УДК 681.322

© 2000 р. М.М. Колесніков

Чернівецький національний університет ім. Ю.Федьковича, Чернівці

МЕТОД ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ НА БАЗІ СЕГМЕНТОВАНИХ ЛОКАЛЬНИХ МЕРЕЖ ЕОМ СПЕЦИФІКАЦІЇ 10*BASE-T*

Запропоновано метод технічного захисту інформації в сегментованих локальних мережах ЕОМ специфікації 10*BASE-T* на фізичному рівні еталонної моделі *ISO*/*OSI* із застосуванням нелінійного концентратора, структуру та модель функціонування нелінійного концентратора з керованою нелінійністю портів. Обгрунтовано переваги застосування даного методу у мережевих автоматизованих інформаційних системах у порівнянні з раніше відомими.

The method of the information security in the segmented local computer networks of the specification 10*BASE-T* at a physical level of a standard model *ISO*/*OSI* with application of the nonlinear concentrator as well as the structure and model of operation of the nonlinear concentrator with controlled nonlinearity of ports are offered. The advantages of application of a method in the network automized information systems in comparison with earlier known are justified.

При використанні автоматизованих систем (АС) у процесі інформаційної діяльності, наприклад закладів освіти, обробляється та транспортується інформація з обмеженим доступом, яка підлягає захисту від впливу руйнуючих інформаційних процесів на її конфіденційність, цілісність, доступність та спостережність.

Варто відзначити, що поняття "обмежений доступ" у широкому розумінні означає вимогу до всіх учасників інформаційної діяльності, зокрема власників АС та інформації, розпорядників, персонал, користувачів АС в процесі обробки та транспортування інформації, що здійснюються в АС від їх імені, обов'язкового дотримання прийнятих у встановленому порядку правил (регламенту) доступу до інформації в АС. Наприклад, програмне забезпечення (ПЗ) комп'ютерної системи, яке у встановленому порядку введене в експлуатацію, є інформацією з обмеженим доступом, оскільки існують правила роботи з ПЗ, визначені в експлуатаційній документації.

В умовах сучасного освітянського закладу, де інформатизація навчального процесу відбувається через впровадження технологій дистанційної освіти (ДО) [6], значну частину інформації з обмеженим доступом складають цифрові інформаційні ресурси (ЦІР), що обробляються і транспортуються комп'ютерними мережами.

З урахуванням поширення нових моделей загроз [2,5], до функціональних профілів захищеності АС класів 2 і 3 висуваються додаткові вимоги по забезпеченню цілісності та доступності оброблюваної інформації, включаючи ЦІР.

Більшість АС класів 2 в закладах освіти побудовано на базі мереж ЕОМ локальних специфікації 10*BASE-T* стандарту *IEEE*-802.3*i*.

Типова конфігурація мереж рівня робочих груп – сегментований концентраторами домен колізій зі середовищем передачі, що поділяється за методом *CSMA*/*CD* та з використанням напівдуплексного режиму обміну [3].

На рис.1 показано АС на базі трисегментної локальної мережі *Ethernet* з кореневим концентратором *H*1 (повторювачем), який, разом зі сервером, підключеним до сегменту *C*, розміщений в ізольованому приміщенні. Через сервер може здійснюватися, зокрема, вихід робочих груп сегментів *A* та *B* у метамережу Інтернет з використанням, наприклад, методу трансляції мережевих адрес або проксі-серверу.

Слід зауважити, що використання для сегментації мережі саме некерованих концентраторів у випадку, що розглядається, є економічно обгрунтованим технічним рішенням. Застосувати найдешевше активне мережеве обладнання стає можливим, оскільки відоме правило "80/20" [3] у даному випадку не виконується, отже, ізоляція

