

ЗАТВЕРДЖЕНО  
ЄААД.468244.185-ЛУ

Підп. та дата	
Інв. № дубл	
Взам. інв. №	
Підп. та дата	
Інв. № ориг.	

Центр сертифікації ключів  
ринку електричної енергії

Пояснювальна записка техноробочого проекту

ЄААД.468244.185.П2

2014 р.

## ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ .....	3
1. ЗАГАЛЬНІ ПОЛОЖЕННЯ .....	4
1.1. Повне найменування автоматизованої системи, що розробляється .....	4
1.2. Мета створення та головне призначення ЦСК.....	4
1.3. Перелік керівних документів, на підставі яких створюється ЦСК .....	4
2 ХАРАКТЕРИСТИКА ОБ'ЄКТУ ВПРОВАДЖЕННЯ .....	6
2.1 Характеристика автоматизованої системи центру сертифікації ключів ринку електричної енергії .....	6
3 ОСНОВНІ ТЕХНІЧНІ РІШЕННЯ.....	10
3.1 Рішення щодо структури.....	10
3.2 Опис комплексу технічних засобів .....	10
3.3 Призначення та загальна характеристика комплексу.....	12
3.4 Опис рішень щодо криптографічного захисту інформації.....	13
4 ЗАХОДИ ЩОДО ВВЕДЕННЯ В ДІЮ .....	15
4.1 Підготовка автоматизованої системи.....	15
4.2 Підготовка персоналу .....	17
5 Вимоги до облаштування приміщень АС ЦСК .....	19
5.1 Вимоги до облаштування приміщень .....	19
5.2 Вимоги до системи електроживлення та електричної безпеки .....	19
5.3 Вимоги до системи протипожежної безпеки .....	20
5.4 Вимоги до системи кондиціювання повітря .....	20
5.5 Вимоги до системи охоронної сигналізації.....	20
5.6 Вимоги до системи відеоспостереження .....	20
5.7 Вимоги до системи телефонного зв'язку та ЛОМ .....	20

## ПЕРЕЛІК СКОРОЧЕНЬ

ДБЖ	- Джерело безперебійного живлення
ЕОМ	- Електронно-обчислювальна машина
ЕОТ	- Електронно-обчислювальна техніка
ЕЦП	- Електронний цифровий підпис
ЄСПД	- Єдина система програмної документації
ЗТМ	- Зовнішні телекомунікаційні мережі
ІТС	- Інформаційно-телекомунікаційна система
КЗІ	- Криптографічний захист інформації
КТЗ	- Комплекс технічних засобів
КСЗІ	- Комплексна система захисту інформації
ЛОМ	- Локальна обчислювальна мережа
МЕ	- Міжмережний екран
НКІ	- Носій ключової інформації
ОС	- Операційна система
ПЕОМ	- Персональна ЕОМ
ПЗ	- Програмне забезпечення
ПТК	- Програмно-технічний комплекс
РС	- Робоча станція
РМ	- Робоче місце
СУБД	- Система управління базами даних
ТЗІ	- Технічний захист інформації
ЦСК	- Центр сертифікації ключів
СМР	- Control Messages Protocol (протокол управляючих повідомлень)
GPS	- Global Positioning System (глобальна система позиціонування)
GSM	- Global System for Mobile Communications (глобальна система мобільного зв'язку)
IPS	- Intrusion Prevention System (система попередження втручань)
HTTP	- Hyper Text Transfer Protocol
LDAP	- Lightweight Directory Access Protocol (протокол доступу до каталогу)
NTP	- Network Time Protocol (мережний протокол синхронізації часу)
OCSP	- Online Certificate Status Protocol (протокол визначення статусу сертифіката)
SMS	- Short Message Service (служба коротких повідомлень)
TSP	- Time-Stamp Protocol (протокол отримання позначок часу)
ЗТМ	- Зовнішні телекомунікаційні мережі
ВОЛЗ	- Волоконно-оптичні лінії зв'язку

## 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

### 1.1. Повне найменування автоматизованої системи, що розробляється

Повне найменування: автоматизована система центру сертифікації ключів ринку електричної енергії (далі -ЦСК ринку електричної енергії).

### 1.2. Мета створення та головне призначення ЦСК

Метою створення є реалізація ЦСК регламентних процедур та механізмів обслуговування сертифікатів відкритих ключів користувачів (далі - користувачів), надання послуг фіксування часу, а також реалізація ЕЦП і шифрування даних та управління особистими ключами і сертифікатами відкритих ключів користувачів системи.

### 1.3. Перелік керівних документів, на підставі яких створюється ЦСК

- Закон України від 22.05.2003 № 852-IV "Про електронний цифровий підпис";
- Закон України від 22.05.2003 № 851-IV "Про електронні документи та електронний документообіг";
- Указ Президента України від 22.05.1998 № 505/98 "Про Положення про порядок здійснення криптографічного захисту інформації в Україні";
- Постанова Кабінету Міністрів України від 02.07.2014 № 228 "Про затвердження Положення про Міністерство юстиції України";
- Постанова Кабінету Міністрів України від 13.07.2004 № 903 "Про затвердження Порядку акредитації центру сертифікації ключів";
- Постанова Кабінету Міністрів України від 28.10.2004 № 1451 "Про затвердження Положення про центральний засвідчувальний орган";
- Постанова Кабінету Міністрів України від 28.10.2004 № 1452 "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності";
- Постанова Кабінету Міністрів України від 28.10.2004 № 1454 "Про затвердження Порядку обов'язкової передачі документованої інформації";
- Постанова Кабінету Міністрів України від 13.03.2002 № 288 "Про затвердження переліків центральних органів виконавчої влади, на які покладаються функції технічного регулювання у визначених сферах діяльності та розроблення технічних регламентів";
- Постанова Кабінету Міністрів України від 26 травня 2004 р. № 680 "Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу";
- Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Державного комітету України з питань технічного регулювання та споживчої політики від 25.04.2007 № 75/91 "Про затвердження Правил проведення робіт із сертифікації засобів захисту інформації". Зареєстровано в Міністерстві юстиції України 14 травня 2007 р. за № 498/13765;
- Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 "Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації". Зареєстровано в Міністерстві юстиції України 30 липня 2007 р. за № 862/14129;
- Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.06.2008 № 100 "Про затвердження Положення про державну експертизу у сфері криптографічного захисту інформації". Зареєстровано в Міністерстві юстиції України 16 липня 2008 р. за № 651/15342;
- Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.2005 № 3 "Про затвердження Правил посиленої сертифікації". Зареєстровано в Міністерстві юстиції України 27 січня 2005 р. за № 104/10384;
- Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 "Про затвердження Вимог до форматів криптографічних повідомлень". Зареєстровано в Міністерстві юстиції України 14 січня 2013 р. за № 108/22640;
- Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 24.07.2007 за № 143 «Про затвердження Положення про порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного

цифрового підпису". Зареєстровано в Міністерстві юстиції України 8 серпня 2007 р. за N 914/14181;

