Розділ 11

ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ТА ЗАСТОСУВАННЯ ЗАСОБІВ КЗІ В НАЦІОНАЛЬНІЙ СИСТЕМІ ІВК (ЕЦП)

У розділі 10 зазначалося, що для забезпечення вищого рівня гарантій в ІВК необхідно застосовувати на всіх рівнях програмно-апаратні або апаратні засоби КЗІ. Там же обґрунтовані вимоги до таких засобів, які базуються на федеральних стандартах США FIPS 140-2 та FIPS 140-3. У цьому розділі подано обґрунтування вимог, проектування, аналізу, властивості та особливості застосування апаратно-програмних засобів КЗІ серії «Гряда». На рис. 11.1 наведено структурну схему програмно-технічного комплексу ЦСК з виділеними елементами апаратно-програмних засобів КЗІ серії «Гряда» [235].

11.1. АПАРАТНИЙ ЗАСІБ ТИПУ ЕЛЕКТРОННИЙ КЛЮЧ «КРИСТАЛ-1»

Електронний ключ «Кристал-1» (далі – ЕК) є апаратним засобом КЗІ типу «П» та «Ш» класу В2. Підприємство-розробник: ЗАТ «Інститут інформаційних технологій», м. Харків.

ЕК призначений для апаратної реалізацій криптографічних перетворень у складі апаратно-програмних засобів і комплексів КЗІ, що реалізовані на основі ЕОМ. Область застосування: апаратно-програмні засоби та комплекси КЗІ типу «П», «Ш» та «Р», що призначені для захисту конфіденційної інформації.

До складу виробу повинні входити:

– електронний ключ (ЕК);

– носій інформації з інсталяційним пакетом програм;

– комплект експлуатаційних документів;

– комплект тари та упакування.

ЕК повинен бути виконаний у вигляді малогабаритного з'ємного USB-пристрою. Конструктивно ЕК має бути виконаний на двошаровій друкованій платі, яка розмішена у пластиковому корпусі одноразової зборки, або в корпусі, виконаному у вигляді компаундної заливки. На друкованій платі встановлюються електронні компоненти ЕК та USB-з'єднувач типу A-plug (виделка).

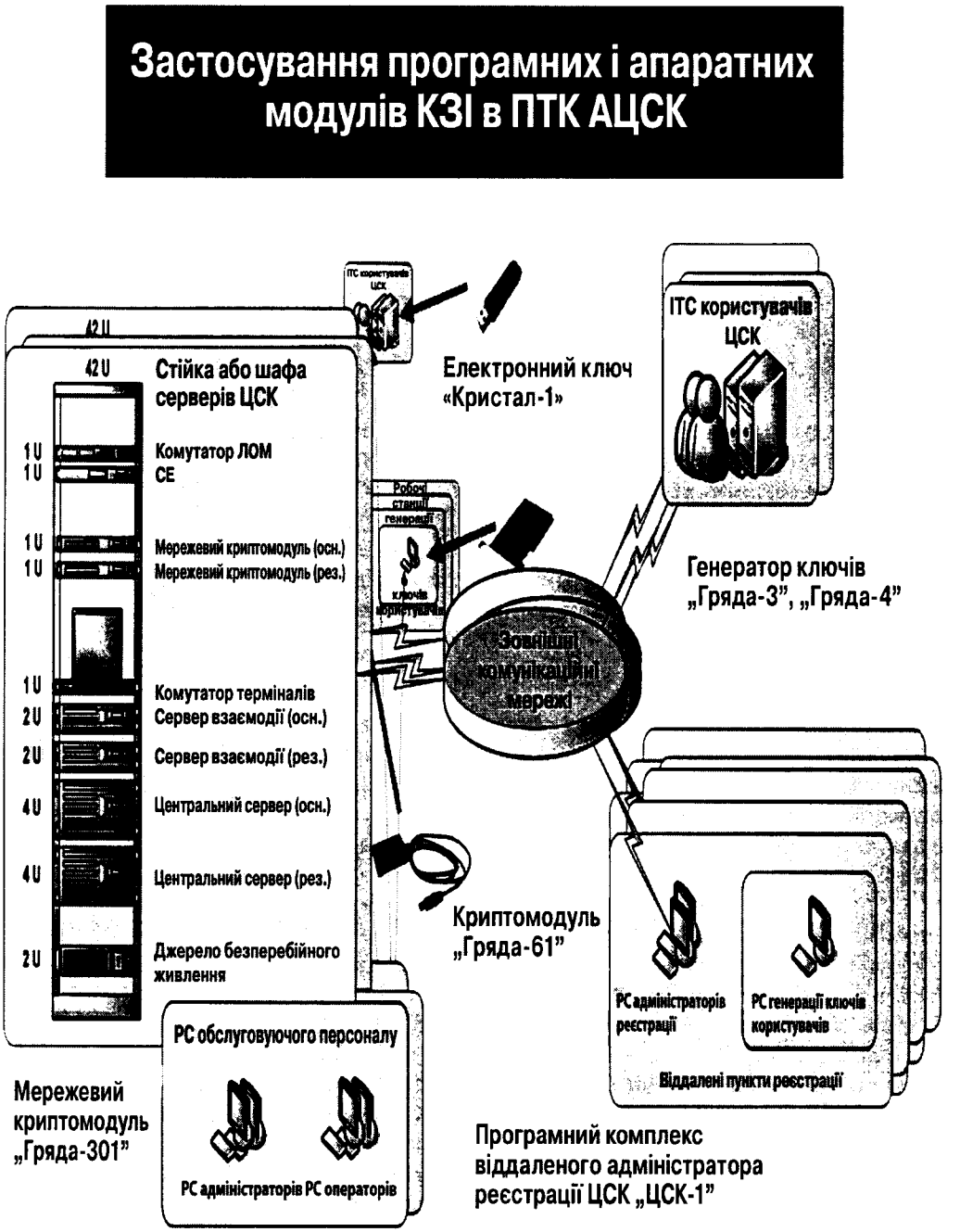

Рис. 11.1. Схема застосування програмних засобів КЗІ в ЦСК (варіант)

ЕК має бути виконаний у кліматичному виконанні групи 2 згідно з ГОСТ 21552-90. Відповідно до цього ЕК належить до групи 1 технічних засобів, призначених для експлуатації в наземних стаціонарних приміщеннях і спорудах.

Електроживлення ЕК, з'єднаного з ЕОМ через USB-роз'єм, повинне здійснюватися від блоку електроживлення ЕОМ через контакти USB-роз'єму.

Основні масогабаритні та інші технічні характеристики ЕК повинні відповідати наведеним у табл. 11.1 (рис. 11.2, 11.3).

Таблиця 11.1. **Основні масогабаритні та інші технічні характеристики ЕК**

Найменування	Норма
Габаритні розміри друкованої плати, мм, не більше – довжина – ширина	 50 15
Габаритні розміри ЕК, мм, не більше – довжина – ширина – висота	 75 25 11
Маса, г, не більше	20
Споживана потужність від блоку електроживлення ЕОМ, Вт, не більше	0,5

Рис. 11.2. Електронний ключ «Кристал-1»

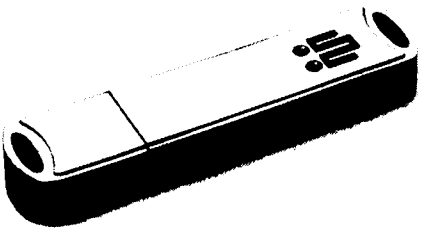

Рис. 11.3. Електронний ключ «Кристал-1Д»

ЕК призначений для виконання таких функцій:

1) управління особистими ключами ЕЦП та протоколу розподілу ключових даних, що включає:

– прийом та зберігання загальних параметрів для алгоритму ЕЦП згідно з ДСТУ 4145-2002 та протоколом розподілу ключів;

– генерацію особистого ключа ЕЦП та протоколу розподілу ключів з використанням алгоритму генерації випадкових бітових послідовностей згідно з ДСТУ 4145-2002 і вбудованого апаратного генератора випадкових сигналів (ГВС);

– зберігання особистих ключів ЕЦП та протоколу розподілу ключів в зашифрованому вигляді з контролем цілісності;

– знищення особистих ключів ЕЦП та протоколу розподілу ключів;

2) формування ЕЦП від даних, що завантажуються з ЕОМ, за алгоритмом згідно з ДСТУ 4145-2002 з використанням особистого ключа ЕЦП;

3) генерацію ключів сеансу для ГОСТ 28147-89;

4) формування спільного секретного ключа за протоколом розподілу ключових даних з використанням власного особистого ключа протоколу розподілу та відкритого ключа протоколу розподілу утримувача;

5) зашифрування та розшифрування ключів сеансу для ГОСТ 28147-89 з використанням сформованого спільного секретного ключа за алгоритмом згідно ГОСТ 28147-89 (режим простої заміни);

6) прийом і зберігання 2-х довгострокових ключових елементів (ДКЕ) для ГОСТ 28147-89, що використовуються в алгоритмі генерації випадкових бітових послідовностей за ДСТУ 4145-2002 та протоколі розподілу ключових даних;

7) автентифікації користувача перед початком роботи шляхом гешування пароля доступу до ЕК за алгоритмом згідно з ГОСТ 34.311-95 та порівнянням з еталоном, що зберігається в ЕК;

8) управління параметрами автентифікації користувача, що включає встановлення та зміну даних автентифікації користувача;

9) прийом, зберігання, надання доступу та знищення довільних даних користувача в ЕК.

