

ЗАТВЕРДЖЕНО
ЄААД.468244.185-ЛУ

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

Центр сертифікації ключів
ринку електричної енергії

Опис КТЗ

ЄААД.468244.185.П9.01

ЗМІСТ

1 СТРУКТУРА КТЗ	4
1.1 Склад КТЗ	4
1.2 Опис розміщення КТЗ	4
2 ЗАСОБИ ЕОТ	5
2.1 Склад засобів ЕОТ	5
2.2 Характеристики засобів ЕОТ	5
2.2.1 Центральні сервери ЦСК	5
2.2.2 Сервери взаємодії	5
2.2.3 РС адміністратора безпеки	5
2.2.4 РС адміністратора сертифікації та системного адміністратора	5
2.2.5 РС адміністратора реєстрації	6
2.2.6 РС генерації ключів користувачів	6
2.2.7 Дисковий масив	6
2.2.8 Обладнання синхронізації часу (GPS-приймач);	6
2.2.8 Обладнання сповіщення адміністраторів (GSM-модуль);	6
2.2.9 Сервер моніторингу та синхронізації часу	6
3 КОМУНІКАЦІЙНЕ ОБЛАДНАННЯ	7
3.1 Склад комунікаційного обладнання	7
3.2 Характеристики комунікаційного обладнання	7
3.2.1 Комутатор ЛОМ ЦСК	7
3.2.2 Комутатор РС	7
3.2.3 ME	7

ПЕРЕЛІК СКОРОЧЕНЬ

БД	- База даних
ВОЛЗ	- Волоконно-оптичні лінії зв'язку
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
КЗЗ	- Комплекс засобів захисту
КЗІ	- Криптографічний захист інформації
КТЗ	- Комплекс технічних засобів
КСЗІ	- Комплексна система захисту інформації
ЛОМ	- Локальна обчислювальна мережа
МЕ	- Міжмережний екран
НКІ	- Носій ключової інформації
НМС	- Накопичувач на магнітній стрічці
ОС	- Операційна система
ПЕОМ	- Персональна ЕОМ або портативний комп'ютер
ПЗ	- Програмне забезпечення
ПЗП	- Постійний запам'ятовуючий пристрій
ПРД	- Правила розмежування доступу
ПТК	- Програмно-технічний комплекс
РС	- Робоча станція
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)
HTTP	- Hyper Text Transfer Protocol
LDAP	- Lightweight Directory Access Protocol (протокол доступу до каталогу)
MTA	- Mail Transfer Agent (модуль передачі електронних поштових повідомлень)
OCSP	- Online Certificate Status Protocol (протокол визначення статусу сертифіката)
TSP	- Time-Stamp Protocol (протокол отримання позначок часу)

1 СТРУКТУРА КТЗ

Структуру КТЗ наведено на структурній схемі КТЗ (документ ЄААД.468244.185.С1).

Кількість та характеристики технічних засобів наведено у специфікації обладнання ЄААД.468244.185.В4.

1.1 Склад КТЗ

До складу комплексу входять такі технічні засоби:

- центральні сервери (сервери ЦСК) (кластер);
- сервери взаємодії (кластер);
- сервер моніторингу та синхронізації часу;
- дисковий масив;
- обладнання синхронізації часу (GPS-приймач);
- обладнання сповіщення адміністраторів (GSM-модуль);
- комутатори (ЛОМ та РС);
- РС генерації ключів користувачів (ізолювана);
- РС обслуговуючого персоналу (адміністратора безпеки, системного адміністратора, адміністратора реєстрації та адміністратора сертифікації).

При роботі комплексу з ним взаємодіють такі технічні засоби, які фізично не входять до його складу:

- технічні засоби користувачів ЦСК ІТС (або зовнішніх ІТС).

Технічні засоби користувачів ЦСК підключається до комплексу через телекомунікаційні мережі.

Функції КТЗ визначено в загальному описі системи (документ ЄААД.468244.185.ПД.01).

Структуру КТЗ наведено на структурній схемі КТЗ (документ ЄААД.468244.185.С1).

Функціональну структуру комплексу наведено на схемі функціональної структури (документ ЄААД.468244.185.С2).

Детальний опис програмного забезпечення наведено в описі програмного забезпечення (документ ЄААД.468244.185.ПА.01).

1.2 Опис розміщення КТЗ

Для розміщення РС обслуговуючого персоналу (адміністратора безпеки, системного адміністратора, адміністратора реєстрації та адміністратора сертифікації) обладнуються окремі робочі місця у приміщенні адміністраторів. Адміністратор сертифікації та системний адміністратор використовують спільну РС.

Центральні сервери ЦСК, сервери взаємодії, комутатор ЛОМ та МЕ розміщуються у екранованій шафі в серверній кімнаті ДП "ЕНЕРГОРИНОК" (неекрановане серверне приміщення). Сервер моніторингу та синхронізації часу розташований у цьому ж приміщенні у окремій серверній стійці,

2 ЗАСОБИ ЕОТ

2.1 Склад засобів ЕОТ

До складу засобів ЕОТ, що входять до КТЗ відносяться:

- центральні сервери (сервери ЦСК) (кластер);
- сервери взаємодії (кластер);
- сервер моніторингу та синхронізації часу;
- РС генерації ключів користувачів (ізольована);
- РС обслуговуючого персоналу (адміністратора безпеки, системного адміністратора, адміністратора реєстрації та адміністратора сертифікації).

2.2 Характеристики засобів ЕОТ

2.2.1 Центральні сервери ЦСК

Сервери ЦСК реалізовані на основі ЕОМ серверного типу.

