ЛИТВИНОВ В. В., д-р техн. наук, проф.
ХОМЕНКО А. В.
ДМИТРАШ О. В.

СПЕЦІАЛЬНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

У даній праці представлені основні риси спеціального програмного забезпечення (СПЗ) локальної обчислювальної мережі (ЛОМ), призначеного для запобігання несанкціонованому доступу користувачів ЛОМ до захищених ресурсів робочих станцій (РС), серверів загального призначення (СЗП) та серверів керування захистом (СКЗ), а саме: захищених дисків РС, СЗП та СКЗ, реєстру ОС РС, СЗП та СКЗ, процесів, що виконуються на РС, СЗП, СКЗ.

In the given work there are the presented basic lines of the special local area network (CROW—BAR)software (SPZ), intended for prevention of unauthorized division of users CROW-BAR to the protected resources of the work stations (WS), servers of the common setting (SCS)and servers of management by defence (SMD), namely: copyprotected disks CD, SPZ and SMD, register of OS WS, SZP and SCZ, processes, that are executed on WS, SPZ, SMD.

Постановка проблеми

У сучасному суспільстві існує необхідність контролювати доступ до інформації.

Зараз конфіденційність інформації дуже важлива і її втрата може призвести до великих збитків. Прикладом є проблема передачі інформації в комп'ютерній мережі з забезпеченням секретності.

Аналіз досліджень і публікацій

Проблема передачі інформації з застосуванням шифрування розглядалася багатьма вченими, такими як А. Соломаа, Д. Р. Стінсон, Б. Шнайдер. Також існують кілька рішень даної проблеми. У статтях МОДС 2007 запропоновано альтернативне розв'язання проблеми (застосування пристрою захисту мережі [1; 2]). Було сформовано основні принципи його функціонування.

У даній статті запропоновано варіант ПЗ до пристрою захисту мережі.

Формулювання цілей статті

Мета дослідження — забезпечити стійке керування даними та їх захист при передачі по мережі у вигляді голосових та текстових повідомлень. Основний метод досягнення цієї мети — використання надійного керівного алгоритму в реальному часі та передачі даних.

Виклад основного матеріалу

Пристрій захисту мережі (ПЗМ) забезпечує виконання таких функцій:

— ідентифікація користувачів на основі Е-електронного ключа користувача;

— дозвіл або заборона доступу в захищену ЛОМ;

— встановлення захищений зв'язок типу «крапка-крапка» іншими ПЗМ;

— зміна ключів на приймання і передачу через кожні 106 пакетів каналу Ethernet, тобто після передачі кожних 12 640 000 000 зашифрованих бітів у напрямі приймання або передачі, але не рідше ніж один раз на годину;

— прочитування з ЕКК частину ключової інформації користувача і права користувача на доступні для нього ресурси, як локальні, так і серверні, захищеної локальної мережі і передача їх системі забезпечення захисту рабочої станції, а також перевка їх на сервері управління захистом ЛОМ СКЗ);

— керування і передача в журнал, що ведеться на СКЗ, інформації про початок і закінчення роботи користувача, про встановлення / завершення захищеного зв'язку з іншими ПЗМ, про заміну ключів напрямів приймання — передачі для шифрування згідно з алгоритмом ГОСТ 28147-89, про невдалі спроби встановлення захищеного зв'язку ПЗМ, з одного боку, підключається до мережної карти обчислювальної машини, а з іншого — до Ethernet-каналом, утворюючи тим самим буферний пристрій між ПЕОМ і Ethernet-каналом. Узагальнена схема захищуваної ЛОМ наведена на рис. 1.

РС — робоча станція являє собою робоче місце одного або кількох користувачів. Тільки один користувач може отримати доступ до ресурсів РС в даний конкретний момент часу. На РС можуть бути присутні захищені ресурси. Різні користувачі можуть мати різні права щодо користування захищеними ресурсами РС або ЛОМ.

