Опис програмного комплексу криптографічного захисту інформації «Криптосервер»

1. Загальна інформація

Програмний комплекс криптографічного захисту інформації «Криптосервер» (далі – Комплекс) є сукупністю програмних засобів, що призначена для забезпечення конфіденційності та цілісності інформації, яка передається між клієнтськими та серверними частинами прикладних програмних систем та забезпечує захист TCP-з'єднань з використанням механізмів та засобів криптографічного захисту інформації.

Комплекс є сукупністю засобів криптографічного захисту інформації з функціями шифрування інформації, накладання та перевірки електронного цифрового підпису, який використовується під час створення захищеного зв'язку, формування та зберігання ключової інформації, а також надання послуг встановлення автентичності даних, які надходять, зберігаються та обробляються в комп'ютеризованих системах оброблення інформації.

2. Склад Комплексу

Комплекс складається з наступних компонентів:

Центр генерації ключів (ЦГК) - програмний модуль, призначений для генерації закритих і відкритих ключів, а також для запису ключових носіїв інформації для всіх компонентів Комплексу. Центр генерації ключів встановлюється на комп'ютері, що не має мережевих з'єднань.

Відповідно до «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації», затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 р. №141 та зареєстрованим в Міністерстві юстиції України за № 862/14129 від 30.07.07, зі змінами та доповненнями, ЦГК є засобом криптографічного захисту інформації, який:

- за призначенням відноситься до категорій "П", "Ш" та "К";
- за видом виконання – "А" (засоби, які на конструктивному, алгоритмічному та програмному рівнях є єдиними виробами, що функціонують (експлуатуються) відокремлено від будь-яких інших технічних засобів);
- за класом – "Б2" (відповідає вимогам забезпечення стійкості криптоперетворення в умовах здійснення порушником навмисного зовнішнього впливу (захист від порушника другого рівня).

Центр розподілу ключів (ЦРК) - програмний модуль, призначений для зберігання та видачі мережевими каналами довіреним компонентам Комплексу сертифікатів відкритих ключів, інформації про контур безпеки, що визначає учасників захищеної мережі, та іншої службової інформації.

ЦРК є засобом криптографічного захисту інформації, який:

- за призначенням відноситься до категорій “П”, “Ш”;
- за видом виконання – “Б2” (апаратні, апаратно-програмні або програмні вироби, які підключаються до інших засобів та виконують функції криптографічних перетворень у взаємодії з ними або під їх управлінням);
- за класом – “Б2” (відповідає вимогам забезпечення стійкості криптоперетворення в умовах здійснення порушником навмисного зовнішнього впливу (захист від порушника другого рівня).

Модуль шифрування (МШ) - програмний модуль, призначений для побудови захищеної мережі шляхом створення захищених з'єднань із іншими довіреними модулями шифрування.

МШ є засобом криптографічного захисту інформації, який:

- за призначенням відноситься до категорій “П”, “Ш”;
- за видом виконання – “Б2” (апаратні, апаратно-програмні або програмні вироби, які підключаються до інших засобів та виконують функції криптографічних перетворень у взаємодії з ними або під їх управлінням);
- за класом – “Б2” (відповідає вимогам забезпечення стійкості криптоперетворення в умовах здійснення порушником навмисного зовнішнього впливу (захист від порушника другого рівня).

Модуль керування (МК) - програмний модуль, призначений для дистанційного керування компонентами Комплексу, такими як ЦРК, МШ.

МК є засобом криптографічного захисту інформації, який:

- за призначенням відноситься до категорій “П”, “Ш”;
- за видом виконання – “Б2” (апаратні, апаратно-програмні або програмні вироби, які підключаються до інших засобів та виконують функції криптографічних перетворень у взаємодії з ними або під їх управлінням);
- за класом – “Б2” (відповідає вимогам забезпечення стійкості криптоперетворення в умовах здійснення порушником навмисного зовнішнього впливу (захист від порушника другого рівня).

