

ЗАТВЕРДЖЕНО  
ЄААД.468244.185-ЛУ

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

## Центр сертифікації ключів ринку електричної енергії

Комплексна система захисту інформації.  
Комплекс засобів захисту

Загальний опис системи

ЄААД.468244.185.ПД.02

2014 р.

## ЗМІСТ

1 СКЛАД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМПЛЕКСУ ТЕХНІЧНИХ ЗАСОБІВ КЗЗ .....	4
2 ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМПЛЕКСУ ТЕХНІЧНИХ ЗАСОБІВ КЗЗ .....	5
2.1 Призначення ПЗ КЗЗ.....	5
2.1.1 КЗЗ операційної системи з лінійки Windows .....	5
2.1.2 КЗЗ СКБД Microsoft SQL Server 2012 .....	5
2.1.3 КЗЗ СКБД MySql.....	5
2.1.4 КЗЗ HTTP-сервера Apache .....	5
2.1.5 ОС серверів з лінійки Linux .....	5
2.1.6 Підсистема антивірусного захисту .....	6
2.2 Призначення КТЗ КЗЗ.....	6
2.2.1 Міжмережний екран .....	6
2.2.2 Електронні ключі "Кристал-1" .....	6
2.2.3 Мережні криптомодулі "Гряда-301" .....	6
2.2.4 Криptomодулі "Гряда-61" .....	7
3 ПОРЯДОК ЗАСТОСУВАННЯ КЗЗ.....	8
3.1 Використання елементів КЗЗ на засобах ЦСК .....	8
3.1.1 Використання елементів КЗЗ на РС адміністратора безпеки.....	8
3.1.2 Використання елементів КЗЗ на серверах .....	8
3.1.4 Використання пристрою міжмережної безпеки .....	8
3.2 Порядок налаштування параметрів КЗЗ .....	8

**ПЕРЕЛІК СКОРОЧЕНЬ**

БД	- База даних
ЕОМ	- Електронно-обчислювальна машина
ЕОТ	- Електронно-обчислювальна техніка
ЕЦП	- Електронний цифровий підпис
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
ОС	- Операційна система
ПЗ	- Програмне забезпечення
РС	- Робоча станція
СКБД	- Система керування базами даних
ЦСК	- Центр сертифікації ключів
HTTP	- Hyper Text Transfer Protocol
TSP	- Time-Stamp Protocol (протокол отримання позначок часу)

## 1 СКЛАД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМПЛЕКСУ ТЕХНІЧНИХ ЗАСОБІВ КЗЗ

Комплекс засобів захисту (КЗЗ) призначено для забезпечення конфіденційності, цілісності та доступності інформації, що циркулює та зберігається у, та забезпечення спостережливості, керованості систем, що входять до складу ЦСК.

До складу КЗЗ відносяться:

- КЗЗ локальної обчислювальної мережі;
- КЗЗ робочої станції генерації ключів;
- КЗЗ РС віддаленого адміністратора реєстрації;

КЗЗ локальної обчислювальної мережі складається з програмного забезпечення (ПЗ) та комплексу технічних засобів (КТЗ).

До складу ПЗ КЗЗ входить:

- КЗЗ операційної системи (далі - ОС) з лінійки Windows для РС;
- КЗЗ операційної системи з лінійки Windows для серверів;
- КЗЗ операційної системи з лінійки Linux для серверів;
- КЗЗ серверів, що складається з:
  - КЗЗ СКБД Microsoft SQL Server 2012;
  - КЗЗ СКБД MySql;
  - КЗЗ HTTP-сервера Apache;
- підсистема антивірусного захисту.

До складу КТЗ КЗЗ входить:

- міжмережний екран (далі - МЕ);
- комутатори ЛОМ ЦСК;
- електронні ключі "Кристал-1";
- мережеві криптомодулі "Грядда-301";
- криптомодулі "Грядда-61".

КЗЗ робочої станції генерації ключів та РС віддаленого адміністратора реєстрації складається з КЗЗ операційної системи з лінійки Windows для РС.

Опис ПЗ КЗЗ наведено у документі ЄААД.468244.185.ПА.02.

Опис КТЗ КЗЗ наведено у документі ЄААД.468244.185.П9.02.

## 2 ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМПЛЕКСУ ТЕХНІЧНИХ ЗАСОБІВ КЗЗ

### 2.1 Призначення ПЗ КЗЗ

#### 2.1.1 КЗЗ операційної системи з лінійки Windows

У ролі КЗЗ ОС з лінійки Windows для PC є ОС MS Windows 8.1 Enterprise що забезпечує послуги із захисту інформації при функціонуванні в складі ЦСК з виходом у глобальну обчислювальну мережу. У ролі КЗЗ ОС з лінійки Windows для серверів є ОС MS Windows Server 2012 R2 Standard що також забезпечує послуги із захисту інформації при функціонуванні в складі ЦСК з виходом у глобальну обчислювальну мережу. Так як КЗЗ ОС з лінійки Windows реалізують ідентичні механізми захисту, далі під ОС будуть матися на увазі операційні системи MS Windows 8.1 та MS Windows Server 2012.