- Регламент роботи Центрального засвідчувального органу, затверджений Наказом Міністерства юстиції України від 29.01.2013 № 183/5. Зареєстровано в Міністерстві юстиції України 30 січня 2013 р. за № 191/22723;
- Вимоги до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису, затверджені Наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.08.2012 № 1236/5/453. Зареєстровано в Міністерстві юстиції України 20 серпня 2012 р. за № 1398/21710;
- Роз'яснення Міністерства юстиції України щодо порядку обчислення геш-значення, викладені у Листі Міністерства юстиції України від 15.10.2012 № 12776-026-12/133;
- Інформаційна та технологічна картки адміністративної послуги з видачі Міністерством юстиції України свідоцтва про акредитацію центру сертифікації ключів, затверджені Наказом Міністерства юстиції України від 16.05.2013 № 900/5;
- Лист Міністерства юстиції України № 13.3-33/116 "Щодо інформування про розробку Порядку синхронізації часу із Всесвітнім координованим часом (UTC)";
- Наказ Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 05.12.2013 за № 2563/5/645 "Про затвердження переліків стандартів у сфері електронного цифрового підпису, перспективних для перегляду та гармонізації з європейськими та міжнародними стандартами відповідно до встановлених законодавством процедур";
- Вимоги до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису, затверджені Наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 27.12.2013 № 2782/5/689. Зареєстровано в Міністерстві юстиції України 27 грудня 2013 р. за №№2227/24759, 2228/24760, 2229/24761, 2230/24762;
- Наказ Міністерства юстиції України від 30.07.2014 за № 1249/5 "Про затвердження порядків ведення реєстрів центрального засвідчувального органу". Зареєстровано в Міністерстві юстиції України 1 серпня 2014 р. за № 903/25680, № 904/25681.

## 2 ХАРАКТЕРИСТИКА ОБ'ЄКТУ ВПРОВАДЖЕННЯ

2.1 Характеристика автоматизованої системи центру сертифікації ключів ринку електричної енергії

2.1.1 Опис технічних засобів

2.1.1.1 До складу автоматизованої системи входять такі технічні засоби (структурна схема комплексу технічних засобів наведена на рис. 2.1):

- центральні сервери (сервери ЦСК об'єднані у кластер);
- внутрішнє комунікаційне обладнання ЛОМ;
- дисковий масив;
- сервери взаємодії (кластер);
- міжмережний екран (МЕ) з системою попередження втручань (IPS);
- сервер моніторингу та синхронізації часу;
- обладнання синхронізації часу (GPS-приймач);
- обладнання сповіщення адміністраторів (GSM-модуль);
- мережні криптомодулі (кластер);
- криптомодулі;
- PC обслуговуючого персоналу (адміністратора безпеки, системного адміністратора, адміністратора реєстрації та адміністратора сертифікації);
- PC генерації ключів користувачів (ізольована);
- апаратно-програмні засоби КЗІ.

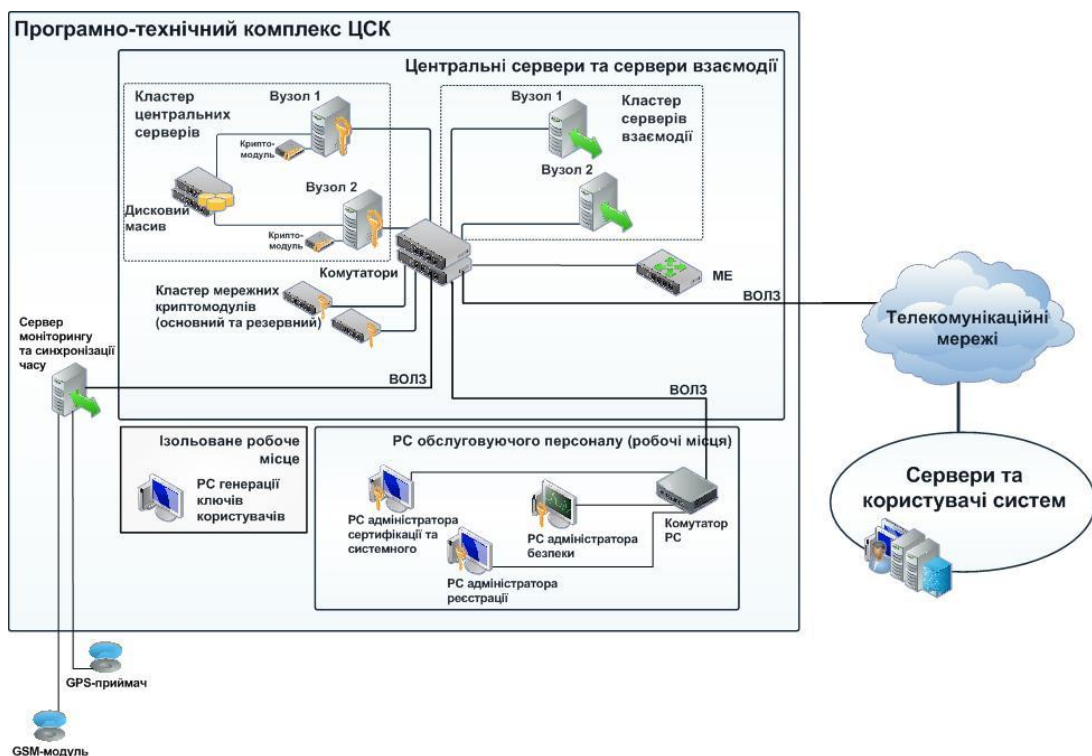


Рисунок 2.1 - Структурна схема комплексу.

2.1.1.2 PC адміністратора безпеки призначена для:

- введення реєстраційних даних посадових осіб (адміністраторів) до реєстру посадових осіб;
- зміну реєстраційних даних посадових осіб у реєстрі;
- видалення реєстраційних даних посадових осіб з реєстру;
- виконання інших функцій, пов'язаних із забезпеченням та підтримкою безпеки інформації, що обробляється у комплексі.

#### 2.1.1.3 PC системного адміністратора призначена для:

- налагодження параметрів технічних засобів комплексу та системного програмного забезпечення;
- діагностування роботи технічних засобів комплексу;
- моніторингу та контролю стану технічних засобів комплексу та виконання ним окремих функцій.

#### 2.1.1.4 PC адміністратора реєстрації призначена для:

- генерації особистого та відкритого ключів адміністратора реєстрації;
- передачі запиту на формування сертифіката адміністратора реєстрації на центральний сервер;
- отримання, зберігання та використання сертифікату адміністратора реєстрації;
- введення та використання особистого ключа адміністратора реєстрації;
- введення реєстраційних даних користувачів до реєстру користувачів;
- зміни реєстраційних даних користувачів у реєстрі;
- видалення реєстраційних даних користувачів з реєстру;
- приймання запитів користувачів на формування сертифікатів, що включає перевірку володіння користувачем особистого ключа, відповідного до відкритого ключа у запиті;
- ініціювання формування сертифікатів користувачів шляхом ведення та передачі запитів користувачів на формування сертифікатів до центрального сервера, що включає підпис запитів користувачів адміністратором (з використанням особистого ключа адміністратора);
- ініціювання скасування, блокування чи поновлення сертифікатів користувачів шляхом ведення та передачі запитів на зміну статусу сертифікатів до центрального сервера, що включає підпис запитів адміністратором (з використанням його особистого ключа).

