УДК 004.056
DOI: 10.31673/2409-7292.2019.011620

В.М. Ахрамович, О.О. Сіренко

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ У ЛОКАЛЬНІЙ МЕРЕЖІ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЗА ДОПОМОГОЮ КОМПЛЕКСУ КОРИСТУВАЧА ЦСК «ІІТ КОРИЧСТУВАЧ ЦСК-1»

Розглянуті основні компоненти підвищення ефективності криптографічного захисту інформації у локальній мережі об'єкта інформаційної діяльності: Проблеми захисту інформації в локальних обчислювальних мережах; комплекс користувача ЦСК "ІІТ Користувач ЦСК-1";

Ключові слова: *інформація, автентифікація, шифрування, захист, криптографія, ЛОМ. аспекти, вразливості, видалення, спотворення, цілісність, програмні засоби, апаратні засоби, криптомодулі, сертифікат, сеанси, розподіл ключів, електронно цифровий підпис, обробка запиту, генерація, захищений сеанс, протоколи розподілу ключів.,*

Вступ

Проблеми захисту інформації в локальних обчислювальних мережах (ЛОМ) постійно знаходяться в центрі уваги не тільки фахівців з розробки і використання цих систем, а й широкого кола користувачів. Під захистом інформації розуміється використання спеціальних засобів, методів і заходів з метою запобігання втрати інформації, що знаходиться в ЛОМ (локальній обчислювальній мережі).

Широке поширення і повсюдне застосування обчислювальної техніки дуже різко підвищили вразливість накопичуваної, зберігаємої та оброблюваної в ЛОМ інформації.

Чітко позначилися три аспекти вразливості інформації:

1. Схильність фізичного видалення чи спотворення.
2. Можливість несанкціонованої (випадкової чи зловмисної) модифікації.
3. Небезпека несанкціонованого отримання інформації особами, для яких вона не призначена.

Основна частина

Для надійно криптографічного захисту інформації в ЛОМ, в тому числі використовується комплекс користувача ЦСК "ІІТ Користувач ЦСК-1".

Комплекс у складі системи електронного документообігу чи іншої прикладної системи (далі - системи) призначений для:

1) автентифікації користувачів системи при підключенні до сервера та забезпечення конфіденційності і цілісності даних, які передаються між користувачами та сервером;

2) забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, з використанням електронного цифрового підпису.

Зазначені функції комплекс (рис. 1,2) виконує шляхом застосування механізмів криптографічного захисту інформації, яка обробляється у системі.

Автентифікація користувачів системи на сервері здійснюється під час підключення користувачів до сервера (встановлення з'єднання з сервером) шляхом реалізації протоколу взаємної автентифікації сторін. Забезпечення конфіденційності та цілісності інформації, яка передається між користувачем та сервером системи під час їх взаємодії, реалізується шляхом шифрування інформації та формування і перевіряння криптографічних контрольних сум.

Забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, реалізуються шляхом формування та перевіряння електронного цифрового підпису від даних та документів, як на стороні користувача системи, так і на стороні сервера.

Комплекс включає до свого складу програмні засоби КЗІ (видів "Б", підвид "Б2", та "В", категорії "К", "П" та "Ш", класу Б2), та апаратно-програмні засоби КЗІ (виду "Б", підвид "Б2", категорії "П" та "Ш", класу Б2).

Програмні засоби КЗІ реалізують логіку роботи комплексу та інтегровані безпосередньо у користувальницьку та серверну частини системи (користувача та сервер), через визначені інтерфейси.