СЗП — сервер загального призначення, на якому зберігаються захищені ресурси, до яких можуть мати доступ користувачі РС через ЛОМ. Різні користувачі можуть мати різні права щодо користування захищеними ресурсами СЗП.

СКЗ — сервер керування захистом, на якому працює СПЗ, що стежить за безпекою захищуваної ЛОМ.

СКЗ має два мережеві інтерфейси:

— через ПЗМ приєднаний до захищуваної ЛОМ;

— приєднаний до СУБД.

Між цими двома інтерфейсами існує адміністративна заборона на трансляцію пакетів.

Тільки один користувач (адміністратор СКЗ) може отримати доступ до СКЗ задля виконання в даний конкретний момент часу.

СУБД — сервер на якому зберігається інформація:

— про структуру ЛОМ;

— про користувачів ЛОМ;

— про права користувачів щодо тих чи інших ресурсів, розміщених на РС та СЗП;

— про фільтри та задачі, що мають виконуватися на СПЗ комп'ютерів захищуваної ЛОМ.

СУБД — фізично від'єднана від захищуваної ЛОМ завдяки окремому інтерфейсу до СКЗ та адміністративній забороні трансляції пакетів між двома мережевими інтерфейсами, що має СКЗ.

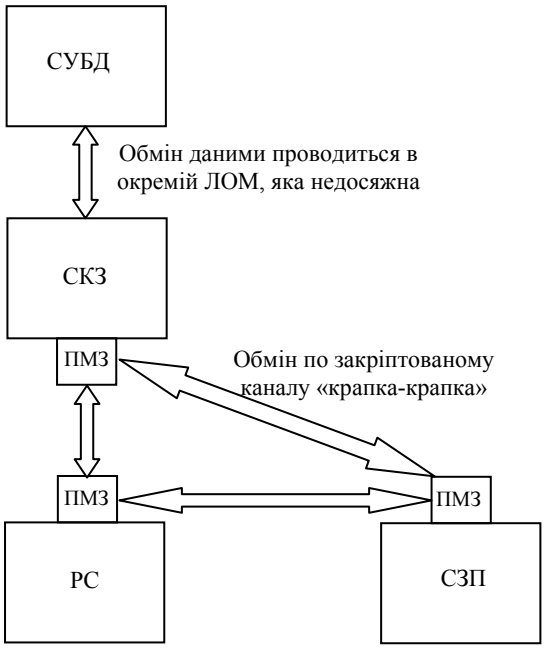

Рис. 1. Узагальнена схема захищуваної ЛОМ

РС, СЗП, СКЗ приєднані до ЛОМ через пристрій захисту мережі (ПЗМ), інших шляхів взаємодії між ними та ЛОМ не існує.

СПЗ РС, СЗП і СКЗ у своїй основі мають спільну організацію та структуру. В основі кожного з трьох комплектів ПЗ лежить ядро, яке забезпечує цілісність системи та виконання її задач. Також для кожного з комплектів ПЗ створена множина модулів, які реєструються в ядрі та призначені для виконання тих чи інших задач. Структурна схема СПЗ СКЗ наведена на рис. 2.

