застосуванням. При здійсненні наступних спроб доступу до цього застосування будуть використовуватися збережені облікові дані, тобто їх не потрібно буде вводити повторно.

#### 2.2.1.4 Аудит подій безпеки

В ПЗ Стенду ЕЦП є присутній набір засобів аудиту, призначених для моніторингу та виявлення небажаних умов і подій, які виникають в обчислювальному середовищі. Моніторинг системних подій дозволяє виявляти порушників системи безпеки, а також фіксувати спроби фальсифікації та видалення даних, які знаходяться на локальному комп'ютері. Під час аудиту найчастіше реєструються такі події як доступ до об'єктів, керування групами користувачів і обліковими записами груп, а також вхід користувачів в систему і вихід з неї. Аудит дозволяє вести моніторинг конкретних подій, наприклад, неуспішних спроб входу до системи. Перегляд журналу безпеки виконується за допомогою засобів перегляду подій. Політика аудиту дозволяє визначати події, для яких повинен проводитися аудит.

#### 2.2.1.5 Групові політики

В ПЗ Стенду ЕЦП є присутній набір шаблонів політик, які можуть застосовуватися для керування конфігураційними даними користувачів і налагодженням комп'ютера в конкретному обчислювальному середовищі. Цей набір може розширюватися адміністратором Стенду ЕЦП. Застосування групової політики здійснюється з метою контролю використання програм, мережних ресурсів і операційної системи користувачами і комп'ютерами.

#### 2.2.2 Конфіденційність персональних даних

Під час тестування використовуються тестові сертифікати відкритих ключів, отримані від ЦСК різних розробників надійних засобів ЕЦП, що не мають персональних даних підписувачів, але мають ознаки центрів, що їх згенерували. Під час тестування використовуються лише тестові електронні документи (дані), які не мають жодного виду інформації, що підлягає захисту.

### 2.3 Загальна архітектура об'єкта розробки

#### 2.3.1 Технічне обладнання

Технічне обладнання (сервер тестування та робочі станції операторів тестування) повинно мати можливість працювати з усіма існуючими операційними системами і мати такі характеристики:

№	Назва технічного обладнання та його параметри	Кількість одиниць
<b>1.</b>	<b>Робоча станція оператора тестування у складі:</b>	<b>3</b>
	Центральний процесор: Intel Corei7-4770w – не нижче або аналогічний	
	Материнська плата: LGA1150 ASUS Z97-K – не нижче або аналогічна	
	Оперативний запам'ятовуючий пристрій: тип - DDR3, об'єм - 32 ГБ (2 шт.)	
	Накопичувач на жорсткому магнітному диску: об'єм – не нижче 1 ТБ	
	Пристрій оптичних дисків: тип - DVD-RW	
	ОС: Microsoft Windows 8.1	
	Офісний пакет: Microsoft Office 2013	
	Програваач віртуальних машин: VMWare Player 9	
<b>2.</b>	<b>Сервер тестування (Supermicro SYS-7037R-TLF) у складі:</b>	<b>3</b>
	Центральний процесор: Intel Xeon E5-2600 – не нижче або аналогічний (2 шт.)	
	Материнська плата: LGA1150 ASUS Z97-K – не нижче або аналогічна	
	Оперативний запам'ятовуючий пристрій: тип - DDR3, об'єм - 32 ГБ (2 шт.)	
	Накопичувач на жорсткому магнітному диску: об'єм – не нижче 1 ТБ (2 шт.)	

	Пристрій оптичних дисків: тип DVD-RW	
	ОС: Microsoft Windows Server 2012 Standard	
	Програваач віртуальних машин: VMWare Player 9	

### 2.3.2 Додаткове технічне обладнання

Також, для охоплення всього спектру технічних засобів можуть використовуватись:

- робоча станція Apple MAC mini A1347 з ОС Apple OS X Mountain Lion;
- планшети:
- ASUS Google Nexus 7 16Gb з ОС Google Android – 1 шт.;
- Apple iPad mini A1489 with Retina display Wi-Fi 16GB (Space Gray) з ОС Apple iOS – 1 шт.;
- Microsoft Surface RT 32Gb Touch Cover (Black) з ОС Microsoft Windows RT.