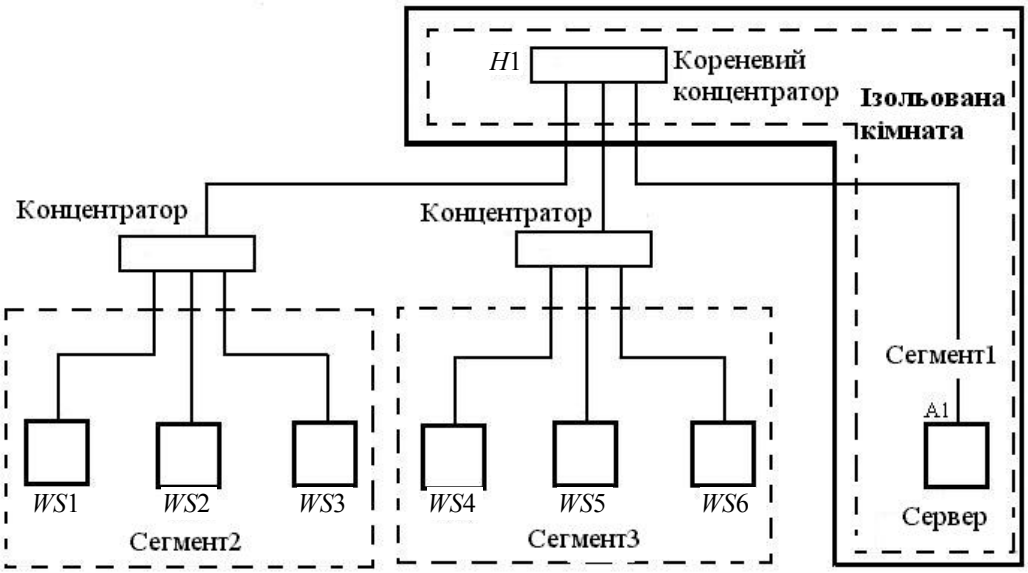

Рис.1. АС на базі мережі ЕОМ локальної специфікації 10*BASE-T* із застосуванням мережевого обладнання фізичного рівня моделі *OSI*.

внутрісегментного трафіку з метою збільшення ефективності роботи мережі застосуванням мостів або комутаторів і пов'язані з цим додаткові витрати недоцільні. Активне обладнання мережі функціонує за стандартом *IEEE*-802.3*i* на фізичному рівні еталонної моделі *ISO*/*OSI*, надаючи можливість необмеженого доступу до ЦІР у сегментах *A*, *B*, *C*.

Для технічного захисту інформації, яка обробляється на робочих станціях робочих груп сегментів *A* та *B* однорангової (за принципом управління) мережі, може виникнути завдання обмеження (наприклад, блокування) доступу з сегменту *A* у сегмент *B* і навпаки так, щоб доступ із сегментів *A* і *B* до серверу в сегменті *C* залишався можливим.

Якщо політикою безпеки дозволено використання лише протокольного стека *TCP*/*IP*, то можна передбачити існування моделі загроз, згідно з якою порушник у сегменті *A*, діючи за змовою з порушником у сегменті *B*, отримує можливість нелегально встановити на робочих станціях, наприклад, немаршрутизований протокол *NetBEUI* [3] з подальшими атаками ресурсів сегмента *A* з сегмента *B* і навпаки.

Відомим методом рішення поставленої вище задачі є блокування доступу шляхом селекції кадрів з визначеними фізичними (MAC) адресами відправника та отримувача кадру на канальному рівні моделі *ISO*/*OSI*. Засобом реалізації методу є заміна активного обладнання першого, фізичного рівня моделі *ISO*/*OSI* (кореневого концентратора *H*1) на обладнання другого, канального рівня моделі *ISO*/*OSI* (керований мультипортовий міст або комутатор).

Недоліками методу блокування доступу селекцією протокольних блоків канального рівня можна вважати збільшення вартості активного мережевого обладнання, додаткові затримки трансляції кадрів, пов'язані з обробкою адресних полів. Майже аналогічні недоліки властиві методу блокування міжсегментного доступу маршрутизацією трафіка на мережевому рівні моделі *ISO*/*OSI* шляхом заміни кореневого концентратора *H*1 на маршрутизатор, який є активним обладнанням третього (мережевого) рівня моделі *ISO*/*OSI* [3].

Можливим рішенням задачі є застосування локальних програмних засобів захисту (ЛПЗЗ) шляхом введення програмної надлишковості безпосередньо у склад ПЗ робочих станцій сегментів однорангової мережі без змін у складі активного обладнання. Застосування ЛЛПЗ, наприклад *Firebox SOHO* фірми *Watch Guard*, замість захисту ЦІР сегментів робочих груп апаратними засобами міжмережевого екранування знижує вартість захисту в декілька разів [4]. Серед ЛПЗЗ найчастіше застосовуються сервери-посередники (*proxy*), міжмережеві екрани, наприклад *Lock Down* 2000 (*IP-firewall*) з відповідним налагодженням вирішуючих правил приймання і передавання пакетів через інтерфейси з *IP*-адресами робочих станцій із захищеними ЦІР.