#### 2.1.1.5 PC адміністратора сертифікації призначена для:

- генерації особистого та відкритого ключів ЦСК;
- введення та використання особистого ключа ЦСК;
- створення резервних копій особистого ключа ЦСК, а також відновлення особистого ключа з резервних копій;
- формування та передачі запиту на формування сертифіката ЦСК до ЦЗО;
- отримання та запису сертифікату ЦСК у реєстр сертифікатів;
- публікації сертифікату ЦСК на інформаційному ресурсі (на веб-сторінці сервера взаємодії);
- публікації списків відкликаних сертифікатів на інформаційному ресурсі ЦСК (на веб-сторінці);
- приймання запитів на формування сертифікатів користувачів та посадових осіб (адміністраторів);
- формування сертифікатів на основі запиту шляхом, що включає підпис сертифікатів (з використанням особистого ключа ЦСК);
- формування списків відкликаних сертифікатів користувачів шляхом, що включає підпис списків відкликаних сертифікатів (з використанням особистого ключа ЦСК);
- ручного резервного копіювання та архівування реєстру сертифікатів;
- моніторингу та контролю виконання автоматизованих функцій, зокрема:
  - публікації реєстру сертифікатів на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці) центральним сервером;
  - публікації списків відкликаних сертифікатів на інформаційному ресурсі центральним сервером;
  - публікації сертифікату ЦСК на інформаційному ресурсі центральним сервером.

#### 2.1.1.6 Центральні сервери (сервери ЦСК) призначені для:

- публікації сертифікату ЦСК на інформаційному ресурсі (у LDAP-каталозі);
- зберігання реєстру посадових осіб (адміністраторів) та забезпечення доступу до реєстраційних даних;
- використання реєстру посадових осіб;
- перевірки реєстраційних даних користувачів шляхом перевірки унікальності розпізнавального імені користувача;
- зберігання реєстру користувачів та забезпечення використання реєстраційних даних;

- використання реєстру користувачів;
- резервного копіювання та архівування реєстру користувачів;
- приймання та реєстрації запитів на формування сертифікатів користувачів та посадових осіб (адміністраторів);
- зберігання запитів на формування сертифікатів у базі даних запитів;
- архівування бази даних запитів на формування сертифікатів;
- перевірки унікальності відкритих ключів користувачів;
- зберігання реєстру сертифікатів;
- використання реєстру сертифікатів;
- автоматизованого резервного копіювання та архівування реєстру сертифікатів;
- публікації реєстру сертифікатів на інформаційному ресурсі ЦСК;
- приймання та реєстрації запитів користувачів і адміністраторів реєстрації на скасування, блокування чи поновлення сертифікатів;
- зберігання запитів на скасування, блокування чи поновлення сертифікатів у базі даних запитів;
- архівування бази даних запитів на скасування, блокування чи поновлення сертифікатів;
- скасування, блокування або поновлення сертифікатів на основі запитів;
- внесення інформації про поточний статус сертифіката до реєстру сертифікатів;
- публікації списків відкликаних сертифікатів на інформаційному ресурсі ЦСК;
- приймання через сервер взаємодії та обробку запитів користувачів на визначення статусу сертифікатів з використанням протоколу визначення статусу сертифіката (OCSP), шляхом формування інформації про статус сертифікатів;
- приймання через сервер взаємодії та обробку запитів користувачів на формування позначок часу, шляхом формування позначок часу та передачу сформованих позначок часу користувачам;
- внесення сформованих позначок часу у базу даних;
- зберігання сформованих позначок у базі даних;
- архівування бази даних позначок часу.

#### 2.1.1.7 Сервери взаємодії призначені для:

- приймання та передачі запитів користувачів та адміністраторів реєстрації на формування сертифікатів користувачів на центральний сервер;
- забезпечення доступу користувачів до реєстру сертифікатів на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці);
- приймання та передачі запитів користувачів та віддалених адміністраторів реєстрації на скасування, блокування чи поновлення сертифікатів користувачів на центральний сервер;
- забезпечення доступу користувачів до списків відкликаних сертифікатів на інформаційному ресурсі ЦСК;
- забезпечення доступу користувачів до інформації про статус сертифікатів з використанням протоколу визначення статусу сертифіката (OCSP), шляхом приймання та передачі запитів на визначення статусу сертифіката на центральний сервер та передачі інформації про статус у зворотному напрямку;
- приймання та передачі запитів користувачів на формування позначок часу на центральний сервер;
- передачі сформованих на центральному сервері позначок часу користувачам;
- забезпечення доступу до сертифікату ЦСК на інформаційному ресурсі.

#### 2.1.1.8 Сервер моніторингу та синхронізації часу призначений для:

- синхронізації часу з Центральним засвідчувальним органом та системою GPS;
- надання даних точного часу усім іншим компонентам ЦСК;
- збирання і аналізу даних моніторингу.

2.1.1.9 Обладнання синхронізації часу (GPS-приймач) призначене для отримання сигналів точного часу від системи GPS.

2.1.1.10 Обладнання сповіщення адміністраторів (GSM-модуль) призначене для відправки SMS-повідомлень адміністраторам про виникнення позаштатних ситуацій, або у відповідності до налаштувань сповіщень сервера моніторингу.



2.1.1.11 Мережні криптомодулі призначені для:

- зберігання особистих ключів серверів ЦСК;
- виконання криптографічних операцій.

2.1.1.11 Криptomодулі призначені для:

- зберігання особистих ключів ЦСК;
- виконання криптографічних операцій.

2.1.1.12 АПЗ КЗІ призначені для

- зберігання особистих ключів персоналу ЦСК;
- виконання криптографічних операцій.

2.1.1.13 Комутатори та інше внутрішнє комунікаційне обладнання призначене для забезпечення внутрішньої взаємодії засобів комплексу та утворення ЛОМ.

2.1.1.14 МЕ з IPS призначені для фільтрації мережного трафіку між телекомунікаційними мережами та сервером взаємодії. Міжмережний екран Cisco ASA - 5512 реалізує такі механізми захисту інформації:

- можливість автентифікації та авторизації користувачів;
- фільтрацію інформаційних потоків відповідно до поточної політики безпеки на основі мережних атрибутів (будь-яких полів мережних пакетів, вхідного та вихідного мережного інтерфейсу);
- заборону доступу неавторизованих користувачів зовнішньої мережі до ресурсів внутрішньої мережі та навпаки;
- використання механізмів NAT для приховання справжніх мережних адрес;
- облік подій за допомогою ведення журналу системних подій (syslog) та (SNMP) на сервері моніторингу та керування обладнанням;
- розподілення на зони захисту для забезпечення розширеної політики безпеки;
- можливість застосування механізму гарячого резервування.

2.1.1.15 РС генерації ключів користувачів призначена для:

- генерації особистого та відкритого ключів користувача та запис особистого ключа на носій ключової інформації (НКИ);
- формування та запису на носій інформації запиту на формування сертифіката користувача.

2.2.1 Опис програмного забезпечення

Склад ПЗ за розміщенням на засобах ЕОТ комплексу:

- ПЗ центральних серверів;
- ПЗ серверів взаємодії;
- ПЗ сервера моніторингу та синхронізації часу;
- ПЗ РС адміністратора сертифікації та РС системного адміністратора;
- ПЗ РС адміністратора безпеки;
- ПЗ РС адміністратора реєстрації;
- ПЗ РС генерації ключів користувачів.