ЕК включає такі функціональні вузли:

– процесор із вбудованими: генератором тактових частот; оперативним запам'ятовуючим пристроєм (ОЗП), постійним запам'ятовуючим пристроєм (ПЗП), контролером шини USB;

– генератор випадкового сигналу (ГВС);

– стабілізатори напруг живлення всіх компонентів ЕК.

Процесор призначений для:

– збереження у вбудованому ПЗП та виконання програм, що реалізують функції ЕК;

– збереження у вбудованому ПЗП особистих ключів, даних автентифікації та довільних даних користувача;

– організації обміну інформацією з ЕОМ через інтерфейс USB.

ГВС призначений для генерації аналогового випадкового сигналу та перетворення його на двійкові логічні рівні, які використовуються при формуванні випадкових послідовностей (чисел) за алгоритмом згідно з ДСТУ 4145-2002.

Для підвищення надійності ГВС складається з двох каналів і кожен канал включає:

– фізичний датчик випадкового аналогового сигналу на базі шумового діода типу КГ;

– аналого-цифровий перетворювач на основі компаратора; для підвищення завадостійкості компаратор має гістерезис, що створюється за допомогою позитивного зворотного зв'язку;

– лічильний тригер, стани якого з рівною ймовірністю приймають нульове та одиничне значення.

Рівноймовірні логічні стани з виходів лічильних тригерів двох каналів ГВС зчитуються з порту процесора в регістр. Програмне забезпечення процесора об'єднує два логічних стани в один випадковий біт за допомогою команди «додавання за модулем 2» і перетворює випадкові біти на паралельний код по 32 розряди командами зсуву. 32-розрядні випадкові слова запам'ятовуються в оперативному запам'ятовуючому пристрої процесора і використовуються для формування початкових станів генератора випадкових послідовностей згідно з ДСТУ 4145-2002.

Програмні забезпечення ЕК включають:

– внутрішні програмні компоненти ЕК (внутрішні програми);

– системні програмні компоненти (драйвери або модулі ядра ОС Microsoft Windows та Linux/UNIX);

– програмний комплекс тестування та конфігурування ЕК (модуль, що виконується для ОС Microsoft Windows та ОС Linux/UNIX).

Внутрішні програми ЕК призначені для:

– прийому та зберігання у ПЗП загальних параметрів для алгоритму ЕЦП згідно з ДСТУ 4145-2002 та протоколу розподілу ключів;

– генерації особистого ключа ЕЦП та протоколу розподілу ключів з використанням алгоритму генерації випадкових бітових послідовностей ЕЦП згідно з ДСТУ 4145-2002 і вбудованого апаратного ГВС;

– зберігання у ПЗП особистих ключів ЕЦП та протоколу розподілу ключів в зашифрованому вигляді з контролем цілісності;

– знищення з ПЗП особистих ключів ЕЦП та протоколу розподілу ключів;

– формування ЕЦП від даних, що завантажуються з ЕОМ, за алгоритмом згідно з ДСТУ 4145-2002 з використанням особистого ключа ЕЦП;

– генерації ключів сеансу для ГОСТ 28147-89;

– формування спільного секретного ключа за протоколом розподілу ключових даних з використанням власного особистого ключа протоколу розподілу та відкритого ключа протоколу розподілу утримувача;

– зашифрування та розшифрування ключів сеансу для ГОСТ 28147-89 з використанням сформованого спільного секретного ключа за алгоритмом згідно з ГОСТ 28147-89 (режим простої заміни);

– прийому та зберігання у ПЗП 2-х ДКЕ для ГОСТ 28147-89, що використовуються в алгоритмі генерації випадкових бітових послідовностей за ДСТУ 4145-2002 та протоколі розподілу ключових даних;

– автентифікації користувача перед початком роботи шляхом гешування пароля доступу до ЕК за алгоритмом згідно з ГОСТ 34.311-95 та порівнянням з еталоном, що зберігається у ПЗП;

– управління параметрами автентифікації користувача;

– прийому, запису та зберігання у ПЗП довільних даних користувача;

– надання доступу та знищення довільних даних користувача з ПЗП.

Системні програмні компоненти призначені для:

– забезпечення коректного розпізнавання ЕК ОС ЕОМ;

– передачі кодів команд і вхідних даних для виконання відповідних внутрішніх програм криптографічного модуля, які виконують перетворення вхідних даних на вихідні;

– отримання з ЕК результатів виконання команд і вихідних даних.

Програмний комплекс тестування та конфігурування призначений для:

– перевірки роботоздатності ЕК;

– конфігурування параметрів ЕК у ОС ЕОМ;

– встановлення або зміни даних автентифікації користувача ЕК шляхом їх завантаження в ЕК;

– форматування ЕК, що включає знищення особистих ключів та довільних даних користувача в ЕК та встановлення даних автентифікації.

Після апаратного скидання ЕК виконує автоматичне тестування функціональних елементів і внутрішніх програм. Тестування функціональних елементів повинне включати статистичний контроль виходу апаратного ГВС.

Перевірка правильності виконання криптографічних перетворень включає перевірки таких процедур:

– зашифрування і розшифрування за алгоритмом ГОСТ 28147-89 у режимі простої заміни (контрольні приклади (тести) № 1, 9 з методики перевірки правильності програмної реалізації алгоритму шифрування згідно з ГОСТ 28147-89, погодженої з ДСТСЗІ СБ України від 05.07.2003, зареєстрованої 17.07.2003 за № 31);

– вироблення імітовставки за ГОСТ 28147-89 (контрольні приклади (тести) № 25, 26 з методики перевірки правильності програмної реалізації алгоритму шифрування згідно з ГОСТ 28147-89, яка погоджена з ДСТСЗІ СБ України від 05.07.2003, зареєстрованої 17.07.2003 за № 31);

– формування та перевіряння ЕЦП за алгоритмом згідно з ДСТУ 4145-2002 (контрольні приклади (тести) № 139 (варіант 1), 142 (варіанти 1, 3), 152 (варіант 3) з методики перевірки правильності програмної реалізації алгоритмів формування та перевіряння цифрового підпису згідно з ДСТУ 4145-2002, погодженої з ДСТСЗІ СБ України від 23.09.2004, зареєстрованої 03.08.2004 за № 61);

– гешування за алгоритмом ГОСТ 34.311-95 (контрольні приклади (тести) № 1, 6 з методики перевірки правильності програмної реалізації алгоритму гешування згідно з ГОСТ 34.311-95, погодженої з ДСТСЗІ СБ України від 05.07.2003, зареєстрованої 17.07.2003 за № 29).

Статистичний контроль виходу апаратного ГВС здійснюється згідно з методикою генерації ключових даних. У разі непроходження окремого тесту повинен видаватися статус непроходження із зазначенням типу тесту. Подальше виконання наступних тестів і використання ЕК повинне блокуватися. При неуспішному виконанні тестування ЕК з першого разу виконується повторне тестування. При успішному повторному тестуванні блокування повинне знімати ся. У разі повторного невиконання блокування не знімається і ЕК вважається несправним.

До складу ключових даних ЕК входять:

– ДКЕ для ГОСТ 28147-89, що використовуються в алгоритмі генерації випадкових бітових послідовностей згідно з ДСТУ 4145-2002 та протоколі розподілу ключових даних;

– загальні параметри ЕЦП для алгоритму ДСТУ 4145-2002 та протоколу розподілу ключів;

– особистий і відкритий ключі ЕЦП для алгоритму ДСТУ 4145-2002;

– особистий і відкритий ключі протоколу розподілу ключів.

ДКЕ для ГОСТ 28147-89, загальні параметри ЕЦП для алгоритму ДСТУ 4145-2002 та протоколу розподілу ключів завантажуються з ЕОМ в ЕК під час генерації ключів та зберігаються у внутрішньому ПЗП.

Особисті й відкриті ключі ЕЦП та протоколу розподілу ключів генеруються в середині ЕК. Після чого особисті ключі повинні зберігатися у внутрішньому ПЗП, а відкриті – передаватися в ЕОМ для подальшого їх розповсюдження та виготовлення сертифікатів. Параметри еліптичних кривих для алгоритму ДСТУ 4145-2002 та ДКЕ для алгоритму ГОСТ 28147-89 постачаються відповідно до вимог.

Захист від НСД до інформації, що обробляється в ЕК, здійснюється шляхом:

– використання командного (процедурного) інтерфейсу взаємодії системних програмних компонентів з ЕК, що виключає прямий доступ до внутрішніх вузлів і програм ЕК;

– зберігання ключових даних (особистих ключів) у ПЗП в захищеному вигляді;

– автентифікації користувача до початку роботи з ЕК.