Зазначені ЛПЗЗ забезпечують гнучке керування

доступом і функціонують на різних рівнях моделі ISO/OSI, розташованих вище фізичного рівня. Проте самі ЛПЗЗ являють собою інформацію з обмеженим доступом, яка підлягає захисту. Застосування ЛПЗЗ вимагає експлуатаційних витрат на розподілене адміністрування. При комплексуванні з операційними системами закордонного виробництва ЛПЗЗ утворюють підсистему захисту з низькою операційною та технологічною гарантованістю, що пов'язано з необхідністю проведення досліджень на відсутність недокументованих функцій і відповідними додатковими витратами.

Альтернативний метод технічного захисту – блокування міжсегментного доступу введенням та використанням статичної нелінійності портів концентратора 10*BASE-T* на фізичному рівні моделі *OSI*. Під статичною нелінійністю портів концентратору в подальшому будемо розуміти селективну трансляцію портами трафіка, яка дозволяється або забороняється в залежності від процесів, що породжують трафік. Наприклад, для частини трафіка, яка несе інформацію про наявність колізії (процес фізичного рівня), статично нелінійний порт концентратора прозорий, у той час як для іншої частини трафіка, яка є забороненим міжсегментним потоком даних, порт залишається непрозорим.

Пропонований у цій роботі метод і його реалізація дозволяють здійснювати технічний захист інформації шляхом постійного у часі блокування трансляції даних на фізичному рівні еталонної моделі *ISO*/*OSI* між визначеними портами концентратора при збереженні трансляції сигналу колізії та можливості функціонування мережі за протоколом *CSMA*/*CD* у відповідності з *IEEE*-802.3*i*.

Згідно із введеним означенням, у залежності від наявності чи відсутності властивості нелінійності портів, концентратор 10*BASE-T* називається нелінійним або лінійним. Якщо вважати спрощеною моделлю лінійного концентратора 10*BASE-T* орієнтований повнозв'язний мультиграф, вершини якого моделюють порти, а дуги – шляхи трансляції даних і сигналів колізії між портами, тоді модель статичного нелінійного концентратора може бути задана системою з двох графів. Перший граф, що моделює можливі шляхи трансляції сигналу колізії, збігається з графом лінійного концентратора. Другий граф, який моделює шляхи трансляції даних, утворюється з першого шляхом зменшення степеня довільної вершини графа із видаленням відповідної дуги.

На рис.2 показано структуру і відповідну графову модель лінійного трипортового концентратора специфікації 10*BASE-T*, аналіз якої використано для з'ясування можливості надання портам концентратора властивості статичної нелінійності. У структурі лінійного концентратора показано транслюючі формувачі *RD*1…*RD*3 і *TD*1…*TD*3, формувач *CD* сигналу *CP* "Наявність колізії". Активний стан виходу *CD* (сигнал *CP*) виникає за умови одночасної передачі даних з двох і більше формувачів *TDi* (*i*=1,2,3) на входах формувача *CD*.

Функцію стану виходу формувача *CD* – булеву функцію станів виходів транслюючих формувачів, з'єднаних з входами *CD*, – для трипортового лінійного концентратора можна записати у вигляді

$$CP = TD1 \bigcap TD2 \bigcup TD2 \bigcap TD3 \bigcup TD1 \bigcap TD3,$$

де *CP* – булева змінна, яка моделює сигнал наявності чи відсутності колізії; *TDi* – булеві змінні, що моделюють наявність чи відсутність передавання даних відповідним транслюючим формувачам.

Особливістю структури концентратора специфікації 10*BASE-T* є формування сигналу колізії у формувачі *CD* так, що стає непотрібним спотворення сигналів на виходах формувачів *RDi* і, відповідно, на портах концентратора як умови формування *jam*-послідовності колізійного домену мережі. Звідси випливає можливість розділення ланцюгів передачі вхідних сигналів формувача *CD* і відповідних паралельних ланцюгів передачі однойменних сигналів на входи формувачів *RDi* портів концентратора специфікації 10*BASE-T*.

На рис.3 показано структуру і відповідну графову модель нелінійного концентратора, отриманого зі структури лінійного концентратора 10*BASE-T* шляхом розірвання ланцюгів трансляції даних між виходом формувача *TD*1 та входом формувача *RD*2, виходом *TD*2 та входом *RD*1. На рис.3 місця розриву ланцюгів умовно позначені символом *X*. Зміни в структурі лінійного концентратора блокують трансляцію даних з виходів формувачів *TD*1, *TD*2 на входи формувачів *RD*2, *RD*1 портів кореневого концентратора. Схема формування і трансляція сигналу *jam* для всіх без винятку портів концентратора залишаються без змін.