3. Опис функцій Комплексу

Комплекс реалізує наступні функції:

- Захист даних;
- Керування;
- Аудит;
- Ідентифікація та авторизація;
- Захист функціонування.

Захист даних

Забезпечується захист інформації, яка передається по загальнодоступним каналам передачі даних, від несанкціонованого ознайомлення й/або модифікації, шляхом шифрування даних, що передаються, встановлення захищеного каналу та передачу по ньому даних між локальними мережами.

Шифрування здійснюється на підставі сеансових ключів, що мають обмежений час життя.

Розподіл ключів здійснюється з використанням асиметричного криптографічного алгоритму узгодження ключа, що використовує закритий ключ однієї сторони обміну та відкритий ключ іншої сторони. Відкриті ключі поширюються вільно між всіма учасниками обміну. Для забезпечення цілісності та достовірності відкриті ключі підписуються ЦГК.

Для шифрування обміну даними між двома модулями використовується симетричний ключ, вироблений на основі закритого ключа одного модуля й сертифіката відкритого ключа іншого. Необхідні сертифікати запитуються модулями із ЦРК.

Для транспортування ключових даних від ЦГК до інших компонентів Комплексу повинні використовуватись носії ключової інформації.

Керування

Забезпечується можливість конфігурування та налаштування параметрів компонентів Комплексу, необхідних для їх функціонування.

Налаштування параметрів виконується Адміністратором Комплексу за допомогою відповідного компоненту (Модуль керування).

Описані параметри та налаштування одержується Модулями шифрування під час їх запуску на виконання в межах виконання процедури їх ідентифікації в структурі Комплексу.

Аудит

Компоненти Комплексу дозволяють проводити аналіз записів у файлах протоколів.

Кожний компонент Комплексу веде локальний журнал реєстрації подій, який є можливість переглянути безпосередньо на комп'ютері, на якому цей компонент встановлений. Крім того, всі події, які мали місце бути в процесі функціонування Комплексу, реєструються централізовано за допомогою засобів Модуля керування.

Ідентифікація й автентифікація

Доступ до можливостей Комплексу мають лише особи з відповідними повноваженнями.

Під час запуску на виконання кожний з компонентів Комплексу проходить процедуру ідентифікації за допомогою засобів Модуля керування. За результатами цієї процедури компонент одержує/або не одержує дозвіл на функціонування у складі Комплексу.

Захист функціонування

Компоненти Комплексу мають:

- вбудовані засоби перевірки цілісності: виконується перевірка цілісності файлів, що виконуються;
- механізми перевірки відповідності параметрів налаштування Модулів шифрування, що описані у відповідних конфігураційних файлах, параметрам, що зберігаються в централізованій базі даних Модуля керування.

4. Опис процесу функціонування

1 етап: генерація ключових даних.

Виконується за допомогою засобів ЦГК у відповідності до вимог документу «Порядок генерації та розповсюдження ключових даних». Після генерації ключові дані надаються відповідальним особами, які виконують їх інсталяцію та відповідають за збереження.

2 етап: виконання налаштування параметрів та ведення бази даних сертифікатів

Адміністратор Комплексу після генерації ключових даних компонентів Комплексу виконує імпорт всіх сертифікатів до бази даних ЦРК, після чого виконує своєчасне оновлення змін, що стосуються стану сертифікатів (відкликання, блокування, оновлення).

Крім того, за допомогою засобів МК Адміністратор виконує опис можливих зв'язків для МШ.

3 етап: процедура взаємодії модулів шифрування

Крок 1. Запуск МШ на виконання. Виконуються наступні дії:

- автентифікація та ідентифікація Адміністратора;
- перевірка цілісності МШ;
- перевірка відповідності налаштувань у конфігураційному файлі;
- реєстрація МШ модулем керування.

Крок 2. Встановлення захищеного зв'язку.