Захист і контроль цілісності особистих ключів у ПЗП здійснюється на паролі захисту, який передається в ЕК під час операцій з одним із особистих ключів. Особисті ключі повинні контролюватися на цілісність шляхом вироблення імітовставки за ГОСТ 28147-89 та захищатися шляхом зашифрування в режимі простої заміни ГОСТ 28147-89 на ключі, який отриманий шляхом гешування рядка пароля за ГОСТ 34.311-95.

Автентифікація користувача перед початком роботи здійснюється шляхом передачі в ЕК пароля доступу до ЕК, гешування паролю за алгоритмом згідно з ГОСТ 34.311-95 і порівнянням з еталоном, що зберігається у ПЗП. На підставі результату порівняння ЕК повинен приймати рішення про успішність автентифікації.

Вимоги стійкості до механічних та кліматичних впливів

ЕК, що встановлюється в ЕОМ, призначений для експлуатації в приміщеннях з нормальними кліматичними умовами:

– температура навколишнього повітря – (5...40) °С;

– відносна вологість навколишнього повітря – (40...80) %;

– атмосферний тиск – 84–107 кПа (630–800 мм рт. ст.).

ЕК, що встановлений у ЕОМ, повинен зберігати працездатність при дії вібрації з частотою від 5 до 35 Гц, амплітуда зсуву 0,35 мм.

Надійність виробу

Показники надійності ЕК належать до групи 1, вид – невідновлюваний, відповідно до ГОСТ 27.003-90. Номенклатура показників для нормальних кліматичних умов експлуатації за ГОСТ 21552-84:

– середній наробіток на відмовлення – не менше 15000 г;

– середній термін служби – 10 років;

– ресурс USB-з'єднувача – не менше 1500 з'єднань/ роз'єднань;

– ресурс постійного запам'ятовуючого пристрою – не менше 10000 операцій запису в кожен сектор, термін зберігання даних – не менше 10 років, кількість операцій читання не обмежена;

– коефіцієнт технічного використання – не менше 0,95.

ЕК забезпечує як цілодобову, так і змінну роботу з урахуванням проведення технічного обслуговування. Вимоги до безвідмовності: ресурс виробу до відмовлення за технічним станом – 15000 годин протягом терміну служби, у тому числі термін збереження 1 рік.

11.2. АПАРАТНИЙ ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ (АГВЧ)

АГВЧ призначений для апаратної генерації послідовностей випадкових чисел на основі фізичних датчиків шуму в складі апаратно-програмних засобів і комплексів КЗІ, що реалізовані на основі ЕОМ. Область застосування: апаратно-програмні засоби та комплекси КЗІ типу «К», «Ш», «П» та «Р», призначені для захисту конфіденційної інформації, що не є власністю держави.

АГВЧ виконаний у вигляді малогабаритного пристрою, який має кронштейн для розміщення всередині системного блоку ЕОМ та з'єднується з системною платою ЕОМ через USB-інтерфейс за допомогою кабелю.

Конструктивно АГВЧ виконаний на двошаровій друкованій платі, яка розмішена у пластиковому корпусі та нерозбірно поєднана з ним шляхом заливки компаундом. На друкованій платі встановлюються електронні компоненти АГВЧ.

Основні масогабаритні й інші технічні характеристики пристрою наведено в табл. 11.2. Зовнішній вигляд виробу наведено на рис. 11.4.

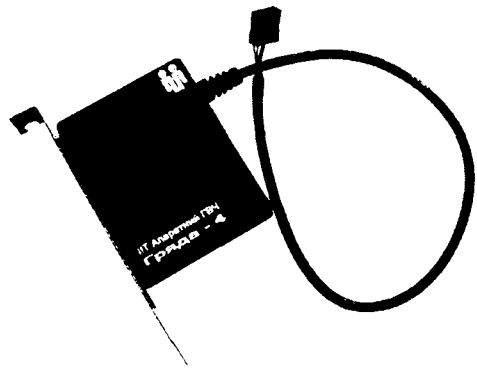

Рис. 11.4. Апаратний генератор випадкових чисел (АГВЧ)

До складу виробу входять:

– апаратний модуль;

– носій інформації з інсталяційним пакетом програм;

– комплект експлуатаційних документів;

– комплект тари та упакування.

Таблиця 11.2. **Основні масогабаритні та інші технічні характеристики АГВЧ**

Найменування	Норма
Габаритні розміри друкованої плати, мм, не більше: – довжина – ширина	 55 40
Габаритні розміри АГВЧ без урахування кронштейна та USB-кабеля, мм, не більше: – довжина – ширина – висота	 80 60 25
Довжина USB-кабеля, м – не менше – не більше	 0,1 0,4
Маса, г, не більше	200
Споживана потужність від блоку електроживлення ЕОМ, Вт, не більше	0,5

АГВЧ виконує такі функції:

– генерацію випадкових послідовностей заданої довжини;

– передачу до ЕОМ сформованої послідовності через USB-інтерфейс, використовуючи командний протокол обміну.

АГВЧ включає такі функціональні вузли:

– мікроконтролер із вбудованими: генератором тактових частот; оперативним запам'ятовуючим пристроєм (ОЗП), постійним запам'ятовуючим пристроєм (ПЗП), контролером шини USB;

– генератор випадкового сигналу (ГВС);

– стабілізатори напруг живлення всіх компонентів АГВЧ.

Мікроконтролер призначений для збереження у вбудованому ПЗП та виконання внутрішніх програм, що реалізують функції АГВЧ, зазначені у пункті 3.2.6;

ГВС призначений для генерації аналогового випадкового сигналу та перетворення його на двійкові логічні рівні, які використовуються при формуванні випадкових послідовностей (чисел).

ГВС складається з двох каналів для підвищення надійності, і кожен канал включає:

– фізичний датчик випадкового аналогового сигналу на базі шумового діода КГ401А;

– аналого-цифровий перетворювач на основі компаратора; для підвищення завадостійкості компаратор повинен мати гістерезис, що створюється за допомогою позитивного зворотного зв'язку;

– лічильний тригер, стани якого з рівною ймовірністю приймають нульове та одиничне значення.

Рівноймовірні логічні стани з виходів лічильних тригерів двох каналів ГВС зчитуються з порту мікроконтролера в регістр. Програмне забезпечення мікроконтролера об'єднує два логічних стани в один випадковий біт за допомогою команди «додавання за модулем 2» і перетворює випадкові біти на паралельний код по 32 розряди командами зсуву. 32-х розрядні випадкові слова запам'ятовуються в ОЗП мікроконтролера.

Програми АГВЧ включають:

– внутрішні програмні компоненти АГВЧ (внутрішні програми);

– системні програмні компоненти (драйвери або модулі ядра ОС Microsoft Windows та Linux/UNIX);

– програмний комплекс тестування АГВЧ (модуль, що виконується для ОС Microsoft Windows та ОС Linux/UNIX).

Внутрішні програми АГВЧ призначені для:

– зчитування випадкових сигналів з порту мікроконтролера, їх первинної обробки та формування в ОЗП мікроконтролера випадкової послідовності заданої довжини;

– організації інформаційного обміну з ЕОМ через USB-інтерфейс.

Системні програмні компоненти призначені для:

– забезпечення коректного розпізнавання АГВЧ ОС ЕОМ;

– передачі кодів команд і вхідних даних, необхідних для формування та отримання з АГВЧ результуючої випадкової бітової послідовності.

Програмний комплекс тестування призначений для перевірки роботоздатності АГВЧ.

Спеціальні вимоги до показників призначення виробу

Після формування випадкової послідовності перед передачею її до ЕОМ, до якої встановлено АГВЧ, повинен здійснюватись її технологічний контроль згідно з *методикою*.

У разі непроходження технологічного контролю, використання сформованої послідовності повинне блокуватися. У цьому випадку повинна бути сформована наступна послідовність. Якщо вона також не проходить технологічний контроль, подальше використання АГВЧ повинне блокуватися.

Програмний комплекс тестування АГВЧ повинен проводити статистичний контроль випадкових послідовностей, які формуються АГВЧ згідно з методикою генерації ключових даних, погодженої з контролюючим органом. У разі непроходження АГВЧ генерації статистичного контролю випадкових послідовностей його використання забороняється.

11.3. АПАРАТНИЙ МОДУЛЬ ЦИФРОВОГО ПІДПИСУ «ГРЯДА-41П»

Апаратний засіб КЗІ – модуль цифрового підпису «Гряда-41П» (далі – АМП) є засобом виду «Б», категорії «П», класу «Б1».

Модуль виконує такі функції:

1) управління особистим ключем ЕЦП, що включає:

– прийом і зберігання загальних параметрів для алгоритму ЕЦП згідно з ДСТУ 4145-2002;

– генерацію особистого ключа ЕЦП з використанням алгоритму генерації випадкових бітових послідовностей згідно з ДСТУ 4145-2002 і вбудованим апаратним ГВЧ;

– зберігання особистого ключа ЕЦП в зашифрованому вигляді;

– запис особистого ключа ЕЦП на зовнішні НКІ в захищеному вигляді (резервне копіювання особистого ключа ЕЦП);

– зчитування особистого ключа ЕЦП із зовнішніх НКІ та запис в АМП (відновлення особистого ключа ЕЦП);

– знищення особистого ключа ЕЦП в АМП та на зовнішніх НКІ.