КЗЗ ОС призначено для:

- забезпечення захисту від несанкціонованого доступу (НСД) до об'єктів захисту ЦСК, що зберігаються у файловій системі PC;
- забезпечення безперервності функціонування ОС;
- ведення журналів аудиту;
- забезпечення можливості адміністрування, керування і підтримки ОС.

#### 2.1.2 КЗЗ СКБД Microsoft SQL Server 2012

У якості серверу БД у КЗІ використовується MS SQL Server 2012. Штатний КЗЗ сервера БД MS SQL Server 2012 є інтегрованим з КЗЗ операційних систем.

КЗЗ СКБД Microsoft SQL Server 2012 має забезпечувати:

- керування безпекою сервера БД на основі ролей;
- розмежування прав доступу до об'єктів БД на основі ролей;
- розмежування прав доступу на виконання команд Transact-SQL да виконання процедур, що зберігаються;
- забезпечення шифрування об'єктів БД;
- забезпечення заборони доступу до об'єктів БД;
- вести аудит подій сервера.

#### 2.1.3 КЗЗ СКБД MySql

У якості серверу БД у КЗІ використовується MySQL Server 5. КЗЗ СКБД призначена для:

- керування безпекою сервера БД на основі облікових записів;
- розмежування прав доступу на виконання команд SQL да виконання процедур, що зберігаються;
- забезпечення заборони доступу до об'єктів БД;
- вести аудит подій сервера.

#### 2.1.4 КЗЗ HTTP-сервера Apache

УКЗІ в якості веб-сервера використовується Apache.

Основними функціями штатного КЗЗ веб-сервера є:

- керування доступом до ресурсів веб-сервера на основі облікових записів та груп;
- аудит подій безпеки;
- мінімізація привілеїв;
- захист цілісності конфігураційних файлів;
- контроль використання ресурсів;
- ідентифікація та автентифікація при обміні.

#### 2.1.5 ОС серверів з лінійки Linux

У якості ОС серверів взаємодії використовуються ОС з лінійки Linux - дистрибутив FreeBSD 9.2.

КЗЗ ОС реалізує такі функції:

- забезпечення захисту від несанкціонованого доступу (НСД) до об'єктів захисту ЦСК, що зберігаються у файловій системі;
- забезпечення безперервності функціонування ОС;
- ведення журналів аудиту;
- забезпечення можливості адміністрування, керування і підтримки ОС.

#### 2.1.6 Підсистема антивірусного захисту

У якості засобу антивірусного захисту використовується "ESET Endpoint Security". Програмний засіб антивірусного захисту має чинний, позитивний експертний висновок Адміністрації Держспецзв'язку України у сфері ТЗІ.

Засоби антивірусного захисту реалізують такі функції:

- застосування евристичних методів захисту у процесі викриття шкідливого ПЗ;
- захист файлової системи;
- оновлення антивірусних баз.

### 2.2 Призначення КТЗ КЗЗ

#### 2.2.1 Міжмережний екран

Міжмережний екран забезпечує такі функції:

- контроль транзитної інформації протоколів прикладного рівня;
- захист від мережеских атак, таких як, відмова в обслуговуванні, атака фрагментами та інших, що можуть здійснюватися із зовнішньої телекомунікаційної мережі;
- трансляцію IP-адресів та портів протоколів транспортного рівня;
- перевірку та відстеження стану всіх мережеских з'єднань;
- фільтрацію пакетів на підставі списків контролю доступу (на основі MAC-адреси або IP-адреси, номеру TCP- або UDP-порта відправника/приймальника);
- захист від витоку за межі ЦСК ключів обслуговуючого персоналу ЦСК та особистої інформації про користувачів ЦСК;
- ідентифікація та автентифікація адміністраторів;
- контроль власної цілісності;
- самотестування.

#### 2.2.2 Електронні ключі "Кристал-1"

Електронні ключі "Кристал-1" виконують такі функції:

- автентифікацію оператора ЕОМ при доступі до ключа;
- генерацію особистих та відкритих ключів для алгоритму ЕЦП;
- генерацію особистих та відкритих ключів для протоколу розподілу ключів;
- генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора;
- зберігання особистих ключів у внутрішній пам'яті та захист їх від НСД;
- формування і перевірку ЕЦП;
- обчислення геш-функції;
- розподіл ключових даних на основі асиметричного протоколу розподілу;
- зберігання довільних даних у внутрішній пам'яті та захист їх від НСД;
- контроль цілісності і працездатності вбудованого програмного забезпечення та ін.