- користувач ініціює захищене з'єднання, шляхом запуску клієнтської частини прикладного програмного забезпечення;
- МШ1 визначає МШ2, з яким буде встановлено захищений зв'язок. Визначення МШ2 виконується шляхом аналізу виконаних налаштувань;
- МШ1 та МШ2 обмінюються ідентифікаційною інформацією й виконують процедури автентифікації з використанням сертифікатів відкритих ключів, які запитуються у ЦРК. Захищене з'єднання може бути встановлено тільки після виконання процедур взаємної автентифікації компонентів Комплексу.

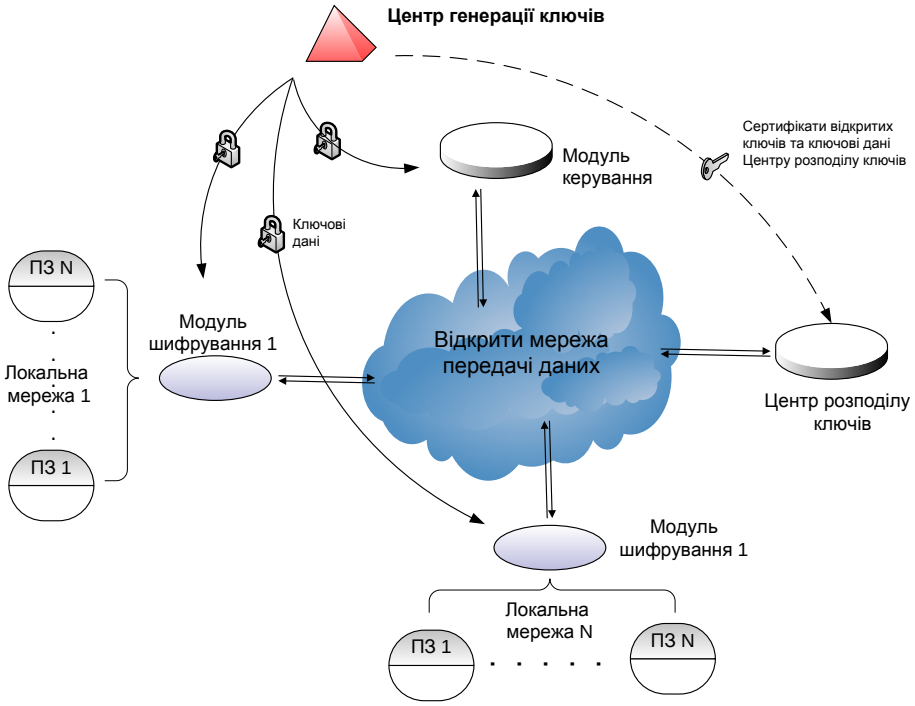


Рис. 1 Структурна схема Комплексу

5. Варіанти побудови Комплексу

Варіант 1.

ЦГК залишається у власності ТОВ «СКЗ «Криптософт». На договірній підставі, в оговорені терміни та у відповідності до розробленого протоколу виконується передача ключових даних до автоматизованої системи Замовника, в межах якої функціонує решта компонентів Комплексу.