ПЗ для кожного з засобів ЕОТ поділяється на системне та функціональне.

До системного відноситься ПЗ, що забезпечує загальне функціонування засобів ЕОТ (ОС, СУБД, засоби доступу до СУБД, штатні КЗЗ ОС, СУБД та засоби їх адміністрування тощо). До функціонального - ПЗ, що забезпечує виконання спеціальних функцій засобів у складі комплексу (програмні комплекси та компоненти, що реалізують функції елементів ЦСК).

В якості серверної ОС центральних серверів використовується Microsoft Windows 2012 Server R2 Standard x64.

В якості серверної ОС серверів взаємодії використовується FreeBSD 9.2.

Робочі станції адміністраторів ЦСК функціонують під управлінням ОС Microsoft Windows 8.1 Enterprise.

### 3 ОСНОВНІ ТЕХНІЧНІ РІШЕННЯ

#### 3.1 Рішення щодо структури

Побудова обчислювальної мережі ЦСК визначається завданнями, що вирішуються ЦСК, і зумовлює структуру ЦСК. В основу побудови мережі закладений модульний принцип, який дозволяє гнучко змінювати систему в частині її нарощення та перерозподілу потужності.

#### 3.2 Опис комплексу технічних засобів

##### 3.2.1 Склад комплексу технічних засобів

До програмно-апаратних засобів ЦСК відносяться:

- активне мережне обладнання:
  - Міжмережевий екран Cisco ASA - 5512 - 1 шт.
- засоби захисту:
  - МКМ «Гряди-301» - 2 шт;
  - КМ «Гряди-61» - 2 шт;
- серверна компонента, до складу якої входять:
  - сервери центральні ЦСК - 2 шт;
  - сервери взаємодії ЦСК - 2 шт;
  - сервер синхронізації та моніторингу - 1 шт.
  - GPS - приймач;
  - GSM - модуль.
- робочі станції, на яких встановлено системне та прикладне програмне забезпечення для організації роботи адміністраторів ЦСК;
- PC генерації ключів користувачів ЦСК.

##### 3.2.2 Структурована кабельна система

Для здійснення інформаційного обміну між складовими системи побудовано СКС. Архітектура СКС приміщень ЦСК - "зірка" з мінімальною кількістю проміжних сполучень між робочими станціями та активними мережними пристроями. Елементна база системи (кросове обладнання, інсталяційний (магістральний) кабель, інформаційні розетки, кросувальні шнури) розраховані на передачу інформаційного сигналу зі смугою частот до 125МГц і придатні для побудови локальної мережі за технологією Fast Ethernet IEEE 802.3u (з пропускну здатністю каналів 100 Мбіт/с) або Gigabit Ethernet IEEE 802.3ab (з пропускну здатністю каналів 1000 Мбіт/с). Комплекс у складі ЦСК взаємодіє із зовнішньою телекомунікаційною мережею через широкосмуговий тракт зв'язку на швидкості не менше 512 кБіт/с (Передбачена можливість резервування цього тракту). Елементи СКС розташовані в межах контрольованої зони.

##### 3.2.3 Зовнішні канали зв'язку

Обмін інформацією між Користувачами та ЦСК здійснюється орендованими каналами передачі даних.

##### 3.2.4 Підсистема гарантованого електроживлення

Підсистема гарантованого електроживлення складається з пристроїв безперебійного живлення, розрахованих на забезпечення активного мережного обладнання, серверів, робочих місць адміністраторів та чергової зміни ЦСК електроенергією протягом 15 хвилин при 100% навантаженні, яка також призначена для захисту обладнання від зовнішніх дестабілізуючих факторів при наявності відхилень у параметрах електроживлення у вхідних мережах електропостачання.

##### 3.2.6 Серверна компонента

Центральні сервери та сервери взаємодії функціонують автоматизовано. сервери об'єднані у відповідні кластери.

Засоби серверу ЦСК підтримують можливість автоматичного резервного копіювання реєстру сертифікатів, реєстру користувачів, бази списків відкликаних сертифікатів та бази позначок часу на зовнішні носії інформації (DVD або зовнішні жорсткі диски).

Всі технічні засоби комплексу забезпечують можливість діагностування та отримання інформації про стан їх функціонування засобами моніторингу.

РС адміністратора безпеки, системного адміністратора, адміністратора реєстрації, центральні сервери, сервери взаємодії та сервер синхронізації та моніторингу взаємодіють через внутрішню телекомунікаційну мережу на основі кабельної мережі та комутатора і утворюють ЛОМ.

### 3.2.7 Склад комплексу програмних засобів

До програмних засобів ЦСК відносяться:

- системне програмне забезпечення (операційні системи Microsoft Windows Server 2012 R2 Standard, Microsoft Windows 8.1 Enterprise, Linux FreeBSD 9.2;
- СУБД а засобами їх адміністрування Microsoft SQL Server 2012 із штатним КЗЗ;
- програмний комплекс сервера ЦСК “ІТ ЦСК-1. Ключі ЦСК”, “ІТ ЦСК-1. СМР-сервер”, “ІТ ЦСК-1. ТСП-сервер”, “ІТ ЦСК-1, ОСРР-сервер”, “ІТ ЦСК-1. Службові модулі сервера ЦСК”;
- HTTP-сервер Apache з модулем формування HTML-документів PHP;
- СУБД MySQL;
- LDAP-сервер Open LDAP із штатним КЗЗ;
- модуль передачі електронних поштових повідомлень (MTA) та поштовий сервер із штатним КЗЗ Exim ;
- програмний комплекс сервера взаємодії ІТ ЦСК-1. Сервер взаємодії;
- засоби адміністрування та аудиту СУБД сервера ЦСК Microsoft SQL Server 2012 та штатні ODBC-драйвери ОС;
- засоби управління комутатором та ME Термінальний клієнт SSH, HTTPS-клієнт, окремі штатні засоби управління пристроями;
- засоби адміністрування системного ПЗ сервера взаємодії Термінальний клієнт SSH;
- програмний комплекс адміністратора сертифікації ІТ ЦСК-1. Адміністратор сертифікації;
- програмний комплекс адміністратора реєстрації ІТ ЦСК-1. Адміністратор реєстрації;
- програмний комплекс користувача ЦСК ІТ Користувач ЦСК-1;
- антивірусне ПЗ: ESET Endpoint Security 5 або аналогічне;
- інше програмне забезпечення, необхідне для функціонування системи архівації даних та захисту інформації.

### 3.2.8 Антивірусний захист комп'ютерних систем

Антивірусний захист комп'ютерних систем впроваджений з метою здійснення організаційних і технічних заходів щодо забезпечення захисту технічних засобів ЦСК від зараження комп'ютерними вірусами.

Антивірусний захист комп'ютерних систем призначений для захисту центральних серверів та робочих станцій ЦСК від комп'ютерних вірусів та перекриває можливі шляхи проникнення вірусів в ЦСК через:

- файли, що виконуються;
- електронну пошту;
- системні області жорстких дисків або дискет, в тому числі і магнітно-оптичних дисків;
- документи Microsoft Word;
- електронні таблиці Microsoft Excel;
- бази даних Microsoft Access;
- презентації Microsoft PowerPoint;
- HTML сторінки із Java або Active-X аплетами;
- інші шляхи зараження .