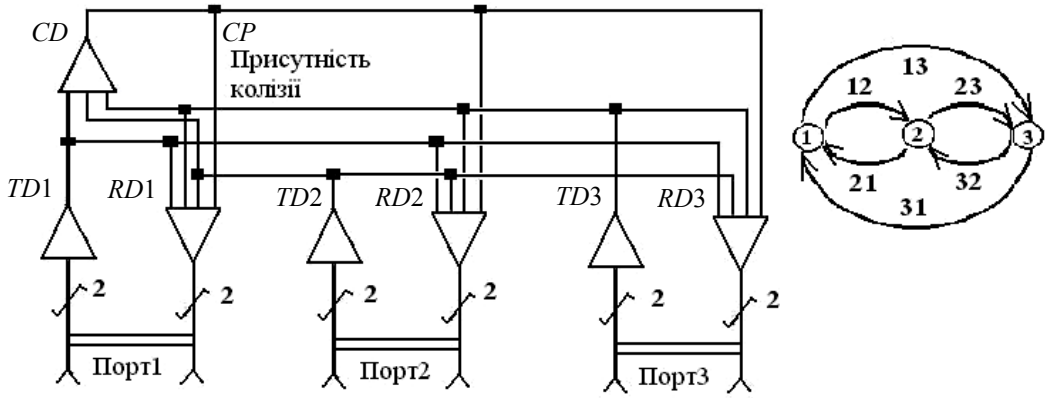

Рис.2. Структура і графова модель лінійного концентратора специфікації 10*BASE-T*

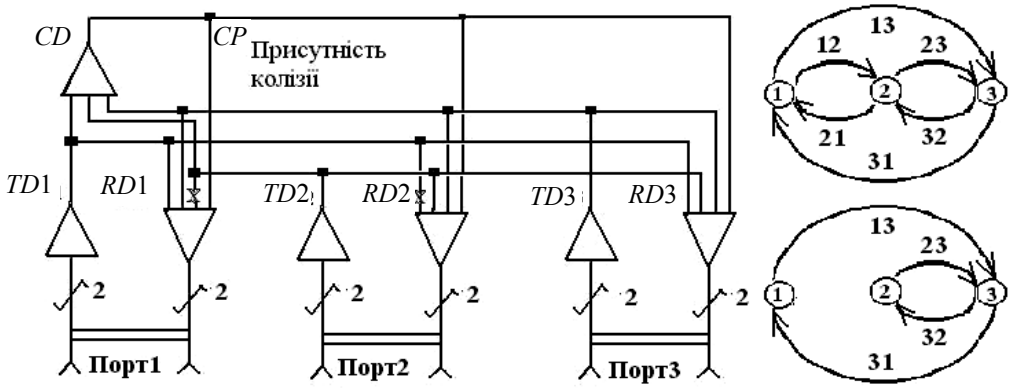

Рис.3. Структура і графова модель тривходового нелінійного концентратора специфікації 10*BASE-T*

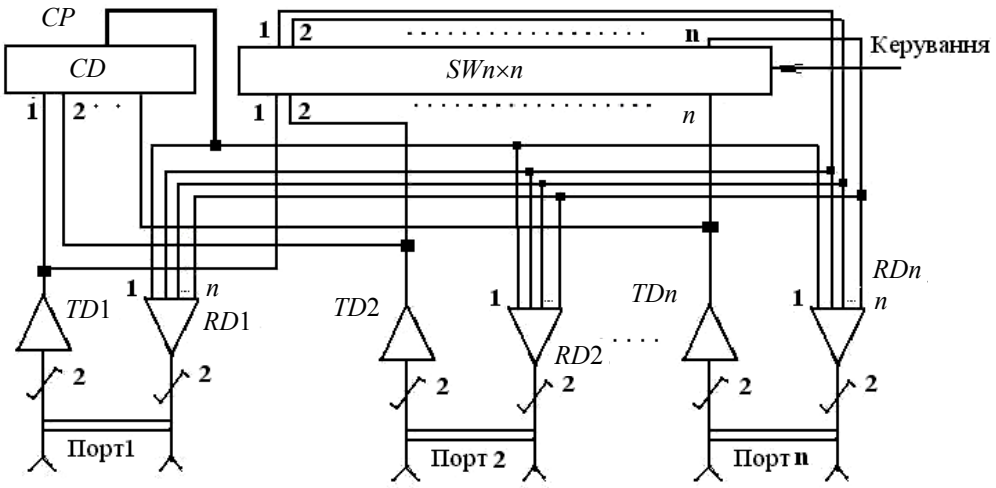

Рис.4. Структура n-портового нелінійного концентратора з керованою статистичною нелінійністю портів

Графову модель тривходового нелінійного концентратора зі статичною нелінійністю портів 1 та 2 і лінійним портом 3 зображено на рис.3. У відповідності з наведеним вище, перший граф у моделюючій системі нелінійного тривходового концентратора повністю збігається з моделюючим графом відповідного лінійного концентратора, зображеного на рис.2. Другий граф системи має зменшені на одиницю степені вершин 1 та 2, що відповідає видаленню з першого графа дуг 12 і 21.

