

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**

Опис КТЗ

ЄААД.468244.185.П9.02

ЗМІСТ

1 СТРУКТУРА КТЗ	4
2 ОПИС КОМПЛЕКСУ ТЕХНІЧНИХ ЗАСОБІВ КЗЗ.....	5
2.1 Міжмережний екран	5
2.1.1 Контроль транзитної інформації протоколів прикладного рівня	5
2.1.2 Захист від мережеских атак, що можуть здійснюватися із зовнішньої телекомунікаційної мережі ..	5
2.1.3 Трансляція IP-адресів та портів протоколів транспортного рівня.....	5
2.1.4 Перевірка та відстеження стану всіх мережеских з'єднань	6
2.1.5 Фільтрація пакетів на підставі списків контролю доступу	6
2.1.6 Захист від витоку за межі ЦСК ключів обслуговуючого персоналу ЦСК	6
2.1.7 Ідентифікація та автентифікація адміністраторів.....	6
2.1.8 Аудит подій.....	6
2.1.9 Контроль власної цілісності	7
2.1.10 Самотестування.....	7
2.2 Комутатори ЛОМ ЦСК.....	7
2.2.1 Ідентифікація та автентифікація адміністраторів.....	7
2.2.2 Ідентифікація користувачів за мережними адресами.....	8
2.2.3 Контроль власної цілісності	8
2.2.4 Керування доступом до портів та мережеских потоків	8
2.2.5 Самотестування.....	8
2.3 Електронні ключі "Кристал-1"	8
2.4 Мережні криптомодулі "Гряди-301"	8
2.5 Криptomодулі "Гряди-61"	9

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 СТРУКТУРА КТЗ

Опис основних функцій КТЗ описаний у документі ЄААД.468244.185.П9.01.

Структура комплексу технічних засобів (КТЗ) комплексу засобів захисту (КЗЗ) наводиться за принципом цільового використання.

Опис програмного забезпечення (ПЗ) КЗЗ наведено у документі ЄААД.468244.185.ПА.02.

Прив'язка до конкретних засобів ЕОТ ЦСК та опис комплексної системи захисту інформації (КСІ) наведено у загальному описі системи (документ ЄААД.468244.185.ПД.02).

До складу КТЗ КЗЗ входить:

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

2 ОПИС КОМПЛЕКСУ ТЕХНІЧНИХ ЗАСОБІВ КЗЗ

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;
- аудит подій;
- контроль власної цілісності;
- самотестування.

2.1.1 Контроль транзитної інформації протоколів прикладного рівня

Функція інтелектуального контролю трафіку заснована на відстеженні вхідних та вихідних з'єднань. Таке відстеження дозволяє забезпечити передачу через МЕ лише такого трафіку, запит на який надано із середини мережі, або якщо для цього трафіку мається явний дозвіл засобами ACL. Інтелектуальний контроль трафіку дозволяє не лише запобігти зловмисному трафіку із зовні але і захищає ЛОМ від атак прикладного рівня.

МЕ дозволяє забезпечити контроль протоколів та застосувань на основі:

- перевірки відповідності протоколам;
- модифікації пакетів з метою забезпечення їх вірної передачі.

Перевірка відповідності протоколам полягає у тому, що МЕ перевіряє чи дійсно мережеский трафік відповідає специфікації протоколу. Це дозволяє захиститися від застосувань, які можуть використовувати дозволені протоколи (наприклад HTTP) з метою виконання сторонніх дій. У МЕ реалізовано функцію викриття та блокування прихованого трафіку таких застосувань (наприклад застосувань, що служать для надання доступу за типом точка-точка (P2P), або застосувань обміну миттєвими повідомленнями).

У деяких випадках трафік, що передається через МЕ може викликати проблеми, які пов'язані з тим, що внутрішня адреса джерела трафіку глибоко приховано у пакеті, що надходить, а отже IP адреса пакету перед відправкою до ЗТМ не відповідає реальній. На МЕ покладається задача відстеження таких випадків та направлення зворотного трафіку до TCP пакету. Без реалізації такої функції трафік FTP, SQL, та деяких мультимедійних протоколів не буде коректно спрямовано до пристрою-джерела.