2) формування ЕЦП від даних, що завантажуються з ЕОМ, за алгоритмом згідно з ДСТУ 4145-2002 з використанням особистого ключа ЕЦП;

3) прийом та зберігання довгострокових ключових елементів (ДКЕ) для ГОСТ 28147-89, що використовується в алгоритмі генерації випадкових бітових послідовностей за ДСТУ 4145-2002 при генерації особистого ключа ЕЦП, та формування ЕЦП;

4) прийом і зберігання ДКЕ для ГОСТ 28147-89, що використовується під час резервного копіювання та відновлення особистого ключа ЕЦП, шляхом відповідного виконання процедур зашифрування і розшифрування особистого ключа ЕЦП за алгоритмом згідно з ГОСТ 28147-89 у режимі простої заміни;

5) автентифікацію користувача перед початком роботи шляхом послідовного виконання:

– порівняння пароля доступу користувача з еталоном, що зберігається в АМП;

– зчитування випадкового числа довжиною 16 байт із зовнішнього НКІ, який приєднується до АПМ під час автентифікації, з еталоном, що зберігається в АМП;

6) управління параметрами автентифікації користувача, що включає встановлення та зміну даних автентифікації користувача;

7) прийом, зберігання, надання доступу та знищення довільних даних користувача в АМП.

Область застосування пристрою – апаратно-програмні засоби та комплекси КЗІ типу «К» та «П», призначені для захисту конфіденційної інформації, що не є власністю держави.

Апаратний модуль реалізує такі криптографічні алгоритми та протоколи:

– шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни та режим вироблення імітовставки);

– ЕЦП за ДСТУ 4145-2002 (усі довжини ключів передбачені стандартом);

– гешування за ГОСТ 34.311-95.

Зовнішній вигляд виробу наведено на рис. 11.5.

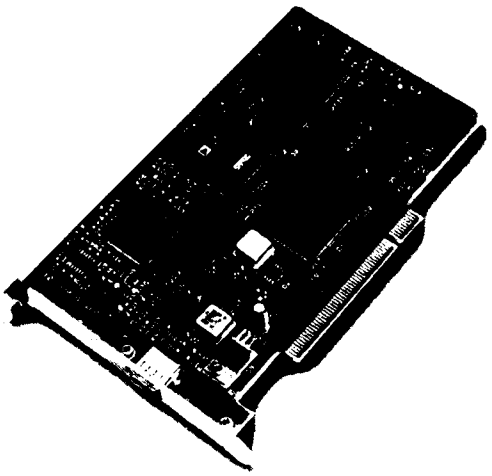

Рис. 11.5. Апаратний модуль цифрового підпису «Гряда-41П»

Швидкість формування ЕЦП за ДСТУ 4145-2002, поле 257 – 2 мс.

До складу виробу входять:

– плата розширення ЕОМ (АМП);

– носій інформації з інсталяційним пакетом програм;

– носій інформації з унікальним ідентифікатором;

– носій ключової інформації (НКІ) з початковими даними автентифікації АМП;

– комплект експлуатаційних документів;

– комплект тари й упакування.

АМП включає такі функціональні вузли:

– сигнальний процесор із вбудованим оперативним запам'ятовуючим пристроєм (ОЗП);

– постійний запам'ятовуючий пристрій (ПЗП);

– динамічний ОЗП, призначений для тимчасового збереження даних і модулів програм, що виконуються;

– контролер інтерфейсу шини PCI-32;

– контролер шини USB 1.1, призначений для забезпечення збереження та завантаження особистого ключа ЕЦП з/до АМП;

– апаратний прискорювач, призначений для скорочення часу виконання криптографічних операцій;

– генератор випадкових чисел (ГВЧ);

– пристрій керування, призначений для забезпечення обміну інформацією між сигнальним процесором і контролерами шин PCI-32 і USB 1.1, а також для первісної ініціалізації елементів АМП;

– генератори частоти 33 МГц та 12 МГц, призначені для формування тактових частот для елементів АМП.

Сигнальний процесор призначений для виконання внутрішніх програмних компонентів.

ПЗП призначений для збереження:
– програм універсального ядра;
– конфігураційного файлу апаратного прискорювача;
– програм криптографічного модуля;
– ключових даних;
– даних автентифікації користувача.

Динамічний ОЗП призначений для тимчасового зберігання модулів програм, що виконуються, і даних.

Пристрій керування призначений для реалізації протоколів обміну між сигнальним процесором і контролерами шин PCI-32 і USB 1.1, а також для первісної ініціалізації вузлів АМП.

Контролер інтерфейсу шини PCI-32, призначений для забезпечення введенння/ виведення даних і команд, що надходять шиною PCI-32 від ЕОМ, повинен реалізувати протокол обміну за специфікацією v2.1 PCISIG або v2.2 UPCISIG та двонаправлений обмін 32-розрядними словами з ЕОМ за командами IN/OUT у темпі шини PCI-32, а також видачу переривань до ЕОМ.

Контролер інтерфейсу шини PCI-32 повинен забезпечувати тимчасове збереження даних і команд, що надходять шиною PCI-32 від ЕОМ, у трьох 32-розрядних службових регістрах: регістрі зв'язку, регістрі даних і регістрі стану.

Регістр зв'язку призначений для збереження даних і статусів завершення команд, які записуються до нього програмами універсального ядра.

Після апаратного (програмного) скидання АМП, автоматичного тестування функціональних елементів і перевірки цілісності внутрішніх програм видаються сигнали закінчення виконання поточної команди і готовності до прийому наступної команди, а також до регістру зв'язку повинен записуватись статус завершення поточної команди.

Регістр зв'язку записує статус завершення команди щодо підтвердження правильності виконання поточної команди після кожного звертання до АМП.

Системні програмні компоненти, що виконуються в ЕОМ, повинні забезпечувати зчитування вмісту регістру зв'язку.

Регістр даних призначений для прийому та збереження команд і даних, що надходять від ЕОМ.

Регістр стану призначений для запису, збереження та видачі сигналів синхронізації роботи АМП.

ГВЧ призначений для формування послідовностей випадкових бітів при генерації випадкових чисел для алгоритму ЕЦП згідно з ДСТУ 4145-2002.

ГВЧ включає:

– два ідентичних незалежних аналого-цифрових канали на базі шумового діода КГ401 і схеми формування амплітуди вихідного сигналу;

– цифровий канал, що забезпечує прийом сигналів від двох аналого-цифрових каналів, цифрову обробку цих сигналів для вирівнювання ймовірності появи «0» і «1», послідовне побітове запам'ятовування випадкового числа в 64-розрядному зсувному регістрі.

ГВЧ забезпечує формування 64-бітового випадкового числа за командою, що надходить від внутрішніх програм.

Як НКІ для зберігання даних автентифікації та резервних копій особистого

ключа ЕЦП повинні використовуватися електронні ідентифікатори (носії) uaToken виробництва ТОВ «Технотрейд» або електронні ключі «Кристал-1» власного виробництва.

Програми АМП включають:

– внутрішні програмні компоненти АМП (програми універсального ядра та програми криптографічного модуля);

– системні програмні компоненти (драйвери або модулі ядра ОС Microsoft Windows та Linux/UNIX);

– програмний комплекс тестування та конфігурування АМП (модуль, що виконується для ОС Microsoft Windows та ОС Linux/UNIX).

Програми універсального ядра АМП призначені для:

– управління функціонуванням вузлів АМП;

– перевірки роботоздатності вузлів АМП та цілісності внутрішніх програм;

– ідентифікації АМП з боку системних програмних компонентів ЕОМ;

– управління обміном даними з ЕОМ за допомогою контролеру інтерфейсу шини PCI-32 та із зовнішніми НКІ, за допомогою інтерфейсу шини USB 1.1, через прийомний і передавальний буфери обміну вбудованого ОЗП;

– зчитування з прийомного буферу вхідних даних, що надходять від ЕОМ через контролер інтерфейсу шини PCI-32;

– обробки команд, що передані з ЕОМ, та виконання відповідних внутрішніх програм криптографічного модуля, що виконують перетворення вхідних даних на вихідні;

– запису в передавальний буфер і видачі через контролер PCI-32 результатів виконання команд і вихідних даних в ЕОМ.