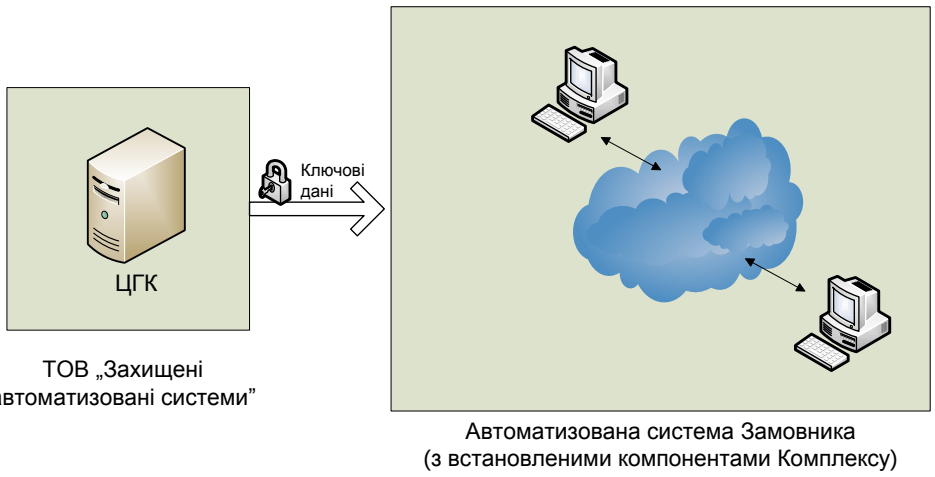


Рис. 2 Побудова Комплексу, якщо ЦГК не є власністю Замовника

Варіант 2.

Комплекс побудовано за класичною схемою (рис. 1). Модулі шифрування встановлюються на граничному ПЕОМ та забезпечують захист вихідних з’єднань, ініційованих у межах локальної мережі.