2.1.2 Захист від мережеских атак, що можуть здійснюватися із зовнішньої телекомунікаційної мережі

З метою забезпечення захисту від атак типу "відмова в обслуговуванні" (DoS) та "розподілена відмова в обслуговуванні" (DDoS) МЕ використовує поєднання кількох технологій. Основним підходом до захисту є відстеження випадків, в яких потоки даних, що надходять до МЕ, залишають напіввідкриті з'єднання. У разі викриття таких випадків МЕ розриває ці з'єднання.

Функція фільтрації трафіку реалізована у МЕ із використанням списків контролю доступу (ACL) на основі яких визначається які дозволи надані протоколам щодо взаємодії із зовнішніми та внутрішніми інтерфейсами МЕ. Використання ACL дозволяє розмежувати доступу користувачів до певних ресурсів, а також керувати надходженням потоків даних із ЗТМ.

Запобігання вторгненням здійснюється МЕ на основі використання набору загальновідомих сигнатур мережеских атак. Існує можливість виконати таке налаштування МЕ, щоб він відкидав паразитні пакети або сповіщав сервер подій МЕ щодо викриття цих атак. Додатково у МЕ реалізовано функцію створення власної політики доступу служб, що підсилює відповідність специфікаціям протоколів або фільтруванню певних видів трафіку.

2.1.3 Трансляція IP-адресів та портів протоколів транспортного рівня

У своїй найпростішій конфігурації транслятор мережних адрес (NAT) функціонує на МЕ, що з'єднує дві мережі; одна із цих мереж (спроектована як внутрішня) адресується за допомогою або часток, або застарілих адрес, які потрібно конвертувати в легальні адреси, перед тим як пакети направляються в іншу мережу (спроектовану як зовнішня). Метою NAT є забезпечення повної функціональності, так, якби приватна мережа мала глобальні унікальні адреси й компонента NAT не існувало.

МЕ може задати взаємно однозначну відповідність між внутрішніми локальними й глобальними адресами. Також він може задати динамічну відповідність між внутрішніми локальними й глобальними адресами. Це задається шляхом опису локальних адрес, які потрібно транслювати, адресного пулу, з якого розподіляються глобальні адреси, і з'єднання обох.

МЕ зберігає адреси в глобальному адресному пулі шляхом трансляції вихідних портів у з'єднаннях TCP (протокол керування передачею) або в діалоговому режимі протоколу UDP (протокол користувальницьких дейтаграмм). Різні локальні адреси будуть перетворюватися в ті ж самі глобальні адреси за допомогою трансляції порту, що забезпечує необхідну унікальність. Коли з'являється необхідність у трансляції, новий номер порту вибирається з того ж інтервалу, що й первісний.

Для трафіка "зовнішні до внутрішніх" можна зконфігувати динамічну трансляцію адрес пунктів призначення. Коли відповідність встановлена, адреса пункту призначення, що відповідає одному з адрес списку доступу, буде замінюватися на адресу з ротаційного пулу. Призначення виробляється за циклічним принципом й виконується тільки в тому випадку, якщо відкривається нове з'єднання із "зовнішніх до внутрішніх". Не весь TCP-трафік пропускається без трансляції.

2.1.4 Перевірка та відстеження стану всіх мережевих з'єднань

Для забезпечення найбільшої працездатності МЕ, увесь час у реальному часі здійснюється відстеження стану всіх мережних з'єднань. Усі мережеві з'єднання повинні займати квоти ресурсів тільки у тому випадку, якщо вони являються активними і вони виконують функцію передачі даних. У випадку, якщо мережні з'єднання не використовуються системою, завислі або являються помилковими, їх ресурси звільняються (анулюються) і можуть бути передані іншим мережним з'єднанням.