#### 2.2.3 Мережні криптомодулі "Гряда-301"

Мережні криптомодулі "Гряда-301" виконують наступні функції:

- автентифікацію ЕОМ при доступі до модуля;
- генерацію особистих та відкритих ключів для алгоритму ЕЦП та протоколу розподілу ключів;
- генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора;
- зберігання особистих ключів у внутрішній пам'яті та захист їх від НСД;

- обчислення геш-функції, формування і перевірку ЕЦП;
- розподіл ключових даних на основі асиметричного протоколу розподілу та шифрування даних;
- контроль цілісності і працездатності вбудованого програмного забезпечення та ін.

#### 2.2.4 Криптомодулі "Гряди-61"

Криптомодулі "Гряди-61" виконують наступні функції:

- автентифікацію ЕОМ при доступі до модуля;
- генерацію особистих та відкритих ключів для алгоритму ЕЦП та протоколу розподілу ключів;
- генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора;
- зберігання особистих ключів у внутрішній пам'яті та захист їх від НСД;
- обчислення геш-функції, формування і перевірку ЕЦП;
- розподіл ключових даних на основі асиметричного протоколу розподілу та шифрування даних;
- контроль цілісності і працездатності вбудованого програмного забезпечення та ін.

### 3 ПОРЯДОК ЗАСТОСУВАННЯ КЗЗ

#### 3.1 Використання елементів КЗЗ на засобах ЦСК

Під елементами КЗЗ розуміється програмне забезпечення КЗЗ або компоненти комплексу технічних засобів КЗЗ.

##### 3.1.1 Використання елементів КЗЗ на РС адміністратора безпеки

На РС адміністратора безпеки ЦСК використовуються такі елементи КЗЗ:

- штатний КЗЗ ОС MS Windows 8.1;
- система антивірусного захисту РС.

Штатний КЗЗ ОС використовується для забезпечення захисту ресурсів РС від НСД.

З РС адміністратора безпеки виконується адміністрування та аудит ОС, КЗЗ серверів та іншого ПЗ, що встановлено на них. Для цього використовується програмний термінал, що емулює локальний термінал серверів. Насправді засоби адміністрування та аудиту ОС, КЗЗ серверів, є частиною їх ОС та виконуються безпосередньо на них.

Керування системою антивірусного захисту здійснюється централізовано за РС адміністратора безпеки за допомогою спеціального програмного забезпечення або веб-інтерфейсу.

САЗ РС використовується для забезпечення захисту РС від шкідливого ПЗ. САЗ РС контролює усі потоки даних (вхідні / вихідні), що передаються на РС - електрона пошта, Інтернет трафік, мережеві взаємодії. Оновлення антивірусних баз САЗ РС здійснюється в автоматичному або ручному режимі із спеціального мережного ресурсу серверу інфраструктури.

##### 3.1.2 Використання елементів КЗЗ на серверах

На центральних серверах використовуються такі елементи КЗЗ:

- КЗЗ ОС MS Windows Server 2012;
- система антивірусного захисту для серверів.

КЗЗ ОС використовується для забезпечення захисту ресурсів серверів від НСД.

САЗ використовується для забезпечення захисту серверів під керуванням ОС Windows від шкідливого ПЗ та дозволяє виконувати захист в умовах високого навантаження на сервер. Налаштування САЗ та оновлення антивірусних баз САЗ серверів здійснюється адміністратором безпеки.

На серверах взаємодії використовуються такі елементи КЗЗ:

- КЗЗ ОС Linux;
- КЗЗ веб-сервера Apache;
- КЗЗ MySQL

КЗЗ ОС, КЗЗ веб-сервера Apache, КЗЗ MySQL використовується для забезпечення захисту ресурсів серверів від НСД.

##### 3.1.4 Використання пристрою міжмережної безпеки

На пристрої міжмережної безпеки налаштований пакетний фільтр, що блокує спроби атак з боку зовнішньої телекомунікаційної мережі на сервер взаємодії та сервер БД. Керування пристроєм мережної безпеки здійснюється шляхом безпосереднього ("консольного") підключення до окремого "довіреного" порту.

#### 3.2 Порядок налаштування параметрів КЗЗ

У процесі експлуатації КСЗІЦСК співробітниками СЗІ ЦСК ринку електричної енергії (згідно посадових обов'язків та інструкцій) проводиться налаштування конкретних політик аудиту, параметрів КЗЗ, визначається склад облікових записів, імен користувачів (груп), їх прав та повноважень.