Програми криптографічного модуля АМП призначені для реалізації:

– прийому та збереження у ПЗП загальних параметрів для алгоритму ЕЦП згідно з ДСТУ 4145-2002;

– генерації особистого ключа ЕЦП з використанням алгоритму генерації випадкових бітових послідовностей згідно з ДСТУ 4145-2002 і вбудованого апаратного ГВЧ;

– збереження особистого ключа ЕЦП у ПЗП в зашифрованому вигляді;

– створення резервних копій особистого ключа ЕЦП на зовнішніх НКІ в захищеному вигляді;

– відновлення особистого ключа ЕЦП з резервних копій на зовнішніх НКІ;

– знищення особистого ключа ЕЦП у вбудованому ПЗП та на зовнішніх НКІ;

– формування ЕЦП від даних, що завантажуються з ЕОМ, за алгоритмом згідно з ДСТУ 4145-2002 з використанням особистого ключа ЕЦП;

– прийому та збереження у ПЗП ДКЕ для ГОСТ 28147-89, що використовується в алгоритмі генерації випадкових бітових послідовностей за ДСТУ 4145-2002 (ДКЕ ГПВЧ) при генерації особистого ключа ЕЦП, та формування ЕЦП;

– прийому та збереження ДКЕ для ГОСТ 28147-89, що використовується під час резервного копіювання та відновлення особистого ключа ЕЦП, шляхом відповідного виконання процедур зашифрування та розшифрування особистого ключа ЕЦП за алгоритмом згідно з ГОСТ 28147-89 у режимі простої заміни (ДКЕ резервного копіювання);

– автентифікації користувача перед початком роботи шляхом послідовного виконання:

• порівняння пароля доступу користувача з еталоном, що зберігається у ПЗП;

• зчитування випадкового числа довжиною 16 байт із зовнішнього НКІ, що приєднується до АПМ під час автентифікації, з еталоном, що зберігається у ПЗП;

– встановлення або зміну даних автентифікації користувача шляхом послідовного виконання:

• прийому та збереження у ПЗП пароля доступу користувача;

• генерації випадкового числа довжиною 16 байт та збереження його у ПЗП та на зовнішній НКІ;

• прийому та запису в ПЗП довільних даних користувача;

• зберігання та надання доступу до довільних даних користувача в АМП;

• знищення довільних даних користувача в ПЗП.

Системні програмні компоненти призначені для:

– забезпечення коректного розпізнавання АМП ОС ЕОМ;

– ідентифікацію АМП;

– запису в приймальний буфер АМП вхідних даних;

– передачу кодів команд для виконання відповідних внутрішніх програм криптографічного модуля, які виконують перетворення вхідних даних на вихідні;

– зчитування з передавального буфера АМП результатів виконання команд і вихідних даних.

Програмний комплекс тестування та конфігурування призначений для:

– перевірки роботоздатності АМП;

– конфігурування параметрів АМП в ОС ЕОМ;

– завантаження в АМП загальних параметрів для алгоритму ДСТУ 4145-2002;

– завантаження в АМП ДКЕ для ГОСТ 28147-89, що використовується в алгоритмі генерації випадкових бітових послідовностей за ДСТУ 4145-2002;

– завантаження в АМП ДКЕ для ГОСТ 28147-89, що використовуються під час резервного копіювання та відновлення особистого ключа ЕЦП;

– встановлення або зміну даних автентифікації користувача шляхом їх завантаження в АМП;

– ініціювання створення резервних копій особистого ключа ЕЦП та відновлення ключа з резервних копій на зовнішніх НКІ.

Спеціальні вимоги до показників призначення виробу

Після апаратного скидання АМП виконується автоматичне тестування функціональних елементів і внутрішніх програм. Тестування функціональних елементів включає статистичний контроль виходу апаратного ГВЧ.

Перевірка правильності виконання криптографічних перетворень включає перевірки таких процедур:

1) зашифрування і розшифрування за алгоритмом ГОСТ 28147-89 в режимі простої заміни (контрольні приклади (тести) № 1, 9 з методики перевірки правильності програмної реалізації алгоритму шифрування відповідно ГОСТ 28147-89;

2) формування та перевіряння ЕЦП за алгоритмом згідно з ДСТУ 4145-2002 (контрольні приклади (тести) № 139, 142 (варіанти 1, 3) з методики перевірки правильності програмної реалізації алгоритмів формування та перевіряння цифрового підпису згідно з ДСТУ 4145-2002;

3) статистичний контроль виходу апаратного ГВС повинен здійснюватися згідно з методикою генерації ключових даних.

У разі непроходження окремого тесту видається статус непроходження із зазначенням типу тесту. Подальше виконання наступних тестів і використання АМП блокується.

При неуспішному виконанні тестування АМП з першого разу виконується повторне тестування. При успішному повторному тестуванні блокування знімається. У разі повторного невиконання блокування не знімається і АМП вважається несправним.

Порядок генерації ключових даних повинен здійснюватися згідно з методикою генерації ключових даних.

До складу ключових даних АМП входять:

– ДКЕ для ГОСТ 28147-89, що використовується у алгоритмі генерації випадкових бітових послідовностей згідно з ДСТУ 4145-2002;

– ДКЕ для ГОСТ 28147-89, що використовуються під час резервного копіювання та відновлення особистого ключа ЕЦП;

– загальні параметри ЕЦП для алгоритму ДСТУ 4145-2002;

– особистий і відкритий ключі ЕЦП для алгоритму ДСТУ 4145-2002.

ДКЕ для ГОСТ 28147-89 та загальні параметри ЕЦП для алгоритму ДСТУ 4145-2002 завантажуються з ЕОМ у АМП під час генерації ключів та зберігаються у внутрішньому ПЗП.

Особистий і відкритий ключі ЕЦП генеруються в середині АМП. Після чого особисті ключі зберігаються у внутрішньому ПЗП, а відкриті – передаються в ЕОМ для подальшого їх розповсюдження.

Параметри еліптичних кривих для алгоритму ДСТУ 4145-2002, та ДКЕ для алгоритму ГОСТ 28147-89 постачаються відповідно до вимог контролюючого органу. Термін дії ДКЕ – 1 рік. Формат ДКЕ для введення в АМП повинен бути визначений в експлуатаційній документації на АМП.

Перед використанням АМП виконується:

– ідентифікація пристрою системними програмними компонентами ЕОМ;

– автентифікація користувача.

Ідентифікація АМП виконується шляхом виконання логічних операцій над 32-розрядним індивідуальним ідентифікатором, що надходить від системних програмних компонентів ЕОМ, та 32-розрядною індивідуальною маскою АМП, що зберігається в ПЗП, з наступним порівнянням отриманого результату з індивідуальним серійним номером АМП.

Збереження індивідуальної маски та серійного номера АМП у блоках 0, 1 ПЗП та її запис в область пам'яті програм універсального ядра АМП здійснюється за допомогою спеціалізованого технологічного стенда при виробництві.

У разі задання невідповідного ідентифікатора АМП формується статус некоректного завершення ідентифікації, поки не буде введений дійсний ідентифікатор.

У разі введення невідповідного ідентифікатора АМП декілька разів підряд виконується стирання вмісту ПЗП. Відновлення працездатності АМП після стирання вмісту ПЗП здійснюється шляхом завантаження на спеціалізованому технологічному стенді.

Захист ключових даних і даних автентифікації в ПЗП здійснюється шляхом шифрування за ГОСТ 28147-89 у режимі простої заміни та вироблення імітовставки за ГОСТ 28147-89 з використанням ключа для заповнення КЗП для ГОСТ 28147-89 та ДКЕ (ключі захисту ПЗП), що записуються в АМП за допомогою спеціалізованого технологічного стенда при виробництві.

Автентифікація користувача виконується таким чином:

1) програмний комплекс з ЕОМ передає у АМП пароль доступу користувача;

2) АМП здійснює порівняння пароля доступу з еталоном, що зберігається у ПЗП;

3) АМП здійснює зчитування випадкового числа довжиною 16 байт із зовнішнього НКІ, що приєднується до АПМ під час автентифікації, та порівнює його з еталоном, що зберігається у ПЗП.

На підставі результату двох порівнянь АМП приймається рішення про успішність чи неуспішність автентифікації.

Захист особистого ключа ЕЦП при резервному копіюванні та записі на зовнішні НКІ здійснюється шляхом шифрування за ГОСТ 28147-89 у режимі простої заміни та вироблення імітовставки за ГОСТ 28147-89 з використанням спільного ключа для заповнення КЗП для ГОСТ 28147-89, який обчислюється шляхом додавання двох ключів (ключі захисту резервних копій) за модулем 2. Два ключі резервних копій генеруються в АМП під час створення резервних копій. ДКЕ для ГОСТ 28147-89, що використовується при захисті, завантажується в АМП з ЕОМ.

Кожний ключ захисту резервної копії записується на окремий НКІ разом із зашифрованим особистим ключем ЕЦП. Відновлення особистого ключа ЕЦП в АМП можливе тільки за наявності двох НКІ.

Захист від НСД до інформації, що обробляється в АМП, здійснюється шляхом:

– використання командного (процедурного) інтерфейсу взаємодії системних програмних компонентів з АМП, що виключає прямий доступ до внутрішніх вузлів і програм АМП;

– обов'язкової ініціалізації АМП із застосуванням індивідуального ідентифікатора АМП;

– зберігання криптографічного модуля в ПЗП у зашифрованому вигляді;

– виконання програм криптографічного модуля тільки у вбудованому ОЗП сигнального процесора (з попереднім розшифруванням безпосередньо перед виконанням в ОЗП);

– зберігання ключових даних (ДКЕ, особистого ключа ЕЦП) і даних автентифікації користувача в ПЗП у захищеному вигляді;

– зберігання особистого ключа ЕЦП при резервному копіюванні в захищеному вигляді;

– автентифікації користувача до початку роботи на основі пароля доступу та зовнішнього НКІ.