2.1.5 Фільтрація пакетів на підставі списків контролю доступу

Одною з основних функцій міжмережного екрана є керування доступом до портів та мережних потоків, тобто виконання функцій брандмауера. За допомогою правил доступу, створюються правила на доступ з певних мережних адрес та портів до відповідних дозволених адрес та портів. Аналогічно створюються правила на заборону доступу до відповідних мережних адрес і портів.

Фільтрації пакетів на підставі списків контролю доступу за основі MAC-адреси або IP-адреси, номеру TCP- або UDP-порта відправника/приймальника унеможливує проведення атак зі сторони зовнішніх телекомунікаційних мереж і забезпечує захист від атаки "відмова у обслуговуванні".

2.1.6 Захист від витоку за межі ЦСК ключів обслуговуючого персоналу ЦСК

Розмежування доступу до ресурсів мережі, належність таблиць розподілення доступу між мережними ресурсами у МЕ забезпечує захист від витоку інформації за межі ЦСК. Жорсткі правила циркуляції інформації забезпечує знаходження ключів обслуговуючого персоналу ЦСК та особистої інформації користувачів ЦСК у межах ЦСК і захищена від витоку за її межі.

2.1.7 Ідентифікація та автентифікація адміністраторів

МЕ забезпечує можливість ідентифікації та автентифікації адміністраторів. Вхід до налаштувань МЕ буде дозволено лише після того, як адміністратор коректно введе свій логін і пароль. У випадку, якщо пароль і логін введено не коректно - дозвіл не надається, а ця подія записується до журналу подій.

2.1.8 Аудит подій

МЕ має можливість ведення аудиту подій. Для ведення аудиту використовується класифікація класів повідомлень, що пов'язані із безпекою (таблиця 2.1). Аудит подій зазвичай фіксує такі повідомлення: стан МЕ, відомості щодо мережевих атак, невдалі спроби автентифікації користувачів, зміни налаштувань МЕ тощо. Реалізовано можливість аналізування журналів подій із застосуванням спеціалізованого ПЗ розробки Cisco.

Таблиця 2.1 - Класи повідомлень, пов'язаних із безпекою

Клас повідомлень	Опис
Попереджувачі	Повідомлення вказують на те, що МЕ виконав дію з усунення проблеми

повідомлення (Alert)	пов'язаною із безпекою або вказують на необхідність дій з боку відповідального адміністратора внаслідок: непрацездатності інтерфейсу, виходу зі строю модулю ME або проблем із кабелем. Причини виникнення цих подій завжди мають розслідуватися та усуватися.
Критичні повідомлення (Critical)	Повідомлення, які вказують на те, що: трафік було заблоковано або відкинуто, було викрито прослуховування трафіку або надані прапорці не коректні для цього трафіку. Причини виникнення цих подій завжди мають розслідуватися та усуватися.
Повідомлення щодо помилок (Error)	Цей тип повідомлення є специфічним для ресурсів ME таких як помилки у таблицях керування (xlate) або збій у слоті переносу. Причини виникнення цих подій завжди мають розслідуватися та усуватися.
Повідомлення застереження (Warning)	Повідомлення звичайно свідчать щодо проблем з'єднання. Значна кількість цих проблем може бути викликана роботою протоколів або кінцевим обладнанням.
Повідомлення сповіщення (Notification)	Повідомлення містять сповіщення щодо дій користувача який підключився до ME та окремі повідомлення щодо блокування Java та ActiveX. Ці повідомлення потребують аналізу з метою контролю відсутності неавторизованих змін до налаштувань ME.
Інформаційні повідомлення (Informational)	Ці повідомлення описують з'єднання, що були встановлені через ME або розірвані. Переважна кількість повідомлень не потребує аудиту, і використовуються у випадках виникнення проблем користувачів щодо встановлення з'єднань.
Технологічні повідомлення (Debugging)	Звичайно ці повідомлення стосуються IPSec. Відповідальний адміністратор використовує ці повідомлення при першому налаштуванні IPSec.