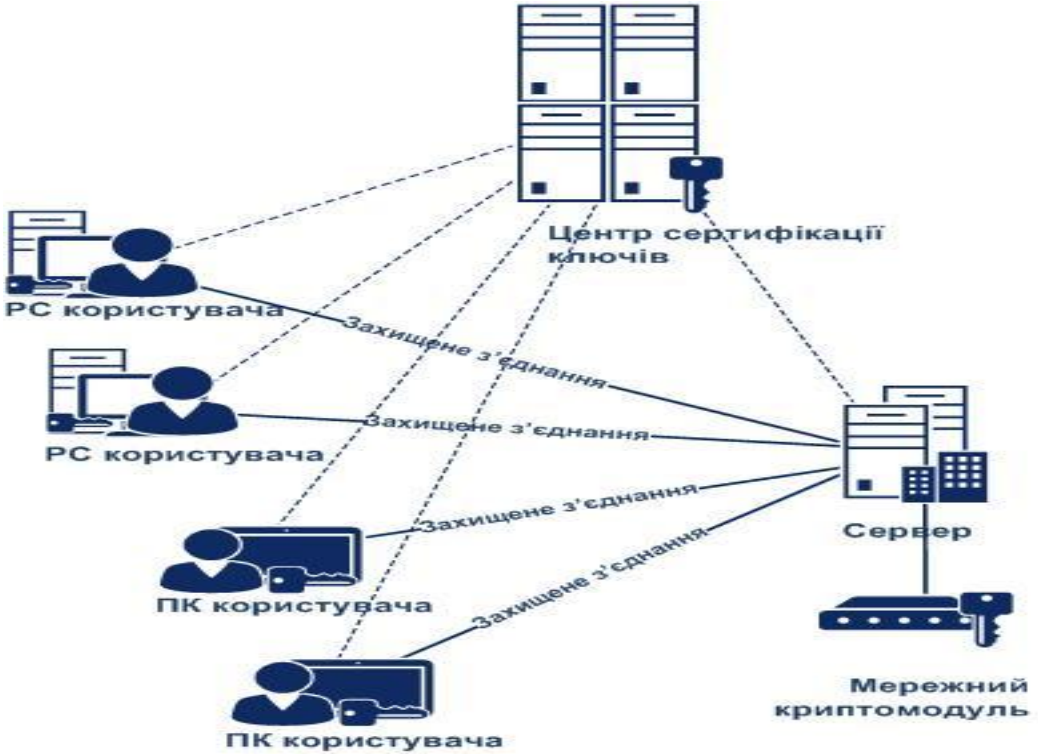

Рис. 1. Структурна схема комплексу захисту

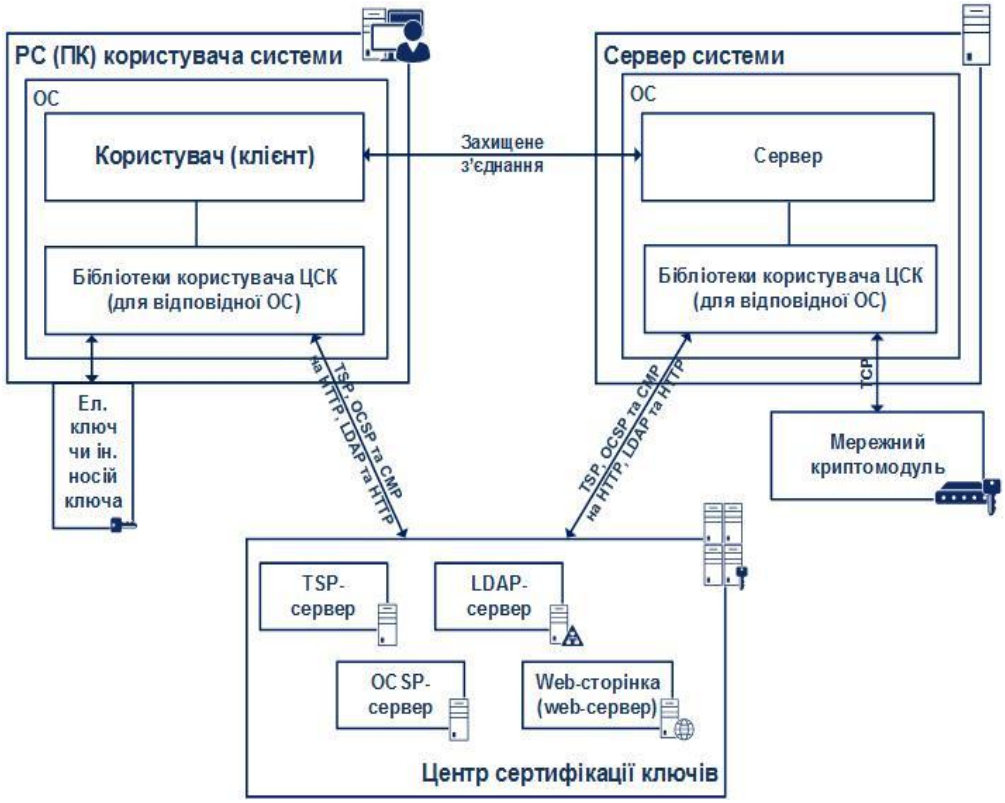

Рис. 2. Функціональна схема комплексу у складі системи

Програмні засоби КЗІ комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережеві криптомодулі тощо.

До складу апаратних засобів комплексу можуть входити:

1) електронний ключ "Кристал-1" ("ІІТ Е. ключ Кристал-1");

2) мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301").

Бібліотеки користувача центру сертифікації ключів (ЦСК) призначені для використання в якості базових засобів КЗІ та виконують наступні функції у їх складі:

1. Роботу з носіями ключової інформації (зчитування особистих ключів з носіїв).

2. Роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС), що включає:

2.1. зчитування сертифікатів та списків відкликаних сертифікатів із файлового сховища;

2.2. визначення статусу сертифіката за допомогою списків відкликаних сертифікатів;

2.3. завантаження списків відкликаних сертифікатів з веб-сторінки ЦСК (з веб-серверу ЦСК);

3. Шифрування та дешифрування даних.

4. Формування та перевірку ЕЦП від даних.

5. Захист сеансів передачі даних (захист з'єднань), що включає:

5.1. реалізацію протоколу взаємної автентифікації сторін під час встановлення сеансу захищеної передачі даних (захищеного з'єднання);

5.2. захист (шифрування та контроль цілісності) сегментів захищеної передачі даних (даних захищеного з'єднання);

6. Інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК);

7. Пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК);

8. Отримання позначок часу у ЦСК (через TSP-сервер ЦСК) тощо.