Ефективний захист від комп'ютерних вірусів забезпечується впровадженням комплексної системи антивірусного захисту. На рівні ЦСК застосовується дворівнева система антивірусного захисту, що передбачає використання багатокomпонентності засобів антивірусного захисту на робочих станціях персоналу та серверах ЦСК. Антивірусне ПЗ, що застосовується в ЦСК, відповідає вимогам ТЗІ та підтверджено у встановленому порядку.

Антивірусний захист комп'ютерних систем рівня ЦСК:

Перший рівень - захист серверів ЦСК. Антивірусне програмне забезпечення, що встановлюється на центральні сервери, виявляє спроби запису заражених, підозрілих файлів на ці сервери, на які встановлюється ПЗ СА ESET Endpoint Security 5. Антивірусні програми, які використовуються на цьому рівні, надають можливість перевірки файлів в режимі реального часу та видалення з них комп'ютерних

вірусів (фоновий режим), а також перевірки за запитом адміністратора безпеки. Антивірусне програмне забезпечення дає можливість блокувати спроби запису заражених, підозрілих файлів на сервери. Кожна така спроба фіксується у протоколах, звітах антивірусної програми із зазначенням імені зараженого файлу та шляху до нього.

Другий рівень - захист автоматизованих робочих місць на робочих станціях персоналу ЦСК встановлюється антивірусне ПЗ CA ESET Endpoint Security 5, відповідність якого вимогам ТЗІ підтверджено у встановленому порядку. Дане ПЗ має у своєму складі антивірусний монітор, що запускається при вмиканні комп'ютера і працює постійно у фоновому режимі без істотного уповільнення роботи системи в цілому або окремих її додатків, а також антивірусний сканер, який здійснює перевірку за запитом користувача або адміністратора безпеки. Дана перевірка має ініціюватися при завантаженні даних із будь-яких зовнішніх носіїв інформації. Система антивірусного захисту настроєна таким чином, що відразу виліковує уражені файли в разі їх знаходження. Налаштування цього антивірусного ПЗ встановлюється за замовчуванням з серверу антивірусного захисту, оновлення встановлюються автоматично.

На рівні користувачів ЦСК система антивірусного захисту є однорівневою. На робочих станціях користувачів ЦСК встановлюється антивірусне ПЗ CA ESET Endpoint Security 5. При цьому кожного разу під час завантаження даних із будь-яких зовнішніх носіїв інформації користувачем має ініціюватися перевірка цих носіїв за допомогою антивірусного сканера.

Ведеться журнал усіх подій, які генерує антивірусне ПЗ на клієнтських робочих місцях, у якому зазначається:

- час та дата виникнення події;
- рівень події (критичний, інформаційний, попередження);
- таке ведеться журнал усіх знайдених вірусів, у якому зазначається:
- час та дату виникнення події;
- рівень події (критичний, інформаційний, попередження);
- дія, що застосовувалася до зараженого файлу;
- результат дії.

### 3.2.9 Концепція зберігання даних

Концепція зберігання даних включає можливість використання декількох рівнів систем зберігання для різноманітних типів даних.

Визначаються такі основних рівня зберігання даних:

- основне сховище з оперативними даними, що використовуються;
- другорядне сховище з копіями основних даних та даними, що мало використовуються.

Ці рівні системи зберігання повинні бути реалізовані в межах однієї дискової підсистеми.

Дискова система зберігання це RAID-масив із кешуванням.

Система зберігання забезпечує автоматичне зберігання даних кеш-пам'яті на дисках при відмові електричного живлення за рахунок резервних батарей.

Дискова система зберігання передбачає автоматичний, постійний контроль цілісності дисків, аналіз поганих секторів, перевірку стану резервних батарей, без втручання адміністратора та без впливу на роботу користувачів.

### 3.3 Призначення та загальна характеристика комплексу

Призначенням є реалізація ЦСК регламентних процедур та механізмів обслуговування сертифікатів відкритих ключів користувачів ЦСК (далі - користувачів), надання послуг фіксування часу, надання користувачам засобів ЕЦП та шифрування, а також засобів генерації особистих і відкритих ключів

Комплекс забезпечує реалізацію регламентних процедур та механізмів роботи ЦСК, пов'язаних з:

- обслуговуванням сертифікатів відкритих ключів (далі - сертифікатів) користувачів, що включає:
  - реєстрацію користувачів;
  - сертифікацію відкритих ключів користувачів;

- розповсюдження сертифікатів;
- управління статусом сертифікатів;
- розповсюдження інформації про статус сертифікатів;
- надання послуг фіксування часу;
- надання користувачам засобів ЕЦП та шифрування даних, а також засобів генерації та управління ключами.

Функціональною основою комплексу є спеціалізовані апаратні та програмні засоби КЗІ і включає:

- програмний комплекс ЦСК "ІІТ ЦСК-1";
- криптомодуль "Грядя-61" ("ІІТ КМ Грядя-61");
- мережний криптомодуль "Грядя-301" ("ІІТ МКМ Грядя-301");
- програмний комплекс користувача ЦСК "ІІТ Користувач ЦСК-1";
- електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1").

Криptomодуль "Грядя-61" призначений для апаратної реалізації формування ЕЦП і у складі центральних серверів чи РС адміністратора сертифікації і забезпечує використання та захист особистого ключа ЦСК. Особистий ключ ЦСК генерується, зберігається та використовується тільки у середині пристрою.

Мережний криптомодуль "Грядя-301" призначений для апаратної реалізації криптографічних перетворень у складі центральних серверів ЦСК (CMP, TSP та OCSP).

У складі програмного забезпечення користувачів ЦСК може використовуватися апаратний електронний ключ "Кристал-1". Електронний ключ призначений для апаратної реалізації криптографічних перетворень. Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливорює доступ до особистих ключів з боку апаратно-програмного середовища.

Комплекс включає у своєму складі програмні засоби КЗІ (виду "Б", підвид "Б2", категорії "К", "П" та "Ш", класу В2), які можуть використовувати апаратні та апаратно-програмні засоби КЗІ (виду "Б", підвид "Б2", або виду "В", категорії "П" або "П" та "Ш", класу "Б1").

#### 3.4 Опис рішень щодо криптографічного захисту інформації

Функціональні характеристики та режими експлуатації комплексу не залежать від типів та характеристик технічних засобів (РС, серверів та комунікаційного обладнання).

В засобах комплексу використовуються такі криптографічні алгоритми та протоколи:

- шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни, режим гамування та режим вироблення імітовставки), TDEA та AES за ISO/IEC 18033-3;
- ЕЦП за ДСТУ 4145-2002 та RSA за ISO/IEC 14888-2:2008 і PKCS#1;
- гешування за ГОСТ 34.311-95 та SHA за ISO/IEC 10118-3:2004;
- протокол розподілу ключових даних Діффі-Гелмана в групі точок еліптичної кривої (направлене шифрування).

Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України № 739 від 18.12.2012 р. Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України.

У ключовій системі комплексу виділені дві підгрупи ключових даних:

- службові ключові дані;
- ключові дані користувачів.

