

ЗАТВЕРДЖЕНО
ЄААД.468244.185-ЛУ

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

**Центр сертифікації ключів
ринку електричної енергії**

Опис програмного забезпечення

ЄААД.468244.185.ПА.01

ЗМІСТ

1 СТРУКТУРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	4
1 СТРУКТУРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	4
2 СКЛАД ТА ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	5
2.1 ПЗ центральних серверів ЦСК	5
2.2 ПЗ серверів взаємодії	5
2.3 ПЗ ПЗ сервера моніторингу та синхронізації часу	5
2.4 ПЗ РС адміністратора сертифікації та системного адміністратора	6
2.5 ПЗ РС адміністратора безпеки	6
2.6 ПЗ РС адміністратора реєстрації	7
2.7 ПЗ РС генерації ключів користувачів	7
3 ТИП ТА ХАРАКТЕРИСТИКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	8

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
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 ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Структура програмного забезпечення (ПЗ) наведена за принципом його використання на технічних засобах (засобах ЕОТ) комплексу.

Функціональна структура комплексу наведена на схемі функціональної структури (документ ЄААД.468244.185.С2).

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

Структура КТЗ наведена на структурній схемі КТЗ (документ ЄААД.468244.185.С1)

Детальний опис та характеристики КТЗ (засобів ЕОТ та комунікаційного обладнання) наведений у описі КТЗ ЄААД.468244.185.П9.01.

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).

2 СКЛАД ТА ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1 ПЗ центральних серверів ЦСК

До складу системного програмного забезпечення сервера входять:

- ОС із штатним КЗЗ;
- СУБД із штатним КЗЗ;
- засоби доступу до LDAP-сервера.

ОС із штатним КЗЗ призначено для забезпечення загальносистемного функціонування сервера та захисту ресурсів сервера від НСД.

СУБД призначено для зберігання та забезпечення доступу до таблиць та інших ресурсів БД з боку ПЗ РС адміністратора безпеки, адміністраторів реєстрації та сертифікації.

До складу спеціального програмного забезпечення сервера входять:

- програмний комплекс ключів ЦСК та серверів ЦСК;
- програмний комплекс серверів ЦСК.

Програмні комплекси сервера ЦСК призначено для реалізації функціональних завдань сервера.

2.2 ПЗ серверів взаємодії

До складу системного ПЗ сервера входять:

- ОС із штатним КЗЗ;
- HTTP-сервер з СУБД та модулями формування HTML-документів із штатним КЗЗ;
- LDAP-сервер із штатним КЗЗ;
- модуль передачі електронних поштових повідомлень (MTA) та поштовий сервер із штатними КЗЗ.

ОС із штатним КЗЗ призначено для забезпечення загальносистемного функціонування сервера та захисту ресурсів сервера від НСД.

HTTP-сервер призначено для забезпечення доступу до інформації на сервері взаємодії за протоколом HTTP шляхом представлення інформації для кінцевого користувача у вигляді web-сторінки (HTML-документа).

СУБД призначено для зберігання та забезпечення доступу до таблиць та інших ресурсів БД з боку HTTP-сервера для заповнення чи зчитування інформації для web-сторінки.

Модулі формування HTML-документів призначено для виконання та інтерпретації скриптів динамічної web-сторінки з використанням даних з БД для формування HTML-документів, що передаються кінцевому користувачу.

Модуль передачі електронних поштових повідомлень (MTA) та поштовий сервер призначено для зберігання, відправки та прийому електронних поштових повідомлень між засобами ЕОТ ЛОМ та зовнішніми кінцевими користувачами.

До складу функціонального ПЗ сервера входить програмний комплекс сервера взаємодії.

Програмний комплекс сервера ЦСК призначено для реалізації функціональних завдань сервера.

Управління сервером взаємодії здійснюється локально або з РС адміністратора безпеки чи системного адміністратора.

2.3 ПЗ ПЗ сервера моніторингу та синхронізації часу

До складу системного ПЗ сервера входять:

- ОС із штатним КЗЗ.

ОС із штатним КЗЗ призначено для забезпечення загальносистемного функціонування сервера та захисту ресурсів сервера від НСД.

До складу функціонального ПЗ сервера входить

- програмний комплекс NTP-сервера;
- програмний комплекс моніторингу.

Програмний комплекс NTP-сервера призначено для надання усім іншим компонентам ЦСК сигналів точного часу для синхронізації.

Програмний комплекс моніторингу призначено для перевірки доступності усіх інших компонентів ЦСК.