Характеристика надійності виробу

Показники надійності АМП належать до групи 2, вид відновлюваний, відповідно до ГОСТ 27.003-83.

Номенклатура показників для нормальних кліматичних умов експлуатації за ГОСТ 21552-84:

– середній наробіток на відмовлення – не менше 15000 г;

– середній час відновлення працездатного стану – більше 0,5 г;

– середній термін служби – 10 років, з урахуванням проведення відновлювальних робіт;

– коефіцієнт технічного використання – не менше 0,95.

АМП забезпечує як цілодобову, так і змінну роботу з урахуванням проведення технічного обслуговування.

Характеристика безвідмовності:

– ресурс виробу до першого ремонту за технічним станом – 15000 годин протягом терміну служби, у тому числі термін збереження 1 рік;

– міжремонтний ресурс – 8500 годин при ремонті за технічним станом протягом терміну служби.

Час готовності АМП, встановленого в ЕОМ, не повинен перевищувати 10 секунд (з моменту запуску тестування).

Технічне обслуговування АМП, встановленого в ЕОМ, повинне проводитися разом з ЕОМ згідно з ТУ на ЕОМ та експлуатаційною документацією на АМП.

У ході виконання роботи підлягає розробці:

– конструкторська та експлуатаційна документація на АМП;

– програмна документація;

– інструкція щодо порядку генерації ключових даних і поводження з ключовими документами;

– інструкція щодо забезпечення безпеки експлуатації АМП.

Конструкторська та експлуатаційна документація на АМП розробляється відповідно до вимог ГОСТ 2.102-68 і включає:

– паспорт;

– технічний опис;

– інструкцію з експлуатації;

– збіркове креслення;

– специфікацію;

– схему електричну функціональну;

– схему електричну принципову;

– збіркове креслення кронштейна.

Програмна документація на внутрішні програмні компоненти АМП, системні програмні компоненти та програмний комплекс тестування розробляються відповідно до вимог ГОСТ 19.101-77 і включають:

– специфікацію;

– тексти програм;

– описи програм;

– відомість експлуатаційних програмних документів;

– настанови операторам.

11.4. АПАРАТНО-ПРОГРАМНИЙ КРИПТОГРАФІЧНИЙ ЗАСІБ «ГРЯДА-61»

Апаратний засіб КЗІ «Гряда-61» криптографічним модулем (КМ) типу «П» та «Ш», класу В2.

КМ призначений для апаратної реалізацій криптографічних перетворень у складі апаратно-програмних засобів і комплексів КЗІ, що реалізовані на основі ЕОМ.

Область застосування: апаратно-програмні засоби та комплекси КЗІ типу «П», «Ш» та «Р», що призначені для захисту конфіденційної інформації.

Виріб виконує такі функції:

– автентифікацію оператора ЕОМ під час доступу до криптомодуля;

– генерацію особистих і відкритих ключів для алгоритму ЕЦП;

– генерацію особистих і 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;

– шифрування даних;

– формування та перевірки 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 й працездатності вбудованого програмного забезпечення та ін.

Область застосування пристрою – апаратно-програмні засоби та комплекси КЗІ типу «К», «Ш», «П» та «Р», призначені для захисту конфіденційної інформації, що не є власністю держави, а також інформаційно-телекомунікаційні системи, призначені для обробки конфіденційної інформації, що не є власністю держави.

Зовнішній вигляд виробу наведено на рис.11.6.

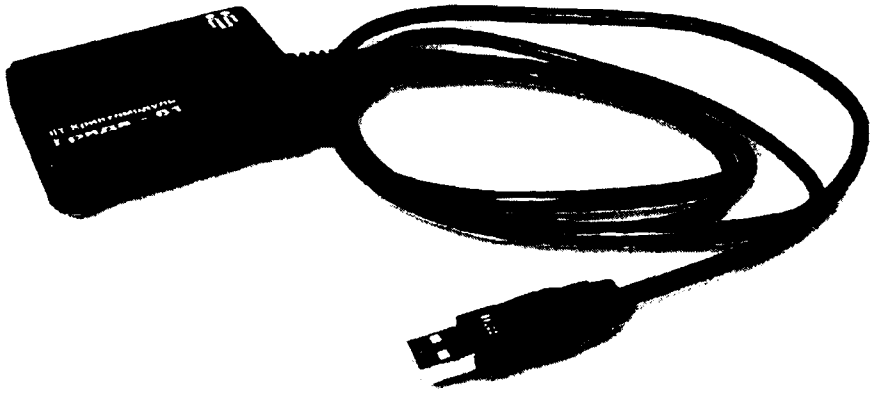

Рис. 11.6. Апаратно-програмний криптографічний засіб «Гряда-61»

КМ виконаний у вигляді малогабаритного USB-пристрою, що приєднується до ЕОМ за допомогою незнімного кабелю.

Конструктивно КМ виконаний на двошаровій друкованій платі, яка встановлена у пластиковий корпус та залита компаундом, що формує захисний шар. На друкованій платі встановлюються електронні компоненти КМ. До друкованої плати нерозбірно приєднаний USB-кабель.

КМ виконаний у кліматичному виконанні УХЛ групи 4.1 згідно з ГОСТ 21552-84. Відповідно до цього КМ належить до групи 1 технічних засобів, призначених для експлуатації в наземних стаціонарних приміщеннях і спорудах. Електроживлення КМ, з'єднаного з ЕОМ через USB-з'єднувач, здійснюється від блоку електроживлення ЕОМ через контакти USB-з'єднувача по ланцюгу +5 В ± 10 %.

Основні масогабаритні й інші технічні характеристики пристрою наведено у табл. 11.3.

Таблиця 11.3. **Основні масогабаритні та інші технічні характеристики пристрою**

Найменування параметру	Значення
Габаритні розміри без урахування кабеля (довжина) × (ширина) × (висота), мм, не більше	66×50×21
Довжина USB-кабеля, м	0,9
Маса, кг, не більше	0,03
Споживана потужність від блоку електроживлення ЕОМ +5В ± 10 %, Вт, не більше:	0,5

Криптографічний модуль реалізує такі криптографічні алгоритми й протоколи:

– шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни та режим вироблення імітовставки);

– ЕЦП за ДСТУ 4145-2002 (усі довжини ключів передбачені стандартом);

– гешування за ГОСТ 34.311-95;

– протокол розподілу ключових даних Діффі-Геллмана в групі точок еліптичної кривої (довжина ключа до 571 бітів).

Швидкість формування ЕЦП за ДСТУ 4145-2002, поле 257–100 мс. Швидкість формування спільного секрету Діффі–Геллмана в групі точок еліптичної кривої, поле 571–800 мс.

Комплектність виробу наведено в табл. 11.4.

Допускається комплектація партії виробів одним комплектом експлуатаційних документів. При цьому паспорт оформлюється на декілька виробів, позначення яких наводиться у відомостях про упакування (п. 5).

Таблиця 11.4. **Комплектність виробу**

Позначення	Найменування	Кіл.	Заводський (або ін.) номер	Примітки
ЄААД.469535.044	Криптомодуль «Гряда-61»	–	див. п. 5	
ЄААД.00044-01 97 01-1	Носій інформації з інсталяційним пакетом програм	1		Оптичний компакт-диск (CD), може не комплектуватись
ЄААД.469535.044 ЕД	Комплект експлуатаційних документів	1		Може не комплектуватись
–	Упакування	–	–	

Програми КМ включають:

– внутрішні програмні компоненти КМ (внутрішні програми);

– системні програмні компоненти (драйвери або модулі ядра ОС Microsoft Windows та Linux/UNIX);

– програмний комплекс тестування та конфігурування КМ (модуль, що виконується для ОС Microsoft Windows та ОС Linux/UNIX).

Внутрішні програми КМ призначені для:

– прийому та зберігання у ПЗП загальних параметрів для алгоритму ЕЦП згідно з ДСТУ 4145-2002 та протоколу розподілу ключів;

– генерації особистого ключа ЕЦП та протоколу розподілу ключів з використанням алгоритму генерації випадкових бітових послідовностей згідно з ДСТУ 4145-2002 і вбудованого апаратного ГВС;

– зберігання у ПЗП особистих ключів ЕЦП та протоколу розподілу ключів в зашифрованому вигляді з контролем цілісності;

– знищення з ПЗП особистих ключів ЕЦП та протоколу розподілу ключів;

– формування ЕЦП від даних, що завантажуються з ЕОМ, за алгоритмом згідно з ДСТУ 4145-2002 з використанням особистого ключа ЕЦП;

– генерації ключів сеансу для ГОСТ 28147-89;

– формування спільного секретного ключа за протоколом розподілу ключових даних з використанням власного особистого ключа протоколу розподілу та відкритого ключа протоколу розподілу отримувача;

– зашифрування та розшифрування ключів сеансу для ГОСТ 28147-89 з використанням сформованого спільного секретного ключа за алгоритмом згідно з ГОСТ 28147-89 (режим простої заміни);

– прийому та зберігання у ПЗП 2-х ДКЕ для ГОСТ 28147-89, що використовуються в алгоритмі генерації випадкових бітових послідовностей за ДСТУ 4145-2002 та протоколі розподілу ключових даних;

– автентифікації користувача перед початком роботи шляхом гешування пароля доступу до КМ за алгоритмом згідно з ГОСТ 34.311-95 та порівнянням з еталоном, що зберігається у ПЗП;

– управління параметрами автентифікації користувача;
– прийому, запису та зберігання у ПЗП довільних даних користувача;
– надання доступу та знищення довільних даних користувача з ПЗП.