До складу службових відносяться:

- особистий ключ та сертифікат ЦСК;
- особисті ключі та сертифікати серверів ЦСК (CMP, TSP та OCSP);
- особисті ключі та сертифікати адміністраторів реєстрації та віддалених адміністраторів реєстрації.

Особистий ключ ЦСК зберігається та застосовується тільки у криптомодулі, що входить до складу сервера ЦСК або РС адміністратора сертифікації.

Особистий ключ ЦСК використовується для формування ЕЦП сертифікатів та списків відкликаних сертифікатів. Сертифікат ЦСК використовується для перевірки ЕЦП, що накладається за допомогою особистого ключа ЦСК.

Особисті ключі серверів ЦСК (OCSP та TSP) використовується для формування ЕЦП від позначок часу та інформації про статус сертифікатів. Сертифікати серверів ЦСК використовується для перевірки ЕЦП, що накладається за допомогою відповідних особистих ключів серверів ЦСК.

Особисті ключі адміністраторів реєстрації призначені для формування ЕЦП запитів на формування сертифікатів, а також запитів на блокування, поновлення та скасування, а сертифікати - для перевірки ЕЦП від вказаних типів даних.

#### 4 ЗАХОДИ ЩОДО ВВЕДЕННЯ В ДІЮ

##### 4.1 Підготовка автоматизованої системи

###### 4.1.1 Підготовка центральних серверів системи

Впровадження комплексу у складі центральних серверів включає:

- встановлення центральних серверів в режим функціонування двохвузлового відмовостійкого кластеру;
- підключення мережових крипто модулів (підключення здійснюється за допомогою комутатора ЛОМ ЦСК);
- підключення криптомодулів;
- інсталяцію програмного комплексу “ІІТ ЦСК-1” на центральні сервери;
- встановлення параметрів програмного комплексу.

Підключення криптомодуля (наявність мережевого доступу з центрального сервера до модуля) необхідне для забезпечення використання модуля в якості апаратного засобу КЗІ центральним сервером.

Підключення мережевого криптомодуля (наявність мережевого доступу з центрального сервера до модуля) необхідне для забезпечення використання модуля в якості апаратного засобу КЗІ центральним сервером.

Інсталяція програмного комплексу ЦСК здійснюється з інсталяційного пакету комплексу засобами ОС сервера у каталог програм.

Встановлення параметрів програмного комплексу захисту включає:

- встановлення параметрів CMP-сервера;
- встановлення параметрів OCSP-сервера;
- встановлення параметрів TSP-сервера;
- встановлення параметрів формувача CBC;
- встановлення параметрів публікатора до LDAP-каталогу.

Генерація ключів та формування сертифікатів здійснюється засобами програмного комплексу та криптомодулів. До складу необхідних ключів та сертифікатів входять:

- особистий ключ та сертифікат ЦСК;
- особисті ключі та сертифікати серверів ЦСК (за необхідністю);
- сертифікати Центрального засвідчувального органу (за необхідністю).

Завантаження сертифікатів Центрального засвідчувального органу у файлове сховище включає копіювання необхідних сертифікатів з носія інформації локально, віддалено через мережу.

###### 4.1.2 Підготовка серверів взаємодії системи

Впровадження комплексу у складі серверів взаємодії включає:

- встановлення серверів взаємодії в режим функціонування двохвузлового відмовостійкого кластеру;
- інсталяцію програмного комплексу “ІІТ ЦСК-1. Сервер взаємодії” на сервери;
- встановлення параметрів.

###### 4.1.3 Підготовка робочої станції адміністратора безпеки

Впровадження комплексу у складі робочої станції адміністратора сервера АБС включає:

- інсталяцію програмного комплексу віддаленого моніторингу засобів програмного комплексу ЦСК;
- встановлення параметрів програмного комплексу віддаленого моніторингу;
- інсталяція засобів управління комутатором та ME Термінальний клієнт SSH, HTTPS-клієнт, окремі штатні засоби управління пристроями.

Інсталяція програмного комплексу віддаленого моніторингу засобів ЦСК здійснюється з інсталяційного пакету комплексу засобами ОС у каталог програм ОС.

Встановлення параметрів програмного комплексу віддаленого моніторингу включає встановлення через засоби графічного інтерфейсу комплексу параметрів мережевого підключення до агента моніторингу на центральному сервері тощо.

#### 4.1.4 Підготовка робочої станції адміністратора сертифікації та системного адміністратора

Впровадження комплексу у складі робочої станції адміністратора сертифікації та системного адміністратора:

- інсталяцію програмного комплексу адміністратора сертифікації;
- встановлення параметрів програмного комплексу адміністратора сертифікації.
- інсталяція засобів управління комутатором та ME Термінальний клієнт SSH, HTTPS-клієнт, окремі штатні засоби управління пристроями.

Інсталяція програмного комплексу адміністратора сертифікації здійснюється з інсталяційного пакету комплексу засобами ОС у каталог програм ОС.

#### 4.1.5 Підготовка робочої станції адміністратора реєстрації

Впровадження комплексу у складі робочої станції адміністратора сервера АБС включає:

- інсталяцію програмного комплексу адміністратора реєстрації;
- встановлення параметрів програмного комплексу адміністратора реєстрації.

Інсталяція програмного комплексу адміністратора реєстрації здійснюється з інсталяційного пакету комплексу засобами ОС у каталог програм ОС.

Встановлення параметрів програмного комплексу адміністратора реєстрації включає встановлення через засоби графічного інтерфейсу комплексу параметрів CMP-сервера, каталогу сертифікатів тощо.

#### 4.1.6 Підготовка робочої станції генерації ключів користувачів

Впровадження комплексу у складі робочої станції станції генерації ключів користувачів:

- інсталяцію програмного комплексу станції генерації ключів користувачів;
- встановлення параметрів станції генерації ключів користувачів.

Інсталяція програмного комплексу станції генерації ключів користувачів здійснюється з інсталяційного пакету комплексу засобами ОС у каталог програм ОС.

Встановлення параметрів програмного комплексу станції генерації ключів користувачів включає встановлення через засоби графічного інтерфейсу комплексу параметрів облікового запису користувача, параметрів запису запитів тощо.

#### 4.1.8 Організація ключової системи

Процедура організації ключової системи для центра сертифікації ключів включає:

- генерацію особистого ключа ЦСК з використанням криптомодуля;
- резервне копіювання особистого ключа ЦСК (в тому числі для переносу на резервний криптомодуль);
- генерацію особистих ключів серверів ЦСК з використанням мережевого криптомодуля;
- резервне копіювання особистих ключів серверів ЦСК (в тому числі для переносу на резервний мережевий криптомодуль);
- формування сертифіката ЦСК (або запиту до центрального засвідчу вального органу);
- формування сертифікатів серверів ЦСК;
- генерація особистих ключів та формування сертифікатів адміністраторів реєстрації ЦСК.

Генерація особистого ключа ЦСК повинна здійснюватися у встановленому центром сертифікації ключів порядку (згідно регламенту ЦСК). Генерація повинна виконуватись з використанням криптомодуля.

Генерація особистих ключів серверів ЦСК також повинна здійснюватися згідно регламенту ЦСК з використанням мережевого криптомодуля (програмно-апаратного засобу КЗІ).