## **2.4 Середовище функціонування і обмеження об'єкта розробки**

### **2.4.1 Середовище функціонування об'єкта розробки**

Передбачається функціонування Стенду ЕЦП в складі одномашинного однокористувачевого комплексу (клас АС 1), при функціонуванні у складі багатомашинного багатокористувачевого комплексу (наприклад, локальної обчислювальної мережі) (клас АС 2) та при функціонуванні у складі розподіленого багатомашинного багатокористувачевого комплексу з необхідністю передачі інформації через незахищене середовище (глобальної обчислювальної мережі) (клас АС 3) [2] (рис. 3).

### **2.4.2 Етапи побудови середовища об'єкта розробки**

2.4.2.1 Стенд тестування технологічної сумісності засобів ЕЦП відповідно до етапів побудови має забезпечити:

2.4.2.1.1 на першому етапі побудови Стенду:

ПЕОМ для напівавтоматизованого тестування засобів ЕЦП шляхом виконання наступних процедур:

- тестування зразків засобів ЕЦП – програмних та/чи апаратних засобів зі складу засобів користувачів ЦСК;
- тестування особистих та відкритих ключів, сертифікатів відкритих ключів та оп-Line-доступ до інформаційних ресурсів діючих ЦСК чи тестових макетів ЦСК розробників;
- здійснення повноциклових процедур формування та перевірки ЕЦП, а також шифрування та розшифрування даних засобами різних розробників із застосуванням усіх можливих протоколів взаємодії з ЦСК (формування позначок часу - TSP-протокол, інтерактивне визначення статусу сертифікатів - OCSP-протокол, завантаження та перевірка статусу сертифікатів за CBC - HTTP-протокол, пошук сертифікатів у LDAP-каталозі - LDAP-протокол) із здійсненням як перехресної перевірки засобів так і перевірки з еталонним засобом. Виконання зазначених перевірок має здійснюватися згідно з погодженою Міністерством юстиції України та Держспецзв'язком України методикою. За основу можуть бути взяті існуючі методики перевірки засобів ЕЦП.

2.4.2.1.2 На другому етапі побудови Стенду:

автоматизоване тестування зразків даних засобів ЕЦП шляхом надання on-line - доступу до сервера тестування, який дозволяє завантажувати зразки даних (даних ЕЦП, зашифрованих даних, запитів та відповідей OCSP-та TSP-протоколів та контейнерів особистих ключів) та отримувати автоматично висновки про їх правильність чи наявність помилок;

2.4.2.1.3 На третьому етапі побудови Стенду:

автоматизоване тестування засобів ЕЦП шляхом розробки вимог до тестового інтерфейсу взаємодії із засобами ЕЦП та отримання від ЦСК та розробників засобів ЕЦП із визначеним тестовим інтерфейсом та подальшою їх перевіркою еталонними тестовими засобами.