Бібліотеки користувача ЦСК інтегруються у зазначену систему (та інші прикладні системи) через визначені інтерфейси (Microsoft CAPI, PKCS#11, GSS-API, JCA) і власні та реалізовані для ОС Microsoft Windows XP/2003 Server/Vista/2008 Server/7/8/8.1/2012 Server/10, Microsoft Windows CE/Mobile 5/6/6.5, Microsoft Windows Phone 7/8, Linux (SuSe/Red Hat/Slackware та ін.), UNIX (AIX/Solaris/FreeBSD та ін.), Apple MAC OS X/iOS, Google Android у вигляді бібліотек підключення (DLL/COM, SO, DYLIB – 32/64-біта) чи у вигляді архівів java-класів для JRE чи java-скриптів тощо. Для всіх бібліотек користувача ЦСК під всі ОС та платформи, що підтримуються, існують приклади використання.

Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі засобів користувача системи.

Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі сервера системи.

У засобах комплексу використовуються такі криптографічні алгоритми та протоколи:

1) алгоритми шифрування за ДСТУ ГОСТ 28147:2009 та TDEA і AES за ISO/IEC 18033-3:2010;

2) алгоритми ЕЦП за ДСТУ 4145-2002 та RSA за PKCS#1 (IETF RFC 3447);

3) алгоритми гешування за ГОСТ 34.311-95 та SHA (SHA-1 і SHA-224/256/384/512) за ДСТУ ISO/IEC 10118-3:2005;

4) протоколи розподілу ключів за ДСТУ ISO/IEC 15946-3 (пп. 8.2) та RSA за PKCS#1 (IETF RFC 3447).

Протоколи розподілу ключових даних реалізуються згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) і вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України № 739 від 18.12.2012 р., та за алгоритмом направленого шифрування RSA згідно PKCS#1 (IETF RFC 3447). Генерація ключових даних

здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України.