Системні програмні компоненти призначені для:
– забезпечення коректного розпізнавання КМ ОС ЕОМ;
– передачі кодів команд та вхідних даних для виконання відповідних внутрішніх програм криптографічного модуля, які виконують перетворення вхідних даних на вихідні;
– отримання з КМ результатів виконання команд і вихідних даних.

Програмний комплекс тестування та конфігурування призначений для:
– перевірки роботоздатності КМ;
– конфігурування параметрів КМ в ОС ЕОМ;
– встановлення або зміни даних автентифікації користувача КМ шляхом їх завантаження в КМ;
– форматування КМ, що включає знищення особистих ключів і довільних даних користувача в КМ та встановлення даних автентифікації.

Вимоги до ключових даних та спеціальні вимоги аналогічні тим, що висуваються до апаратно-програмного модуля «Гряда 41П», що наведені в п. 11.4.

11.5. МЕРЕЖЕВИЙ КРИПТОМОДУЛЬ «ГРЯДА-301»

Мережевий криптомодуль «Гряда-301» (далі – МКМ) є програмно-апаратним засобом серверного типу, тип пристрою – апаратний засіб КЗІ, вид пристрою – «Б», підвид «Б2», категорія пристрою – «П» та «Ш», клас пристрою – «Б1».

Призначення виробу: МКМ призначений для апаратної реалізацій криптографічних перетворень у складі апаратно-програмних засобів і комплексів КЗІ, що реалізовані на основі ЕОМ.

Зовнішній вигляд мережевого криптомодуля «Гряда-301» наведено на рис.11.7. Основні масогабаритні та інші технічні характеристики МКМ повинні відповідати зазначеним у табл. 11.5.

Рис. 11.7. Мережевий криптомодуль «Гряда-301»

Область застосування: апаратно-програмні засоби та комплекси КЗІ типу «П», «Ш» та «Р» , що призначені для захисту конфіденційної інформації.

До складу виробу входять:
– мережевий криптомодуль (МКМ);
– носій інформації з інсталяційним пакетом програм;
– комплект експлуатаційних документів;
– комплект тари та упакування.

МКМ виконується у вигляді окремого пристрою, що з'єднується з ЕОМ через інтерфейс Ethernet за допомогою кабелю.

Конструктивно МКМ виконаний на системній платі, яка разом із джерелом живлення та іншими елементами встановлюються у металевий корпус висотою 1U або 2U, призначений для встановлення в 19-дюймову стійку.

Електроживлення МКМ здійснюється від електричної мережі.

Таблиця 11.5. **Основні масогабаритні й інші технічні характеристики МКМ**

Найменування	Норма
Габаритні розміри без урахування кабелів та елементів кріплення, мм, не більше: – ширина – висота – глибина	 430 88 485
Маса, кг, не більше	18
Напруга живлення від електричної мережі, В	100–240
Частота електричної мережі, Гц	50–60
Споживана потужність від електричної мережі, Вт, не більше:	500

МКМ виконує такі функції:

1) управління особистими ключами ЕЦП та протоколу розподілу ключових даних, що включає:

– прийом та зберігання загальних параметрів для алгоритму ЕЦП згідно з ДСТУ 4145-2002 та протоколу розподілу ключів;

– генерацію особистого ключа ЕЦП та протоколу розподілу ключів з використанням алгоритму генерації випадкових бітових послідовностей згідно з ДСТУ 4145-2002 і вбудованого апаратного генератора випадкових сигналів (ГВС);

– зберігання особистих ключів ЕЦП та протоколу розподілу ключів в зашифрованому вигляді з контролем цілісності;

– запис особистих ключів ЕЦП та протоколу розподілу ключів на зовнішній носій ключової інформації (НКІ) у захищеному вигляді (резервне копіювання особистих ключів);

– зчитування особистих ключів ЕЦП та протоколу розподілу ключів із зовнішнього НКІ та запис у МКМ (відновлення особистих ключів);

– знищення особистих ключів ЕЦП та протоколу розподілу ключів;

2) формування ЕЦП від даних, що завантажуються з ЕОМ, за алгоритмом згідно з ДСТУ 4145-2002 з використанням особистого ключа ЕЦП;

3) генерацію ключів сеансу для ДСТУ ГОСТ 28147:2009;

4) формування спільного секретного ключа за протоколом розподілу ключових даних з використанням власного особистого ключа протоколу розподілу та відкритого ключа протоколу розподілу отримувача;

5) зашифрування і розшифрування ключів сеансу для ДСТУ ГОСТ 28147:2009 з використанням сформованого спільного секретного ключа за алгоритмом згідно з ДСТУ ГОСТ 28147:2009 (режим простої заміни);

6) прийом та зберігання 2-х ДКЕ для ДСТУ ГОСТ 28147:2009, що використовуються в алгоритмі генерації випадкових бітових послідовностей за ДСТУ 4145-2002 та в протоколі розподілу ключових даних;

7) автентифікацію користувача перед початком роботи шляхом гешування пароля доступу до МКМ за алгоритмом згідно з ГОСТ 34.311-95 та порівнянням з еталоном, що зберігається в МКМ;

8) управління параметрами автентифікації користувача, що включає встановлення та зміну даних автентифікації користувача;

9) прийом, зберігання, надання доступу та знищення довільних даних користувача в МКМ.

– МКМ включає такі функціональні вузли:

– системна плата;

– один або два центральні процесори;

– оперативний запам'ятовуючий пристрій (ОЗП);

– постійний запам'ятовуючий пристрій (ПЗП) у вигляді накопичувача на жорсткому магнітному диску (НЖМД) або електронного (flash-) диску;

– вбудований криптомодуль (ВКМ);

– Ethernet-контролер;

– USB-контролер;

– джерело живлення.

Системна плата призначена для розміщення та з'єднання центральних процесорів, ОЗП, ПЗП, контролерів Ethernet, USB та ВКМ.

Системна плата включає генератори системних частот, формувачі напруг живлення центральних процесорів і пам'яті, шини адрес, даних, керування, стандартні роз'єми для встановлення елементів та приєднання ВКМ.

Центральні процесори призначені для виконання внутрішніх програм.

ОЗП призначений для розміщення внутрішніх програм, що виконуються, та тимчасових даних.

ПЗП призначений для зберігання та завантаження внутрішніх програм.

ВКМ призначений для:

– генерації послідовностей випадкових чисел;

– зберігання ключових даних;

– зберігання даних автентифікації користувача.

Як ВКМ повинен використовуватися криптомодуль «Гряда-61» або електронний ключ «Кристал-1».

Ethernet-контролер призначений для підключення МКМ до ЕОМ користувача. Контролер повинен мати електричний інтерфейс типу Ethernet 100/1000 із роз'ємом RJ-45.

USB-контролер призначений для приєднання ВКМ і зовнішніх криптомодулів або електронних ключів. Для приєднання зовнішніх криптомодулів або електронних ключів МКМ повинен мати не менше одного роз'єму USB-розетки типу «А» на передній панелі, а для приєднання ВКМ – не менше одного внутрішнього роз'єму на системній платі.

Джерело живлення призначене для перетворення напруги електричної мережі на напругу, що потребують системна плата та вбудовані пристрої.

Як НКІ для зберігання резервних копій особистих ключів повинні використовуватися криптомодулі «Гряда-61» або електронні ключі «Кристал-1».

Програми МКМ включають:

– внутрішні програмні компоненти МКМ (внутрішні програми);

– системні програмні компоненти (драйвери чи бібліотеки динамічного компонування для ОС Microsoft Windows або модулі ядра чи об'єктів, що поділяються, для ОС Linux/UNIX);

– програмний комплекс тестування та конфігурування МКМ (модуль, що виконується для ОС Microsoft Windows та ОС Linux/UNIX).