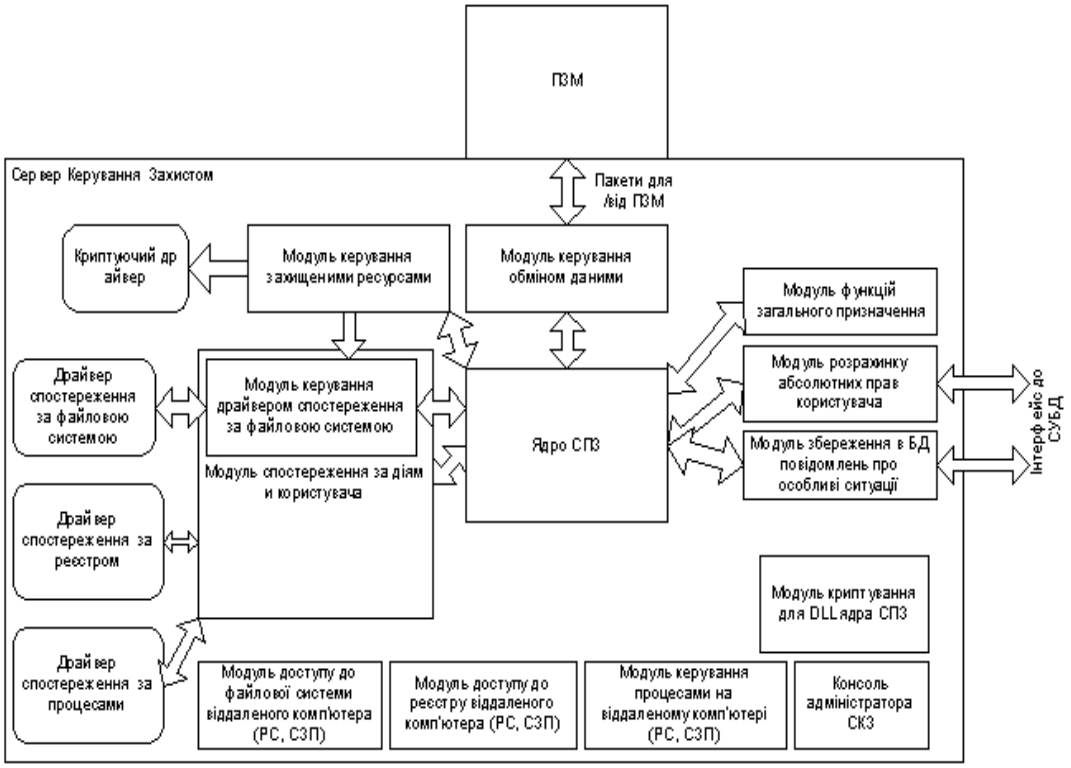

Рис. 2. Структурна схема СПЗ СКЗ

Структура СПЗ РС та СЗП відрізняється від наведеної скороченим переліком моделей та введеними новими модулями, такими як модуль блокування USB, модуль надання доступу до локальної файлової системи та ін.

Висновки

У статті запропонований варіант СПЗ для ПЗМ, який, на думку розробника, є оптимальним на сьогодні. Проте з огляду на тенденції розвитку комп'ютерних технологій, незабаром необхідно буде вносити деякі зміни до проекту.

ЛІТЕРАТУРА

1. *Литвинов В. В., Дмитраш. А. В.*, *Хоменко А. В*. Імітаційна модель розпаралелювання обробки між процесорами в пристрої захисту локальної мережі : Тези допов. на Другий наук.-практ. конф. з міжнар. участю «Математичне та імітаційне моделювання систем. МОДС'2007», м. Київ. 25—29 черв. 2007. — С. 161—164.
2. *Литвинов В. В., Дмитраш. А. В.*, *Хоменко А. В*. Функціональна структура пристроя захисту локальної обчислювальної мережі : Тези допов. на Другий наук.-практ. конф. з міжнар. участю «Математичне та імітаційне моделювання систем. МОДС'2007», м. Київ. 25—29 черв. 2007. — С. 206—210.
3. *Казимир В. В, Гавсиевич И. Б., Чупрынин А. Д., Полікарпов А. И.* Моделирование процессов распространения информации в IP сетях : Тези допов. на Другий наук.-практ. конф. з міжнар. участю «Математичне та імітаційне моделювання систем. МОДС'2007», м. Київ. 25—29 черв. 2007. — С. 200—202.
4. *Литвинов В.В., Казимир В.В.* Модельно-ориентированное управление как стратегия функционирования интеллектуальных производственных систем // Математичні машини і системи. — 2004. — № 4. — С. 143—156.
5. *Шнайдер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М. : ТРИУМФ, 2002. — 815 с.