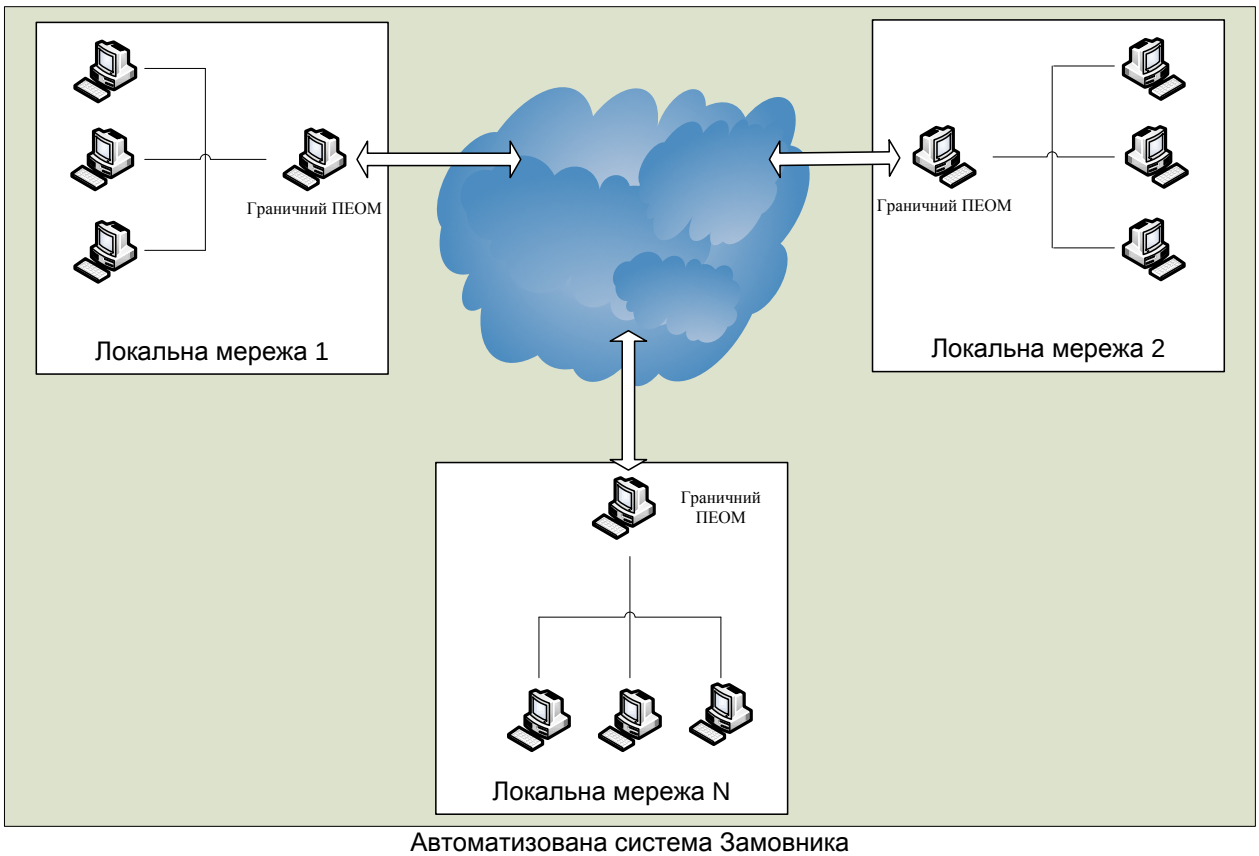


Рис. 3 Побудова Комплексу з використанням граничних ПЕОМ

На граничні ПЕОМ також встановлюються МК та ЦРК. Таким чином, канали зв'язку між граничними ПЕОМ є захищеними, в той час як з'єднання в межах локальної мережі за граничним ПЕОМ – відкритими.

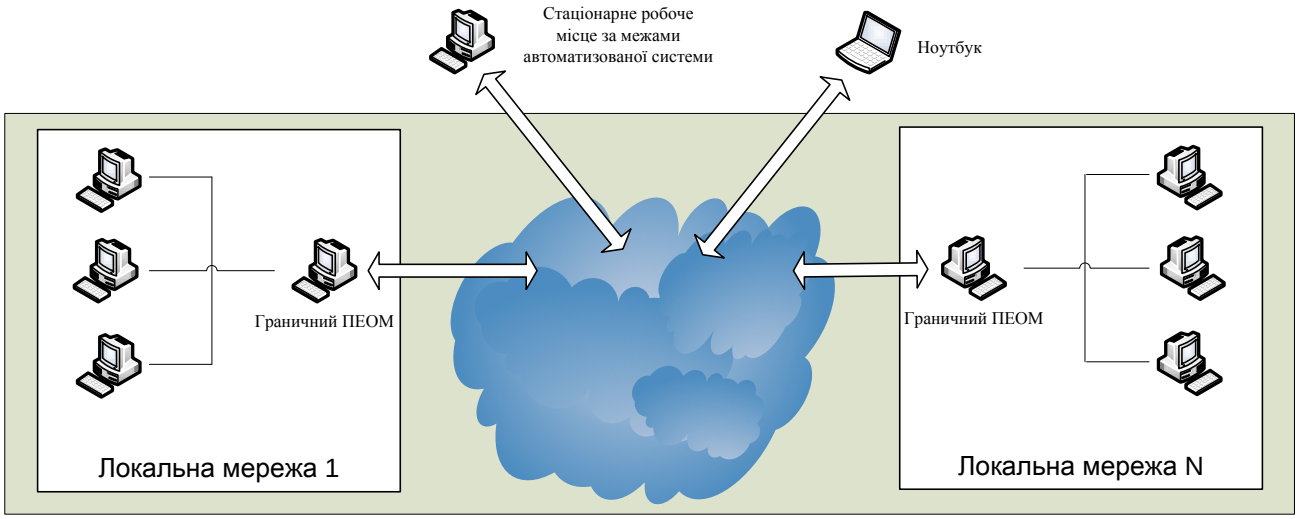
Варіант 3.

Комплекс побудовано за класичною схемою (рис. 1). Модулі шифрування встановлюються на кожний ПЕОМ. При цьому, всі описані в конфігураційному файлі з'єднання, що встановлюються в межах автоматизованої системи, будуть захищеними.

Варіант 4.

Об'єднує варіанти 2 та 3:

- Модулі шифрування встановлюються на граничному ПЕОМ та забезпечують захист вихідних з'єднань, ініційованих у межах локальної мережі;
- Модулі шифрування встановлюються на стаціонарному робочому місце, яке знаходиться за межами автоматизованої системи Замовника, або на переносному ПЕОМ, та забезпечує захист вихідних з'єднань, ініційованих користувачем зазначених засобів.