Внутрішні програми МКМ призначені для:

– прийому та зберігання у ВКМ загальних параметрів для алгоритму ЕЦП згідно з ДСТУ 4145-2002 та протоколом розподілу ключів;

– генерації особистого ключа ЕЦП та протоколу розподілу ключів з використанням алгоритму генерації випадкових бітових послідовностей згідно з ДСТУ 4145-2002 і вбудованим апаратним ГВС;

– зберігання у ВКМ особистих ключів ЕЦП та протоколу розподілу ключів в зашифрованому вигляді з контролем цілісності;

– знищення з ВКМ особистих ключів ЕЦП та протоколу розподілу ключів;

– створення резервних копій особистих ключів ЕЦП та протоколу розподілу ключів на зовнішньому НКІ в захищеному вигляді;

– відновлення особистих ключів ЕЦП та протоколу розподілу ключів з резервних копій на зовнішньому НКІ;

– формування ЕЦП від даних, що завантажуються з ЕОМ, за алгоритмом згідно з ДСТУ 4145-2002 з використанням особистого ключа ЕЦП;

– генерації сеансових ключів для ДСТУ ГОСТ 28147:2009;

– формування спільного секретного ключа за протоколом розподілу ключових даних з використанням власного особистого ключа протоколу розподілу та відкритого ключа протоколу розподілу отримувача;

– зашифрування та розшифрування ключів сеансу для ДСТУ ГОСТ 28147:2009 з використанням сформованого спільного секретного ключа за алгоритмом згідно з ДСТУ ГОСТ 28147:2009 (режим простої заміни);

– прийому та зберігання у ВКМ 2-х ДКЕ для ДСТУ ГОСТ 28147:2009, що використовуються в алгоритмі генерації випадкових бітових послідовностей за ДСТУ 4145-2002 та в протоколі розподілу ключових даних;

– автентифікації користувача перед початком роботи шляхом гешування пароля доступу до МКМ за алгоритмом згідно з ГОСТ 34.311-95 та порівнянням з еталоном, що зберігається у ВКМ;

– управління параметрами автентифікації користувача;

– прийому, запису та зберігання у ВКМ довільних даних користувача;

– надання доступу та знищення довільних даних користувача з ВКМ.

Системні програмні компоненти призначені для:

– забезпечення пошуку та розпізнавання МКМ через мережу;

– передачу кодів команд та вхідних даних для виконання відповідних внутрішніх програм, які виконують перетворення вхідних даних на вихідні;

– отримання з МКМ результатів виконання команд та вихідних даних.

Програмний комплекс тестування та конфігурування призначений для:

– перевірки роботоздатності МКМ;

– конфігурування параметрів МКМ в ОС ЕОМ;

– встановлення або зміну даних автентифікації користувача МКМ шляхом їх завантаження у МКМ;

– форматування МКМ, що включає знищення особистих ключів та довільних даних користувача в МКМ та встановлення даних автентифікації;

– ініціювання створення резервних копій особистих ключів та відновлення ключів з резервних копій на зовнішньому НКІ.

Спеціальні вимоги до конструкції виробу

На працездатність МКМ не повинні впливати ввімкнення (вимкнення) електроживлення пристроїв, які не використовуються при функціонуванні МКМ, а також комплексів сервісної апаратури й освітлення приміщення.

Спеціальні вимоги до показників призначення виробу

Після ввімкнення електроживлення МКМ та завантаження внутрішніх програм повинне виконуватися автоматичне тестування функціональних елементів і внутрішніх програм.

Перевірка правильності виконання криптографічних перетворень повинна включати перевірки таких процедур:

– зашифрування і розшифрування за алгоритмом ДСТУ ГОСТ 28147:2009 у режимі простої заміни (контрольні приклади (тести) № 1, 5, 9, 11 з методики перевірки правильності програмної реалізації алгоритму шифрування відповідно до ГОСТ 28147-89, погодженої з ДСТСЗІ СБ України);

– вироблення імітовставки за ДСТУ ГОСТ 28147:2009 (контрольні приклади (тести) № 25, 26 з методики перевірки правильності програмної реалізації алгоритму шифрування відповідно до ГОСТ 28147-89);

– формування та перевірка ЕЦП за алгоритмом згідно з ДСТУ 4145-2002 (контрольні приклади (тести) № 142, 151, 152 з методики перевірки правильності програмної реалізації алгоритмів формування та перевіряння цифрового підпису);

– гешування за алгоритмом ГОСТ 34.311-95 (контрольні приклади (тести) № 2, 4, 6, 8 з методики перевірки правильності програмної реалізації алгоритму гешування відповідно до ГОСТ 34.311-95).

Статистичний контроль послідовностей випадкових чисел з виходу ВКМ повинен здійснюватися згідно з п. 5.1 методики генерації ключових даних.

У разі непроходження окремого тесту повинен видаватися статус непроходження із зазначенням типу тесту. Подальше виконання наступних тестів і використання МКМ повинне блокуватися.

У разі неуспішного виконання тестування МКМ з першого разу повинне виконуватися повторне тестування. При успішному повторному тестуванні блокування повинне зніматися. У разі повторного невиконання, блокування не знімається і МКМ вважається несправним.

Порядок генерації ключових даних повинен здійснюватися згідно з методикою генерації ключових даних, погодженою з ДСТСЗІ СБ України від 10.03.2005, зареєстрованою 01.11.2004 за № 85.

Протокол розподілу ключових даних повинен реалізовуватися згідно з методикою розподілу ключових даних на основі протоколу Діффі-Геллмана в групі точок еліптичної кривої, погодженою з ДСТСЗІ СБ України від 10.03.2005, зареєстрованою 01.11.2004 за № 85.

До складу ключових даних МКМ повинні входити:

– довгострокові ключові елементи (ДКЕ) для ДСТУ ГОСТ 28147:2009, що використовуються в алгоритмі генерації випадкових бітових послідовностей згідно з ДСТУ 4145-2002 та протоколі розподілу ключових даних;

– загальні параметри ЕЦП для алгоритму ДСТУ 4145-2002 та протоколу розподілу ключів;

– особистий і відкритий ключі ЕЦП для алгоритму ДСТУ 4145-2002;

– особистий і відкритий ключі протоколу розподілу ключів.

ДКЕ для ДСТУ ГОСТ 28147:2009, загальні параметри ЕЦП для алгоритму ДСТУ 4145-2002 та протоколу розподілу ключів повинні завантажуватися з ЕОМ у МКМ під час генерації ключів та зберігатися у ВКМ.

Особисті та відкриті ключі ЕЦП і протоколу розподілу ключів повинні генеруватися в середині МКМ, після чого особисті ключі повинні зберігатися у ВКМ, а відкриті – передаватися в ЕОМ для подальшого їх розповсюдження.

Параметри еліптичних кривих для алгоритму ДСТУ 4145-2002, та ДКЕ для алгоритму ДСТУ ГОСТ 28147:2009 повинні постачатися відповідно до вимог Держспецзв'язку України.

Захист від НСД до інформації, що обробляється у МКМ здійснюється шляхом:

– використання командного (процедурного) інтерфейсу взаємодії системних програмних компонентів з МКМ, що виключає прямий доступ до внутрішніх вузлів і програм МКМ;

– зберігання ключових даних (особистих ключів) у ВКМ у захищеному вигляді;

– автентифікації користувача до початку роботи з МКМ.

Захист і контроль цілісності особистих ключів у ВКМ повинен здійснюватися на паролі захисту, який передається у МКМ під час операцій з одним із особистих ключів. Особисті ключі повинні контролюватися на цілісність шляхом вироблення імітовставки за ДСТУ ГОСТ 28147:2009 та захищатися шляхом зашифрування в режимі простої заміни ДСТУ ГОСТ 28147:2009 на ключі, який отриманий шляхом гешування рядка пароля за ГОСТ 34.311-95.

Автентифікація користувача перед початком роботи повинна здійснюватися шляхом передачі у МКМ пароля доступу до МКМ, гешуванням пароля за алгоритмом згідно з ГОСТ 34.311-95 та порівнянням з еталоном, що зберігається у ВКМ.

На підставі результату порівняння МКМ повинний приймати рішення про успішність автентифікації.

Показники надійності МКМ належать до групи 2, вид – відновлюваний, відповідно до ГОСТ 27.003-90. Номенклатура показників для нормальних кліматичних умов експлуатації за ГОСТ 21552-84:

– середній наробіток на відмовлення – не менше 15000 г;

– середній час відновлення працездатного стану – більше 0,5 г;

– середній термін служби – 10 років;

– коефіцієнт технічного використання – не менше 0,95.

МКМ повинен забезпечувати як цілодобову, так і змінну роботу з урахуванням проведення технічного обслуговування.

Вимоги до безвідмовності: ресурс виробу до відмовлення за технічним станом – 15000 годин протягом терміну служби, у тому числі термін збереження 1 рік.

У ході виконання роботи підлягає розробці:

– експлуатаційна документація на МКМ;

– програмна документація;

– інструкція щодо порядку генерації ключових даних та поводження з ключовими документами;

– інструкція щодо забезпечення безпеки експлуатації МКМ.

Експлуатаційна документація на МКМ повинна розроблятися відповідно до вимог ГОСТ 2.102-68 та включати:

– паспорт;

– технічний опис;

– інструкцію з експлуатації;

– специфікацію;

– перелік елементів.

Програмна документація на внутрішні програмні компоненти МКМ, системні програмні компоненти та програмний комплекс тестування повинна розроблятися відповідно до вимог ГОСТ 19.101-77 і включати:

– специфікацію;

– тексти програм;

– описи програм;

– відомість експлуатаційних програмних документів;

– настанови операторам.