Протокол встановлення захищеного сеансу передачі даних реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно ДСТУ ISO/IEC 9798-3 (п. 5.2.1) та включає:

1. Формування користувачем та передачу даних автентифікації (запиту) на сервер, при цьому користувач виконує наступні дії:

1.1. генерує випадкове число;

1.2. підписує випадкове число та власний сертифікат (за необхідності) власним особистим ключем ЕЦП;

1.3. передає сформовані дані автентифікації (запит) на сервер;

2. Обробку запиту від користувача сервером, при цьому сервер виконує наступні дії:

2.1. отримує дані автентифікації від користувача;

2.2. здійснює пошук (за відсутності сертифіката у запиті) та перевірку чинності сертифіката користувача;

2.3. перевіряє ЕЦП на даних;

2.4. у разі успішної обробки отриманих даних автентифікації – генерує сеансові ключі шифрування та вектори початкової ініціалізації;

2.5. підписує отримане випадкове число та сеансові ключі з векторами початкової ініціалізації власним особистим ключем ЕЦП;

2.6. зашифровує сформовані дані разом з ЕЦП спрямовано на користувача;

2.7. передає підписані та зашифровані дані автентифікації (відповідь) користувачу;

3. Приймання та обробку відповіді користувача від сервера, при цьому користувач виконує наступні дії:

3.1. отримує відправлені дані автентифікації (відповідь) від сервера;

3.2. здійснює пошук та перевірку чинності сертифіката сервера;

3.3. розшифровує дані автентифікації;

3.4. перевіряє ЕЦП на даних;

3.5. перевіряє відповідність випадкового числа у отриманих даних;

3.6. у разі успішної обробки отриманих даних автентифікації (відповіді) завершує роботу протоколу.

Шифрування даних у захищеному з'єднанні здійснюється за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 або TDEA чи AES. В якості криптографічної контрольної суми для контролю цілісності даних у захищеному з'єднанні використовуються коди автентифікації повідомлень (імітовставки), які обчислюються за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 або TDEA чи AES.

Шифрування даних та обчислення кодів автентифікації повідомлень (імітовставок) у захищеному з'єднанні здійснюється на основі сеансових ключів та векторів початкової ініціалізації (синхромаркерів), які розподіляються між користувачем та сервером у результаті виконання протоколу взаємної автентифікації.

Мережевий криптомодуль "Гряда-301" призначений для апаратної реалізації криптографічних перетворень у складі сервера системи.

Пристрій виконує наступні функції:

1) автентифікацію сервера при доступі до модуля;

2) генерацію особистих та відкритих ключів для алгоритму ЕЦП та протоколу розподілу ключів;

3) генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора;

4) зберігання особистих ключів у внутрішній пам'яті та захист їх від НСД;

5) формування ЕЦП;

6) розподіл ключових даних на основі асиметричного протоколу розподілу та шифрування даних;

7) контроль цілісності і працездатності вбудованого програмного забезпечення та ін.

Піводячи підсумок проведенного досліждення, можна сказати, що існуючих методів криптографічного захисту інформації достатньо для захисту ЛОМ

Приведені результати можуть бути використані при проектуванні та розробці ЛОМ з метою підвищення захищеності криптографічними засобами.

Список літератури:

1. Ахрамович В.М. Програми захисту інформації приховуванням її та шифруванням. Науковий Вісник Державної академії статистики, обліку та аудиту 2008, №4.-с.100-109.
2. Ахрамович В.М., Чегренець В.М.. Інформаційна безпека. Практикум/ В.М. Ахрамович, В.М. Чегренець.-К.: ДУТ, 2017.-396с.
3. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV,2009. – 608 с., іл.
4. Конахович Г.Ф., Корченко О.Г., Юдін О.К., Захист інформації в мережах передачі даних: Підручник. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714с., іл.
5. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії : навч. посібн. / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.
6. https://iit.com.ua/services.