2.1.9 Контроль власної цілісності

ME має власні механізми перевірки цілісності для забезпечення безпеки передачі інформації. Забезпечується контроль цілісності:

- програмного забезпечення;
- оновлень таблиць маршрутизації;
- операційної системи.

2.1.10 Самотестування

Самотестування дозволяє перевірити й на підставі цього гарантувати правильність функціонування й цілісність певного переліку функцій КС. Тестові процедури входять у склад програмного забезпечення ME.

Процес самотестування здійснюється на початку роботи, який перевіряє всі модулі системи на коректність виконання своїх функцій. Самотестування забезпечує гарантію коректного функціонування пристрою в цілому.

2.2 Комутатори ЛОМ ЦСК

Комутатори ЛОМ ЦСК мають такі функціональні можливості:

- ідентифікація та автентифікація адміністраторів;
- ідентифікація користувачів за мережними адресами;
- контроль власної цілісності;
- керування доступом до портів та мережних потоків;
- самотестування.

2.2.1 Ідентифікація та автентифікація адміністраторів

Комутатори підтримують як віддалене, так і локальне керування. Локальне керування здійснюється з локальної консолі. Віддалене керування здійснюється за протоколом SSH з робочих станцій адміністраторів. Для автентифікації адміністраторів використовуються паролі. Крім того, підтримується протокол Telnet. Слід зауважити, що паролі при використанні протоколу Telnet передаються у відкритому вигляді. З метою підвищення безпеки при конфігурації виділяються користувацький та привілейований режими роботи. У користувацькому режимі недоступний ряд команд, що є критичними для правильності функціонування комутатора. Для кожного з цих режимів задається окремий пароль адміністратора. За

замовчанням при зберіганні у флеш-пам'яті комутатора шифруються лише паролі привілейованого режиму, однак можливо налаштувати комутатор таким чином, щоб шифрувались усі паролі.

2.2.2 Ідентифікація користувачів за мережними адресами

Для надання доступу до мережі користувачам, вони повинні бути додані до таблиці дозволених мережних адрес. При спробі доступу до мережі, комутатор ідентифікує користувачів і надає доступ до мережних ресурсів. Якщо користувач не має право доступу, комутатор блокує всі спроби доступу до відповідних ресурсів.

2.2.3 Контроль власної цілісності

Керований комутатор ЛОМ має механізми перевірки власної цілісності для забезпечення безпеки передачі інформації. Він забезпечує контроль цілісності власного програмного забезпечення та цілісність операційної системи.

2.2.4 Керування доступом до портів та мережних потоків

Комутатор може здійснювати керування доступом до портів та мережних потоків, тобто виконувати функції брандмауера. За допомогою правил доступу, можливо створювати правила на доступ з обраних мережних адрес та портів на відповідні дозволени адреси та порти. Аналогічно можливо створювати правила на заборону доступу до відповідних мережних адрес та портів.

Правила контролю доступу забезпечують максимально детальний контроль доступу до мережних ресурсів. Трафік може бути розмежований як за IP-адресою так і за портами. Правила розмежування можуть бути згруповані в профілі, назначені групам користувачів. Правила доступу можуть враховувати обмеження за часом дії.

2.2.5 Самотестування

Перевірка усіх модулів комутатора на початку роботи здійснюється процесом самотестування. Цей процес перевіряє всі модулі системи на коректність виконання своїх функцій. Самотестування забезпечує гарантію коректного функціонування пристрою в цілому.

2.3 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.

Електронні ключі "Кристал-1" призначені для захисту конфіденційної інформації.

2.4 Мережні криптомодулі "Гряд-301"

Мережні криптомодулі "Гряд-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.

Мережні криптомодулі "Гряд-301" призначені для захисту конфіденційної інформації.

2.5 Криптомодулі "Гряда-61"

Криптомодулі "Гряда-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.

Криптомодулі "Гряда-61" призначені для захисту конфіденційної інформації.