Формування сертифікатів серверів ЦСК повинне здійснюватися згідно регламенту ЦСК.



## 4.2 Підготовка персоналу

### 4.2.1 Підготовка адміністратора безпеки

Підготовка адміністратора безпеки включає проведення навчання з:

- адміністрування і аудиту ОС та її штатного КЗЗ серверів ЦСК;
- адміністрування і аудиту СУБД та її штатного КЗЗ серверів ЦСК;
- адміністрування і аудиту системного ПЗ та його штатного КЗЗ серверів взаємодії;
- управління комутаторами;
- управління МЕ;
- підключення мережових криптомодулів;
- інсталяції програмного комплексу ЦСК;
- встановлення параметрів програмного комплексу ЦСК;
- налаштування КЗЗ програмного забезпечення ІТС ЦСК;
- інсталяції програмного комплексу віддаленого моніторингу засобів центрального сервера (у т.ч. програмного комплексу ЦСК та мережних криптомодулів);
- встановлення параметрів програмного комплексу моніторингу;
- дій у випадках аварійних ситуацій та відмов засобів тощо.

### 4.2.2 Підготовка адміністратора сертифікації та системного адміністратора

Підготовка адміністратора сертифікації та системного адміністратора включає проведення навчання з:

- налагодження параметрів технічних засобів комплексу та системного програмного забезпечення;
- діагностування роботи технічних засобів комплексу;
- моніторингу стану технічних засобів комплексу;
- ініціювання публікації реєстру сертифікатів у загальнодоступних каталогах (LDAP-каталогах) та на інформаційному ресурсі ЦСК (web-сторінці) сервером ЦСК;
- розсилання реєстрів сертифікатів користувачам засобами електронної пошти;
- ініціювання формування списків відкликаних сертифікатів користувачів сервером ЦСК;
- ініціювання публікації списків відкликаних сертифікатів у загальнодоступних каталогах (LDAP- каталогах) та на інформаційному ресурсі ЦСК (web-сторінці) сервером ЦСК;
- оповіщення користувачів про зміну статусу сертифікатів засобами електронної пошти;
- ініціювання публікації сертифікату ЦСК у загальнодоступних каталогах (LDAP-каталогах) та на інформаційному ресурсі ЦСК (web-сторінці) сервером ЦСК;
- генерації особистого та відкритого ключів ЦСК;
- введення та використання особистого ключа ЦСК;
- створення резервних копій особистого ключа ЦСК, а також відновлення особистого ключа з резервних копій;
- формування та передачі запиту на формування сертифіката ЦСК до ЦЗО;
- отримання та запису сертифікату ЦСК у реєстр сертифікатів;
- публікації сертифікату ЦСК на інформаційному ресурсі (на веб-сторінці сервера взаємодії);
- публікації списків відкликаних сертифікатів на інформаційному ресурсі ЦСК (на веб-сторінці);
- приймання запитів на формування сертифікатів користувачів та посадових осіб (адміністраторів);
- формування сертифікатів на основі запиту шляхом, що включає підпис сертифікатів (з використанням особистого ключа ЦСК);
- формування списків відкликаних сертифікатів користувачів шляхом, що включає підпис списків відкликаних сертифікатів (з використанням особистого ключа ЦСК);
- ручного резервного копіювання та архівування реєстру сертифікатів;
- моніторингу та контролю виконання автоматизованих функцій, зокрема:
  - публікації реєстру сертифікатів на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці) центральним сервером;
  - публікації списків відкликаних сертифікатів на інформаційному ресурсі центральним сервером;
  - публікації сертифікату ЦСК на інформаційному ресурсі центральним сервером.

#### 4.2.3 Підготовка адміністратора реєстрації

Підготовка адміністратора реєстрації включає проведення навчання з:

- введення реєстраційних даних користувачів до реєстру користувачів;
- зміни реєстраційних даних користувачів у реєстрі;
- видалення реєстраційних даних користувачів з реєстру;
- приймання та введення запитів користувачів на формування сертифікатів відкритих ключів на носіях інформації;
- приймання та введення запитів користувачів на скасування, блокування чи поновлення сертифікатів на носіях інформації;
- ініціювання скасування, блокування чи поновлення сертифікатів користувачів сервером ЦСК;
- генерації особистого та відкритого ключів адміністратора реєстрації;
- введення та використання особистих ключів адміністратора реєстрації;
- формування та передачі запиту на формування сертифіката адміністратора реєстрації на сервер ЦСК;
- отримання, зберігання та використання сертифікату адміністратора реєстрації.

## 5 ВИМОГИ ДО ОБЛАШТУВАННЯ ПРИМІЩЕНЬ АС ЦСК

### 5.1 Вимоги до облаштування приміщень

5.1.1 Виконання вимог пожежної безпеки, електричної безпеки та виконання санітарно-гігієнічних норм охорони праці повинно забезпечуватись як на етапі будівельно-монтажних, так і на етапі пусконаладжувальних робіт.

5.1.2 Приміщення ЦСК (спеціальні приміщення) повинні бути обладнані у відповідності до вимог діючих нормативних документів із захисту інформації.

5.1.3 До складу приміщень ЦСК повинні входити:

- серверне приміщення з шафками серверів ЦСК;
- робочі приміщення обслуговуючого персоналу (приміщення адміністраторів ЦСК) з робочими місцями (РМ).

5.1.4 Всі приміщення повинні бути розташовані на одному поверсі.

5.1.5 У робочому приміщенні обслуговуючого персоналу повинні розміщатися РМ з РС адміністратора безпеки, системного адміністратора та адміністратора реєстрації. Всі РС повинні бути реалізовані на базі ПЕОМ (або портативного комп'ютера) та підключатися до комутатора РС. Приміщення повинно бути обладнане системою охоронної та пожежної сигналізації, а також системою кондиціонування.

5.1.6 У серверному приміщенні повинна бути розміщена шафа з серверами ЦСК - екранована шафа центральних серверів та серверів взаємодії (або може бути створене екрановане приміщення). Підключення до комутатора РС повинне здійснюватися через ВОЛЗ. Підключення до ЗТМ може здійснюватися або через ВОЛЗ або за допомогою електричного кабелю через позамережний хвилевід. Приміщення повинно бути обладнане системою охоронної та пожежної сигналізації, а також окремою системою кондиціонування.

5.1.7 Світильники внутрішнього освітлення у приміщеннях ЦСК мають бути встановлені згідно існуючих норм у відповідності до розміщення РМ обслуговуючого персоналу, шаф серверів тощо.

5.1.8 Двері робочого приміщення та двері серверного приміщення мають бути обладнані електронним замком та магнітоконтатним датчиком охоронної сигналізації.

5.1.9 У стінах всіх приміщень ЦСК повинні бути передбачені отвори для введення комунікацій (ліній пожежної та охоронної сигналізації, заземлення, силових фідерів (ліній) електроживлення та ін.).

### 5.2 Вимоги до системи електроживлення та електричної безпеки

5.2.1 Силові фідери повинні бути розраховані на струм не менше 50 А і виконані кабелями типу АВВГ (АВРГ або аналогічними) у гнучких екранах або трубах. Силовий щит, від якого здійснюється електроживлення внутрішнього обладнання приміщень, повинен мати автоматичні запобіжники на струм 30 А.