Заміна лінійного концентратора *H*1 у мережі (рис.1) нелінійним концентратором дає можливість блокувати на першому (фізичному) рівні еталонної моделі *ISO*/*OSI* доступ до інформації з обмеженим доступом у сегменті *A* з сегмента *B* і навпаки при тому, що доступ із сегментів *A* і *B* у сегмент *C* і навпаки залишається прозорим. Отже, апаратними засобами нелінійного концентратора забезпечується технічний захист інформації від реалізації наведеної вище моделі загроз.

Узагальнену структуру *n*-портового концентратора 10*BASE-T* з керованою статичною нелінійністю портів наведено на рис.4. У структуру лінійного *n*-портового концентратора специфікації 10*BASE-T* додатково введено *n*×*n* комутатор *SW* сигналів *RDi* (*i*=1…*n*), *n* входів якого попарно з'єднано з відповідними виходами формувачів *TDi* кожного із *n* портів концентратора, а *n* виходів комутатора попарно з'єднано з відповідними *n* входами формувачів сигналів *RDi*.

Статичний сигнал "Керування" формує сполучення входів комутатора з потрібними виходами, визначаючи порти концентратора з частковим або повним блокуванням трансляції даних. Зауважимо, що для формування сигналу "Керування" не потрібний аналіз MAC-адреси з подальшою селекцією кадрів, притаманний функціонуванню активного обладнання канального рівня еталонної моделі *ISO*/*OSI* (мости, комутатори). Сигнал "Керування" застосовується для організації перенаправлення або блокування потоку даних між входами та виходами комутатора і відповідними до них портами концентратора. У результаті набір портів концентратора набуває властивостей керованої статичної нелінійності, що дозволяє реалізувати запропонований метод технічного захисту інформації, застосовуючи найдешевше мережеве обладнання фізичного рівня еталонної моделі *ISO*/*OSI* з максимальною швидкістю трансляції даних.

Перевагами запропонованого методу є надійність, простота реалізації, максимальна швидкодія при мінімальних витратах. Метод може застосовуватися в проектуванні АС з мінімальною вартістю активного мережевого обладнання і підсистем захисту інформації з обмеженим доступом, яка обробляється у сегментах однорангової мережі, наприклад, у випадках, коли ЦІР у сегментах належить конкуруючим робочим групам, які колективно використовують ресурси серверу в спільному домені колізій.

Висновки

При вирішенні задач технічного захисту інформації в АС класу 2, 3 на базі однорангової сегментованої локальної мережі ЕОМ специфікації 10*BASE-T* у випадках, коли сегменти з інформацією, яка підлягає захисту, знаходяться у спільному домені колізій, доцільним є використання запропонованого методу технічного захисту інформації блокуванням міжсегментного доступу на фізичному рівні еталонної моделі *ISO*/ *OSI*.

Технічним засобом реалізації методу може бути запропонований у роботі кореневий концентратор специфікації 10*BASE-T*. В його структуру введені зміни, внаслідок яких набір портів концентратора набуває властивісті статичної нелінійності. Це дозволяє прозоро транслювати сигнал колізії між всіма портами концентратора у відповідності з протоколом *CSMA*/*CD* за стандартом *IEEE* 802.3*i*, одночасно блокуючи трансляцію даних між визначеними адміністратором безпеки портами на фізичному рівні еталонної моделі *ISO*/*OSI*.

СПИСОК ЛІТЕРАТУРИ

1. НД ТЗІ 2.5-005–99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціоно-ваного доступу.
2. *Медведовский И.Д., Семьянов П.В., Леонов Д.Г.* Атака на Интернет. - М.: ДМК, 1999.
3. *Олифер В.Г, Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. - СПб: Питер, 1999.
4. *Хлапонин Н.* Защита для малого бизнеса // Компьютерное обозрение. - 2000. - №13. - С.24-26.
5. *Степанов П.Г.* Угрозы безопасности в корпоративных вычислительных системах // Проблемы информационной безопасности. Компьютерные системы. Санкт-Петербургский государственный технический университет. - 1999. - С.32-38.
6. Широкополосные мультисервисные сети – новая платформа телекоммуникационных магистралей и услуг. Аналитический обзор. - Киев: Нора-принт, 1999.