До складу технічних засобів серверів входять:

- ЕОМ серверного типу;
- монітор та пристрої вводу (клавіатура та маніпулятор “миша”) - термінал;

Управління серверами ЦСК здійснюється локально через термінал або віддалено з РС адміністратора безпеки та системного адміністратора.

Сервери у кластері рівноцінні.

Центральні сервери виконую функції обробки CMP-, TSP-, OCSP -запитів та сервера БД. Синхронізація даних у БД здійснюється за рахунок використання спільного дискового сховища.

У криптомодулях зберігається та використовується особистий ключ ЦСК.

Для управління двома серверами через один термінал використовується комутатор терміналів.

2.2.2 Сервери взаємодії

Сервери взаємодії реалізовані на основі ЕОМ серверного типу.

До складу технічних засобів серверів входять:

- ЕОМ серверного типу.

Управління серверами взаємодії здійснюється локально через термінал або віддалено з РС адміністратора безпеки.

Сервери у кластері рівноцінні.

Для управління обома серверами через один термінал використовується комутатор терміналів (той же що й для центральних серверів).

2.2.3 РС адміністратора безпеки

РС адміністратора безпеки реалізована на основі ПЕОМ (персональна ЕОМ або портативний комп'ютер).

До складу технічних засобів РС входять:

- системний блок ПЕОМ;
- монітор;
- ДБЖ;
- пристрої вводу (клавіатура та маніпулятор “миша”).

2.2.4 РС адміністратора сертифікації та системного адміністратора

РС адміністратора сертифікації реалізована на основі ПЕОМ (персональна ЕОМ або портативний комп'ютер).

До складу технічних засобів РС входять:

- системний блок ПЕОМ;
- монітор;
- ДБЖ;
- пристрої вводу (клавіатура, маніпулятор “миша”)
- пристрій для друку (принтер).

2.2.5 РС адміністратора реєстрації

РС адміністратора реєстрації реалізована на основі ПЕОМ(персональна ЕОМ або портативний комп'ютер).

До складу технічних засобів РС входять:

- системний блок ПЕОМ;
- монітор;
- ДБЖ;
- пристрої вводу (клавіатура, маніпулятор “миша”)
- БФП(виконує функції принтера, сканера, ксерокса).

РС віддаленого адміністратора реєстрації за складом не відрізняється від РС адміністратора реєстрації.

2.2.6 РС генерації ключів користувачів

РС генерації ключів користувачів реалізована на основі ПЕОМ у захищеному виконанні.

До складу технічних засобів РС входять:

- системний блок ПЕОМ з апаратним генератором випадкових чисел;
- монітор;
- ДБЖ;
- пристрої вводу (клавіатура, маніпулятор “миша”).

2.2.7 Дисковий масив

Дисковий масив є спеціалізованою ЕОМ, призначеною для надання серверам єдиного інтерфейсу до НЖМД, об'єднаних у надлишкові RAID.

2.2.8 Обладнання синхронізації часу (GPS-приймач);

Обладнання реалізоване у вигляді виносного GPS-приймача, який з'єднується з сервером моніторингу USB-кабелем.

2.2.8 Обладнання сповіщення адміністраторів (GSM-модуль);

Обладнання реалізоване у вигляді виносного GSM-модему, який з'єднується з сервером моніторингу кабелем з інтерфейсом RS-232.

2.2.9 Сервер моніторингу та синхронізації часу

Сервер моніторингу та синхронізації часу

До складу технічних засобів сервера входять:

- ЕОМ серверного типу;
- ДБЖ.

Для управління сервером через один термінал використовується комутатор терміналів (той же що й для центральних серверів).

3 КОМУНІКАЦІЙНЕ ОБЛАДНАННЯ

3.1 Склад комунікаційного обладнання

До складу комунікаційного обладнання, що входить до КТЗ відносяться:

- комутатор ЛОМ ЦСК;
- комутатор РС;
- МЕ.

3.2 Характеристики комунікаційного обладнання

3.2.1 Комутатор ЛОМ ЦСК

Комутатор ЛОМ призначено для об'єднання на основі кабельної мережі РС адміністратора безпеки, системного адміністратора, адміністратора реєстрації, серверів ЦСК та серверів взаємодії.

Управління комутатором здійснюється з локальної консолі, яка підключається безпосередньо до консольного порту комутатора або з РС адміністратора безпеки.

Управління з локальної консолі застосовується при первинному налагодженні та в аварійних ситуаціях з використанням командного інтерфейсу.

Комутатор ЛОМ розміщується в стійці разом з серверами взаємодії, центральними серверами та МЕ.

3.2.2 Комутатор РС

Комутатор РС призначено для об'єднання на основі кабельної мережі РС адміністратора безпеки, системного адміністратора, адміністратора реєстрації, серверів ЦСК та серверів взаємодії.

Управління комутатором здійснюється з локальної консолі, яка підключається безпосередньо до консольного порту комутатора або з РС адміністратора безпеки.

Управління з локальної консолі застосовується при первинному налагодженні та в аварійних ситуаціях з використанням командного інтерфейсу.

Комутатор РС розміщується в кімнаті адміністраторів ЦСК.

3.2.3 МЕ

МЕ призначено для захисту серверів взаємодії та мережі ЦСК від можливих зловмисних дій з зовнішніх по відношенню до ЦСК комунікаційних мереж, шляхом аналізу та блокування шкідливого трафіку та обмеження доступу по портах.

Управління МЕ здійснюється з локальної консолі, яка підключається безпосередньо до консольного порту МЕ або з РС адміністратора безпеки.

Управління з локальної консолі застосовується при первинному налагодженні та в аварійних ситуаціях з використанням командного інтерфейсу.

МЕ розміщується в стійці разом з серверами взаємодії, центральними серверами.