5.2.2 До екранованої шафи (центральных серверів та серверів взаємодії) у серверному приміщенні електроживлення повинно підводитися трьохжильним мідним кабелем у екрані з площею перерізу кожного дроту не менше 2,5 мм<sup>2</sup>. Екран кабелю повинен бути з'єднаний з корпусом екранованої шафи тільки на вводі (з металевим корпусом внутрішнього фільтра завад у шафі).

5.2.3 Кабелі до екранованої шафи серверів в серверному приміщенні повинні бути підключені до двох окремих фідерів електроживлення через автомат вводу резервного живлення.

5.2.5 До РС обслуговуючого персоналу електроживлення повинно підводитися від щита трьохжильним мідним кабелем з площею перерізу кожного дроту не менше 1 мм<sup>2</sup>. Третій ("земляний") провід кабелю підключається до заземлення. Заземлення повинно бути виконане за допомогою окремого контуру заземлення. Біля РС персоналу та у зазначених на схемах місцях мають бути встановлені набори з чотирьох розеток.

5.2.6 Електроживлення кондиціонерів повинно бути здійснено безпосередньо від силових щитів вводу електроживлення. Навантаження фаз повинно бути збалансованим.

5.2.7 У серверному приміщенні повинен бути створений окремий контур заземлення.

5.2.8 Опір заземлення не повинен перевищувати 4 Ом. Елементи заземлення повинні бути підключені до точки вводу заземлення (розподільного щита заземлення) у одній точці. Підключення має

бути здійснено мідним ізольованим кабелем перерізом не менше 3,5 мм<sup>2</sup> з перехідним опором з'єднань не більше 600 мкОм.

5.2.9 Кабелі заземлення корпусів екранованих шаф, всіх металевих частин електроприладів, дроти заземлення розеток повинні бути підключені до болтів (шпильок) розподільчого щитка заземлення по схемі "зірка". Послідовне включення не дозволяється.

5.2.10 При обладнанні системи електроживлення приміщення повинні бути враховані вимоги ПУЕ щодо електричної безпеки, ізоляції струмоведучих частин, попереджувальних написів, тощо.

### 5.3 Вимоги до системи протипожежної безпеки

5.3.1 Всі приміщення ЦСК мають бути обладнані датчиками пожежної сигналізації (димовими та тепловими). Лінії датчиків заводяться на центральний пульт пожежної сигналізації будівлі, який розміщується на посту охорони будівлі. Місця встановлення датчиків повинні бути уточнені на місці згідно існуючих норм.

5.3.2 Приміщення мають бути обладнані вуглекислотними вогнегасниками згідно існуючих норм.

### 5.4 Вимоги до системи кондиціонування повітря

5.4.1 Всі приміщення ЦСК повинні бути обладнані системами кондиціонування повітря.

5.4.2 У серверному приміщенні має бути встановлена система кондиціонування, розрахована на потужність охолодження, яка забезпечить температуру повітря 18-24°C і відносну вологість не більше ніж 60% незалежно від пори року. Вихід холодного повітря з кондиціонера повинен бути направлений безпосередньо на шафи серверів.

5.4.3 У робочих приміщеннях має бути встановлена система кондиціонування, розраховані на потужність охолодження, яка забезпечить температуру повітря 18- 24°C і відносну вологість не більше ніж 60% незалежно від пори року. Вихід холодного повітря з кондиціонера не повинен бути направлений безпосередньо на РМ обслуговуючого персоналу.

5.4.4 Зовнішні блоки кондиціонерів мають бути встановлені в межах контрольованої зони (на зовнішніх стінах будівлі, які виходять на подвір'я та фасад будівлі).

### 5.5 Вимоги до системи охоронної сигналізації

5.5.1 Всі приміщення ЦСК мають бути обладнані системами охоронної сигналізації.

5.5.2. На всіх дверях приміщень мають бути встановлені магнітоконтактні датчики, а самі двері обладнані електронними замками. У всіх приміщеннях повинні бути встановлені датчики руху.

5.5.3. Лінії датчиків з робочих та серверного приміщень повинні бути заведені на охоронний пристрій (пульт), який розміщується на посту охорони будівлі. Довжина ліній датчиків - до 200 м. Місця встановлення датчиків повинні бути уточнені згідно технічних особливостей та вимог до розміщення окремих типів датчиків.

5.5.4. Включення та відключення системи охоронної сигналізації повинно здійснюватися з поста охорони за допомогою пульта охоронної сигналізації.

5.5.5 Для оповіщення охорони будівлі повинні бути передбачені сигнальні лінії від охоронного пристрою до центрального пульта, який розміщується на посту охорони будівлі. Повинні бути виведені дві лінії, які відповідають за дві окремі зони - за робочі приміщення (приміщення адміністраторів) та окремо за серверне приміщення.

### 5.6 Вимоги до системи відеоспостереження

5.6.1 Серверне приміщення ЦСК повинне бути обладнано системою відеоспостереження, яка призначена для постійного запису відеоінформації на сервер (пристрій) відеозапису.

5.6.2 Лінії від відеокамер з серверного приміщення повинні бути заведені на сервер (пристрій) відеозапису, який розміщується в окремому серверному приміщенні. Місця встановлення відеокамер повинні бути уточнені згідно технічних особливостей та вимог до розміщення окремих типів відеокамер.

5.6.3 Зображення з відеокамери, встановленої у серверному приміщенні передається безпосередньо на відеомонітор у приміщенні обслуговуючого персоналу.

### 5.7 Вимоги до системи телефонного зв'язку та ЛОМ

5.7.1 До приміщень ЦСК має бути проведена телефонна лінія для підключення прямого міського номера.

5.7.2 ВОЛЗ локальної мережі передачі даних (ЛОМ) прокладаються по стінах робочих приміщень, підвісній стелі та кабельних каналах в стінах від серверів до комутатора РС згідно вимог до структурованих кабельних мереж. Довжина інформаційних ліній - до 50 м.

5.7.3 Для підключення серверів взаємодії до ЗТМ в серверне приміщення повинні бути проведені інформаційні лінії (ВОЛЗ чи електричний кабель) від комутаційної шафи будівлі. Довжина інформаційних ліній - до 200 м.

5.7.4 GPS-приймач повинен бути змонтований на металевому кронштейні довжиною 1,5 м на зовнішній стіні будівлі. З'єднувальний фідер повинен бути прокладений по зовнішній стіні будівлі у гофрованій трубі та вводиться у серверне приміщення до сервера моніторингу та синхронізації часу через отвір у стіні.

5.7.5 До робочого місця адміністратора реєстрації необхідно підвести телефонну розетку від міської АТС. Всі інші робочі місця обслуговуючого персоналу повинні бути обладнані телефонами внутрішньої АТС будівлі.

5.7.6 Інформаційні лінії кабелю локальної мережі передачі даних (ЛОМ) прокладаються по стінах робочих приміщень від комутатора РС до робочих місць адміністраторів згідно вимог до структурованих кабельних мереж. Довжина інформаційних ліній - до 25 м (уточнюється по місцю). В місцях встановлення інформаційних розеток повинні бути виведені по дві окремі розетки. Тип кабелю - вита пара категорії 5.