Автоматизована система Замовника

6. Криптографічні функції

Комплекс реалізує наступні криптографічні алгоритми:

- алгоритм шифрування даних відповідно до ДСТУ ГОСТ 28147:2009 у режимі гамування із зворотнім зв’язком;
- алгоритм обчислення імітовставки відповідно до ДСТУ ГОСТ 28147:2009 у режимі гамування;
- алгоритм гешування відповідно до ГОСТ 34.311-95;
- алгоритми генерації параметрів, обчислення та перевіряння електронного цифрового підпису (ЕЦП) відповідно до ДСТУ 4145-2002;
- алгоритм генерації псевдовипадкових послідовностей (ПВП) відповідно до Додатку А ДСТУ 4145-2002;
- асиметричний криптографічний алгоритм шифрування, що використовується для розподілу сеансових ключів алгоритму шифрування даних, відповідно до вимог наказу Адміністрації Держспецзв’язку № 112 від 14.05.2010 р.

Реалізація криптографічних алгоритмів міститься у програмній бібліотеці криптографічних перетворень UACrypto, що має позитивний експертний висновок за результатами державної експертизи у сфері КЗІ №5/1-4115 від 18.10.2010 р.

7. Ключова система

Комплекс використовує наступні ключові дані:

- сеансові ключі для алгоритму ДСТУ ГОСТ 28147:2009;
- довгострокові ключові елементи (ДКЕ) для алгоритму ДСТУ ГОСТ 28147:2009;
- ДКЕ для алгоритму ГОСТ 34.311-95;
- закриті та відкриті ключі асиметричних криптографічних алгоритмів.

Відповідно до свого призначення компоненти Комплексу здійснюють генерацію:

- закритого та відкритого ключів для асиметричних криптографічних алгоритмів;
- сеансових ключів для алгоритму ДСТУ ГОСТ 28147:2009 під час ініціалізації сеансу захищеного зв’язку.

Закриті ключі асиметричних криптографічних алгоритмів зберігаються у спеціальних інформаційних об’єктах – захищених ключових контейнерах, при цьому ключові дані повинні зберігатися у зашифрованому вигляді із забезпеченням контролю цілісності.

Розподіл відкритих ключів здійснюється через сертифікати відкритих ключів з використанням інфраструктури відкритих ключів, яка реалізується ЦРК Комплексу.

Розподіл сеансових ключів здійснюється з використанням асиметричного криптографічного алгоритму шифрування.

Розподіл та використання ДКЕ для алгоритму ДСТУ ГОСТ 28147:2009 повинні використовуватися відповідно до вимог Інструкції про порядок постачання і використання ключів для засобів криптографічного захисту інформації, затвердженої наказом Адміністрації ДССЗЗІ від 12.06.2007 р. № 114 та зареєстрованої у Міністерстві юстиції України 25.06.2007 р. за № 729/13996.

8. Технічні показники

За результатами внутрішніх випробувань встановлені наступні параметри:

- швидкість криптографічних перетворювань дорівнює 50 Мб/с;
- середня пропускна здатність МШ (на прикладному рівні) дорівнює 10 Мб/с.

Випробування виконувались на ПЕОМ з наступною конфігурацією:

- Pentium 4 2,8 GHz, 1 Gb, HDD 160 Gb;
- AMD Athlon XP 2,0GHz, 1Gb, HDD 80 Gb.

Примітка:

- *основні обмеження на показники пропускної здатності накладає операційна система, тому значення цієї характеристики можуть змінюватись в залежності від кількості одночасно встановлених з'єднань та потужності ПЕОМ, на якій встановлено МШ.*
- *комфортна робота користувачів з програмним забезпеченням досягається за рахунок захисту лише необхідних з'єднань, у відмінності від апаратних засобів захисту, які шифрують весь трафік.*

9. Умови виконання Комплексу

Компоненти Комплексу функціонують на ПЕОМ під керуванням операційних систем Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Vista.

Склад технічних засобів визначається вимогами зазначених операційних систем.

Вимоги до персоналу не висуваються.