Управління сервером моніторингу та синхронізації часу здійснюється локально або з РС адміністратора безпеки чи системного адміністратора.

2.4 ПЗ РС адміністратора сертифікації та системного адміністратора

До складу системного ПЗ РС входять:

- ОС із штатним КЗЗ;
- засоби антивірусного захисту;
- засоби доступу до БД сервера ЦСК;
- засоби електронної пошти;
- засоби адміністрування системного ПЗ сервера взаємодії.

ОС із штатним КЗЗ призначено для забезпечення загальносистемного функціонування РС та захисту ресурсів РС від НСД.

Засоби доступу до БД сервера ЦСК є частиною ОС або ПЗ СУБД та призначені для забезпечення доступу функціонального ПЗ до таблиць та інших ресурсів БД сервера ЦСК.

Засоби електронної пошти призначені для відправки та прийому електронних поштових повідомлень через сервер взаємодії, на якому виконується модуль передачі поштових повідомлень (поштовий сервер).

До складу функціонального ПЗ РС входить програмний комплекс адміністратора сертифікації.

Програмний комплекс адміністратора сертифікації призначено для реалізації функціональних завдань РС.

Засоби адміністрування системного ПЗ сервера взаємодії призначено для інсталяції та конфігурування системного ПЗ сервера взаємодії і є частиною ПЗ сервера та виконуються безпосередньо на сервері. Для адміністрування через ЛОМ використовується програмний термінал, що емулює локальний термінал сервера.

2.5 ПЗ РС адміністратора безпеки

До складу системного ПЗ РС входять:

- ОС із штатним КЗЗ;
- засоби антивірусного захисту;
- засоби адміністрування та аудиту ОС та її штатного КЗЗ центральних серверів ЦСК;
- засоби адміністрування та аудиту СУБД та її штатного КЗЗ центральних серверів ЦСК;
- засоби адміністрування та аудиту системного ПЗ та його штатного КЗЗ сервера взаємодії;
- засоби управління комутатором ЛОМ;
- засоби управління МЕ.

ОС із штатним КЗЗ призначена для забезпечення загальносистемного функціонування РС та захисту ресурсів РС від НСД.

Засоби адміністрування та аудиту ОС та її штатного КЗЗ серверів ЦСК є частиною ОС серверів ЦСК та виконуються безпосередньо на серверах. Для адміністрування через ЛОМ використовується програмний термінал, що емулює локальний термінал сервера.

Засоби адміністрування та аудиту ОС та її штатного КЗЗ серверів ЦСК є частиною ОС та клієнтської частини ПЗ СУБД.

Засоби адміністрування та аудиту системного ПЗ та його штатного КЗЗ сервера взаємодії є частиною ПЗ сервера та виконуються безпосередньо на сервері. Для адміністрування через ЛОМ використовується програмний термінал, що емулює локальний термінал сервера.

Засоби управління комутатором є частиною ПЗ ОС комутатора та виконуються безпосередньо на комутаторі. Для адміністрування через ЛОМ використовується програмний термінал, що емулює локальну консоль комутатора.

Засоби управління МЕ можуть бути:

- частиною ПЗ ОС МЕ та виконуватися безпосередньо на МЕ, при цьому для адміністрування через ЛОМ використовується програмний термінал, що емулює локальну консоль МЕ;
- спеціальним ПЗ, що розподілено та виконується на РС та МЕ і взаємодіє через ЛОМ з ОС МЕ.

До складу функціонального ПЗ РС входить програмний комплекс адміністратора безпеки.

2.6 ПЗ РС адміністратора реєстрації

До складу системного ПЗ РС входять:

- ОС із штатним КЗЗ;
- засоби антивірусного захисту;
- засоби доступу до БД сервера ЦСК;
- засоби електронної пошти.

ОС із штатним КЗЗ призначена для забезпечення загальносистемного функціонування РС та захисту ресурсів РС від НСД.

Засоби доступу до БД сервера ЦСК є частиною ОС або ПЗ СУБД та призначені для забезпечення доступу функціонального ПЗ до таблиць та інших ресурсів БД СУБД.

До складу функціонального ПЗ РС входить програмний комплекс адміністратора реєстрації.

Програмний комплекс адміністратора реєстрації призначений для реалізації функціональних завдань РС.

2.7 ПЗ РС генерації ключів користувачів

До складу системного ПЗ РС входить ОС із штатним КЗЗ та засоби антивірусного захисту.

ОС із штатним КЗЗ призначено для забезпечення загальносистемного функціонування сервера та захисту ресурсів сервера від НСД.

