УДК 004.032

А.Р. Дячишин, Г.В. Шимчук
Тернопільський національний технічний університет імені Івана Пулюя, Україна

УРАЗЛИВІСТЬ ОСНОВНИХ СТРУКТУРНИХ ЕЛЕМЕНТІВ РОЗПОДІЛЕНИХ КС

A.R. Dyachyshyn, G.V. Shymchuk

VULNERABILITIES BASIC STRUCTURAL ELEMENTS DISTRIBUTED COP

У загальному випадку розподілена КС складаються з наступних основних структурно-функціональних елементів:

– робочих станцій – окремих ЕОМ або відділених терміналів мережі, на яких реалізуються автоматизовані робочі місця користувачів (абонентів, операторів);

– серверів або Host машин (служб файлів, друку, баз даних і тому подібне) не виділених (або виділених, тобто не суміщених із робочими станціями) високопродуктивних ЕОМ, призначених для реалізації функцій зберігання, друку даних, обслуговування робочих станцій мережі й тому подібне;

– міжмережевих мостів (шлюзів, центрів комутації пакетів, комунікаційних ЕОМ) – елементів, що забезпечують з'єднання декількох мереж передачі даних, або декількох сегментів однієї й тієї ж мережі, що мають різні протоколи взаємодії;

– каналів зв'язку (локальних, телефонних, із вузлами комутації і так далі).

Робочі станції є найбільш доступними компонентами мереж і за допомогою них можуть бути зроблені найбільш численні спроби здійснення несанкціонованих дій. З робочих станцій здійснюється управління процесами обробки інформації, запуск програм, введення і коректування даних, на дисках робочих станцій можуть розміщуватися важливі дані і програми обробки. На відео монітори і друкуючі пристрої робочих станцій виводиться інформація при роботі користувачів (операторів), що виконують різні функції та мають різні повноваження по доступу до даних і інших ресурсів системи. Саме тому робочі станції мають бути надійно захищені від доступу сторонніх осіб і містити засоби розмежування доступу до ресурсів з боку законних користувачів, що мають різні повноваження. Крім того, засоби захисту повинні запобігати порушенням нормального налаштування робочих станцій і режимів їх функціонування, викликані ненавмисним втручанням недосвідчених (неуважних) користувачів.

Особливого захисту потребують такі привабливі для зловмисників елементи мереж як сервери (Host-машини) і мости. Перші – як концентратори великої кількості інформації, другі – як елементи, в яких здійснюється перетворення даних при узгодженні протоколів обміну в різних ділянках мережі.

Сприятливою обставиною для підвищення безпеки серверів і мостів є, як правило, наявність можливостей по їх надійному захисту фізичними засобами і організаційними заходами, що дозволяє скоротити до мінімуму число осіб з персоналу мережі, що мають безпосередній доступ до них. Іншими словами, безпосередні випадкові дії персоналу і навмисні дії зловмисників на виділені сервери і мости можна вважати малоймовірними. В той же час, треба чекати масованої атаки на сервери і мости з використанням засобів віддаленого доступу. Тут зловмисники перш за все можуть шукати можливості вплинути на роботу різних підсистем серверів і мостів,

використовуючи недоліки протоколів обміну і засобів розмежування віддаленого доступу до ресурсів і системних таблиць.

Використовуватися можуть всі можливості й засоби, від стандартних (без модифікації компонентів) до підключення спеціальних апаратних засобів, канали, як правило, слабо захищені від підключення і застосування висококласних програм для подолання системи захисту.

Звичайно, сказане вище не означає, що не буде спроб впровадження апаратних і програмних закладок в самі мости і сервери, що відкривають додаткові широкі можливості по несанкціонованому віддаленому доступу. Закладки можуть бути упроваджені як з віддалених станцій (за допомогою вірусів або іншим способом), так і безпосередньо в апаратуру й програми серверів при їх ремонті, обслуговуванні, модернізації, переході на нові версії програмного забезпечення, зміні устаткування.

– Канали і засоби зв'язку також потребують захисту. Через велику просторову протяжність ліній зв'язку (через неконтрольовану або слабо контрольовану територію) практично завжди існує можливість підключення до них, або втручання в процес передачі даних. Можливі при цьому загрози детально викладені нижче.

Література

1.Антонюк А. О. Основи захисту інформації в автоматизованих системах / А. О. Антонюк. Національний ун-т «Києво-Могилянська академія». – К.: КМ Академія, 2003. – Бібліогр.: с. 242-243.

2.Бабак В.П. Теоретичні основи захисту інформації. Підручник / В.П. Бабак. – НАУ, 2008. – 752 с.

3.Бевз О.М. Шифрування даних на основі високонелінійних булевих функцій та кодів з максимальною відстанню / О.М. Бевз, Р.Н. Квєтний. – Вінниця: ВНТУ, 2010.

4.Бобунов А.І. Захист інформації в автоматизованих системах / А.І. Бобунов, В.І. Шестаков. – Житомир: ЖВІРЕ, 2004. – С. 16 - 43

5.Гмурман, А.И. Информационная безопасность/ А.И. Гмурман – М.: «БИТ-М», 2004. –387с.