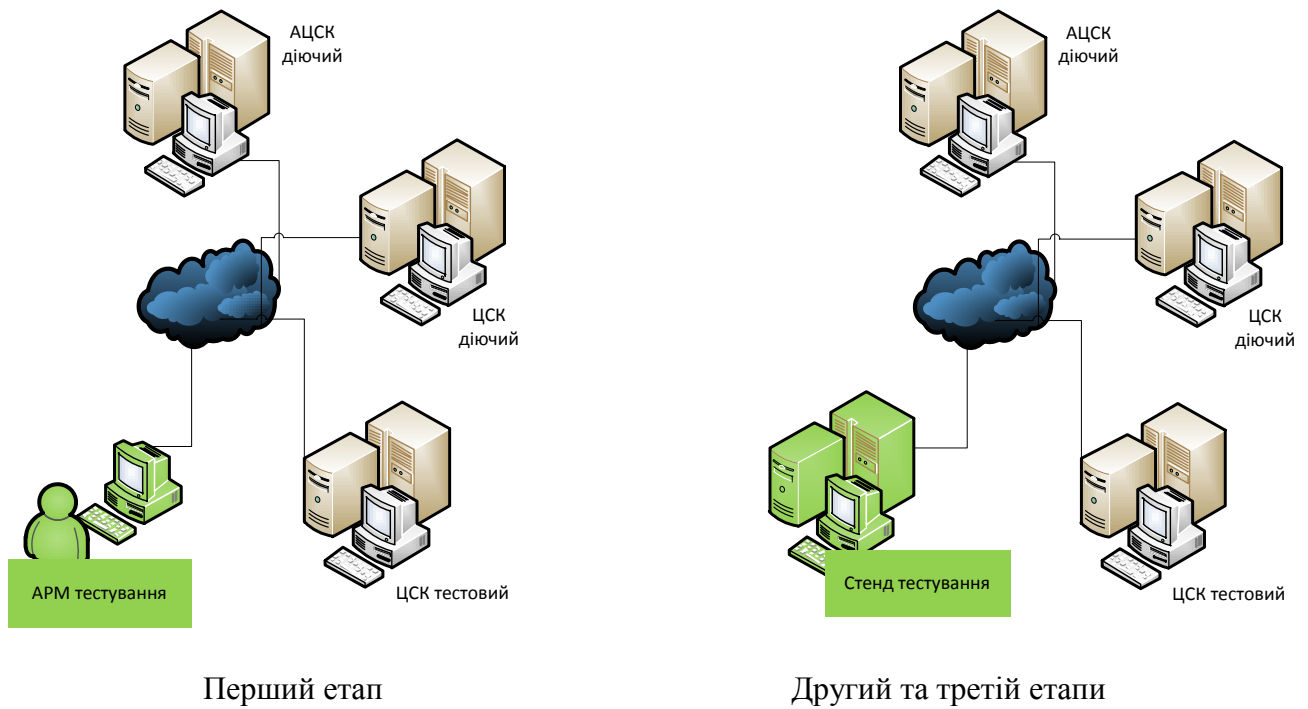


Рис. 1. Схема середовища функціонування об'єкта розробки в АС класів 1, 2, 3.

## **2.4.3 Обмеження об'єкта розробки**

### **2.4.3.1 Апаратні обмеження функціонування об'єкта розробки**

Стенд ЕЦП функціонує на робочій станції (персональному комп'ютері, мобільному комп'ютері типу ноутбук). Нижче наведено список стандартних пристроїв:

- 1) монітор;
- 2) клавіатура;
- 3) графічний маніпулятор „миша”;
- 4) пристрій CD-ROM;
- 5) пристрій НЖМД;
- 6) мережний адаптер.

### **2.4.3.2 Програмні обмеження функціонування об'єкта розробки**

Стенд ЕЦП є модульною системою, що складається з програмних компонентів, які виконують задачі, здійснюючи взаємодію через інтерфейси. Склад програмних компонентів визначається змістом ПЗ розробника та конфігурацією, визначеною для встановлення ПЗ.

Всі програмні компоненти ПЗ розташовані в фізичних межах робочої станції.

Замовник зобов'язується використовувати особисті ключі, відкриті ключі та сертифікати відкритих ключів, а також програмне, програмно-апаратне забезпечення виключно для цілей, зазначених у цих технічних вимогах.

### **3 СПЕЦИФІКАЦІЯ ОБ'ЄКТА РОЗРОБКИ ЩОДО РЕАЛІЗАЦІЇ ВИМОГ НОРМАТИВНИХ ДОКУМЕНТІВ**

Формати ключових даних, ЕЦП та захищених даних, а також протоколів та інтерфейсів взаємодії, які реалізовані у надійних засобах ЕЦП діючої Національної системи ЕЦП (як у складі ПТК ЦСК, так і у складі засобів користувачів ЦСК) повинні відповідати таким нормативно-правовим актам:

- вимогам до формату сертифікатів та списків відкликаних сертифікатів, затвердженим наказом Міністерства юстиції України, Адміністрації Держспецзв'язку України від 20.08.2012 року № 1236/5/453;
- вимогам до формату підписаних даних (даних з ЕЦП – CMS Signed-data/CAdES), затвердженим наказом Міністерства юстиції України, Адміністрації Держспецзв'язку України від 20.08.2012 року № 1236/5/453;
- вимогам до формату захищених даних (зашифрованих даних – CMS Enveloped-data), затвердженим наказом Адміністрації Держспецзв'язку України від 18.12.2012 року № 739;
- вимогам до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису, затвердженим наказом Міністерства юстиції України, Адміністрації Держспецзв'язку України від 20.08.2012 року № 1236/5/453;
- вимогам до форматів запитів на формування позначок часу та самих позначок часу (TSP-протокол), затвердженим наказом Міністерства юстиції України, Адміністрації Держспецзв'язку України від 20 серпня 2012 року № 1236/5/453;
- вимогам до форматів особистих ключів (контейнерів) та інтерфейсів взаємодії з засобами КЗІ, затвердженим наказом Міністерства юстиції України, Адміністрації Держспецзв'язку України від 27 грудня 2013 року № 2782/5/689.