До складу функціонального ПЗ РС входить програмний комплекс робочої станції генерації ключів користувачів ЦСК, який призначено для реалізації функціональних завдань РС.

3 ТИП ТА ХАРАКТЕРИСТИКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Тип та характеристики програмного забезпечення за розміщенням на засобах ЦСК із зазначенням версій та інших характеристик наведено в табл. 1.

Таблиця 1 - Тип та характеристики програмного забезпечення.

ПЗ	Тип та характеристики	
Центральний сервер	ОС із штатним КЗЗ	Microsoft Windows 2012 Server R2 Standard
	Засоби антивірусного захисту	ESET Endpoint Security 5
	СУБД із штатним КЗЗ та засобами їх адміністрування	Microsoft SQL Server 2012
	Засоби доступу до LDAP-сервера	Штатні ОС
	Програмний комплекс сервера ЦСК (програмний комплекс управління ключами ЦСК, програмний комплекс CMP-сервера, програмний комплекс TSP-сервера, програмний комплекс OCSP-сервера, службового програмний комплекс ЦСК)	ІТ ЦСК-1. Ключі ЦСК та серверів ЦСК ІТ ЦСК-1. Сервер обробки запитів ЦСК ІТ ЦСК-1. TSP-сервер ІТ ЦСК-1. OCSP-сервер ІТ ЦСК-1. Службові модулі сервера ЦСК
Сервер взаємодії	ОС із штатним КЗЗ	FreeBSD 9.2
	HTTP-сервер з СУБД та модулями формування HTML-документів із штатним КЗЗ	HTTP-сервер Apache 2.2.22 СУБД MySQL Модуль формування HTML-документів PHP 5.3.28
	LDAP-сервер із штатним КЗЗ	Open LDAP 2.4.40
	Модуль передачі електронних поштових повідомлень (MTA) та поштовий сервер із штатним КЗЗ	Exim 4.84
	Програмний комплекс сервера взаємодії	ІТ ЦСК-1. Сервер взаємодії
PC адміністратора сертифікації та системного адміністратора	ОС із штатним КЗЗ	Microsoft Windows 8.1 Enterprise
	Засоби антивірусного захисту	ESET Endpoint Security 5
	Засоби доступу до БД сервера ЦСК	Штатні ODBC-драйвера ОС
	Засоби електронної пошти	Штатні ОС
	Програмний комплекс адміністратора сертифікації	ІТ ЦСК-1. Адміністратор сертифікації
	Засоби адміністрування системного ПЗ сервера взаємодії	Термінальний клієнт SSH
PC адміністратора безпеки	ОС із штатним КЗЗ	Microsoft Windows 8.1 Enterprise
	Засоби антивірусного захисту	ESET Endpoint Security 5
	Засоби адміністрування та аудиту ОС та її штатного КЗЗ сервера ЦСК	Microsoft Remote Desktop Connection (термінальний клієнт)
	Засоби адміністрування та аудиту СУБД сервера ЦСК	Штатні зі складу інсталляційного пакету Oracle та штатні ODBC-драйвери ОС
	Засоби адміністрування та аудиту системного ПЗ та його штатного КЗЗ сервера взаємодії	Термінальний клієнт SSH
	Засоби управління комутатором	Термінальний клієнт SSH
	Засоби управління ME	Термінальний клієнт SSH, HTTPS-клієнт
	Програмний комплекс адміністратора безпеки	ІТ ЦСК-1. Адміністратор безпеки
PC адміністратора	ОС із штатним КЗЗ	Microsoft Windows 8.1 Enterprise

реєстрації	Засоби антивірусного захисту	ESET Endpoint Security 5
	Засоби електронної пошти	Штатні ОС
	Програмний комплекс адміністратора реєстрації	ІІТ ЦСК-1. Адміністратор реєстрації
РС генерації ключів користувачів	ОС із штатним КЗЗ	Microsoft Windows 8.1 Enterprise
	Засоби антивірусного захисту	ESET Endpoint Security 5
	Програмний комплекс робочої станції генерації ключів користувачів ЦСК	ІІТ ЦСК-1. РС генерації ключів користувачів ЦСК
Сервер синхронізації часу та моніторингу	ОС із штатним КЗЗ	Linux openSUSE
	NTP-сервер	Штатний ОС

Примітка. Версії системного програмного забезпечення не є фіксованими та можуть змінюватись у відповідності до виходу нових версій даного ПЗ, або замінюватись на програмне забезпечення інших виробників відповідної функціональності.