уровнем защищенности ТА и телефонной линии абонентской сети. В состав комплекса входит прибор "Скеля-1", который подключается к абонентским линиям АТС последовательно с оконечным устройством абонента. Количество одновременно контролируемых линий – две. Прибор обеспечивает контроль линий от несанкционированного параллельного подключения любого устройства в режиме "ожидание вызова" с внутренним сопротивлением до 150 кОм и в режиме "разговорный" – не более 5,1 кОм. Прибор имеет функцию контроля линий от обрыва в режиме "ожидание", обеспечивает подачу сигнала шума в обе контролируемые линии с заданным энтропийным коэффициентом качества шума 0,8 и амплитудой не менее 1,5 В в диапазоне частот 0,1-10 кГц, обеспечивает 120 дБ подавления сигналов ВЧ-навязывания в диапазоне частот 0,18-250 кГц. Прибор имеет автоматически включаемое резервное питание и обеспечивает связь с абонентом при отсутствии питания 220 В и выключенном резервном питании (например, при разряде аккумулятора). Прибор работает с концевыми устройствами абонентских линий всех типов (телефоны, факсы, модемы и др.), работающими с аналоговыми сигналами. В комплекс входит отдельный генератор шума "Скеля-2" (с характеристиками, соответствующими генератору шума прибора "Скеля-1"), отдельный прибор для защиты факсов "Скеля-3" (обеспечивает безопасность факса для режима "спикерфон" и исключающий применение кода доступа к факсу), индикатор ВЧ-навязывания "Скеля-4" (определяет наличие опасных сигналов в диапазоне до 50 МГц), определитель емкостной характеристики линии "Скеля-5" и определитель индуктивного несанкционированного подключения к линии "Скеля-6". По мнению авторов разработки – это минимальный набор функций, необходимый для реальной защиты ТА.

*Литература: **1**. В. А. Худяков. "Особенности применения мер технической защиты информации в специальных телекоммуникационных системах". Тез. докл. на "Научно-технической конференции по безопасности информации", г. Киев, КВИУС, 2001. **2**. Перелік засобів забезпечення технічного захисту інформації. Засоби загального призначення. Бизнес и безопасность. № 2, 2001, с. 41.*

УДК 654.1 (045)

ВИКОРИСТАННЯ ПРИНЦИПУ ФІЗИЧНОГО ВІДОКРЕМЛЕННЯ КАНАЛІВ КЕРУВАННЯ В КОРПОРАТИВНИХ IP-МЕРЕЖАХ

Юрій Кочергін
Національний авіаційний університет

Анотація: **З позицій технічного захисту інформації обгрунтована доцільність фізичного відокремлення каналів керування від каналів транспорту даних користувачів при побудові корпоративних комп'ютерних мереж.**
Summary: **From positions of technical protection of the information the expediency of use is proved physical branch of channels of management from channels of transport of the given users at construction of corporate computer networks.**
Ключові слова: **Інформація, система керування, інформаційна безпека.**

I Вступ

Наразі в корпоративних комп'ютерних мережах, що функціонують на основі стеку телекомунікаційних протоколів TCP/IP, технологічна інформація та інформація користувачів, як правило, транспортується одними і тими ж шляхами через спільні канали зв'язку. Іншими словами, маємо ситуацію, коли протокольні блоки даних (Protocol Data Unit – PDU) з даними користувачів і PDU, що містять пакети з керуючою інформацією, циркулюють в спільному фізичному середовищі, несанкціонований доступ до якого в багатьох випадках не є проблемою для зловмисників навіть з невеликими ресурсними можливостями. Зокрема, якщо в підсистемі керування корпоративною мережею для технічного забезпечення експлуатаційних задач використовується найбільш розповсюджена сьогодні схема "агент – менеджер" відповідно до специфікацій протоколу керування SNMP (Simple Network Management Protocol), то PDU з керуючою інформацією за допомогою міжмережного екрану (Firewall) відносно легко можуть бути відфільтровані зловмисником і використані з метою реалізації загроз в підсистемі керування. Тому традиційні методи спільного використання середовищ розповсюдження сигналів для транспорту як інформації користувачів, так і різного роду технологічної інформації не в змозі забезпечити необхідну ступінь захищеності інформаційних ресурсів в більшості корпоративних застосувань.

Основний шлях підвищення захищеності інформації в каналах її транспортування, що практикується сьогодні, – це використання механізмів криптографічного перетворення інформації. Однак застосування

ефективних криптографічних засобів суттєво збільшує вартість системи захисту, а в багатьох випадках ще і ускладнює технологічні схеми обробки інформації до неприйнятного на практиці рівня. Тому розробка шляхів побудови корпоративних комп'ютерних мереж, що дають змогу без застосування "міцної" криптографії заощадливими з економічної точки зору методами підвищити захищеність мережної (особливо, керуючої) інформації, є доцільною.

II Постановка задачі

В роботі пропонується спосіб вирішення задачі підвищення захищеності інформаційних ресурсів підсистем керування в корпоративних комп'ютерних мережах, що базується на принципі фізичного відокремлення технологічних каналів підсистеми керування від каналів, через які циркулює інформація користувачів. Розглядаються корпоративні мережі трьох рівнів масштабованості: на рівні локально розташованого підприємства (кампуса); на рівні корпоративної мережі, фрагменти якої розосереджені по території одного населеного пункту міського типу; на глобальному рівні, коли підрозділи корпорації (і, отже, фрагменти локальних мереж) розташовані у декількох різних населених пунктах (можливо, навіть поза межами України).

III Основна частина

Узагальнена структурна схема корпоративної комп'ютерної мережі, в якій технологічні канали керування відокремлені від каналів транспорту інформації користувачів, зображена на рис. 1.

Із рис. 1 випливає, що як середовище транспортування технологічних сигналів підсистеми керування пропонується використати: канали мереж з комутацією каналів (відомчі або загальнодоступні); виділені канали цифрових та/або аналогових систем передачі різної пропускної спроможності (наприклад, канали тональної частоти, первинних або вторинних групових трактів аналогових систем передачі, потоки E1 цифрових систем передачі тощо); прямі фізичні з'єднання. Вибір виду середовища транспортування технологічних сигналів та необхідної ємності каналів керування залежить, головним чином, від рівня масштабованості корпоративної мережі і необхідного ступеню захищеності інформаційних ресурсів підсистеми керування.

Зокрема, якщо мова йде про невелику корпоративну мережу рівня кампусу, то транспортування технологічних сигналів підсистеми керування між фрагментами локальних мереж цієї мережі (наприклад, між поверхами однієї будівлі) може здійснюватися через прямі фізичні з'єднання. Зрозуміло, що топологічні схеми прокладки фізичних ліній мають суттєво відрізнятися від топологічних схем прокладки основних каналів передачі даних, щоб суттєво ускладнити можливі дії несанкціонованих суб'єктів щодо доступу до ресурсів підсистеми керування. Якщо корпорація має власну АТС, зона обслуговування котрої співпадає з зоною обслуговування комп'ютерної мережі, то доцільно розглянути схему організації транспортування технологічних сигналів комп'ютерної мережі через комутовані телефонні канали власної корпоративної АТС. Така інтеграція ресурсів двох корпоративних мереж на рівні кампусу є можливою, якщо мати на увазі, що в цьому випадку для обміну технологічними сигналами можуть виявитися достатніми невеликі значення ширини смуги каналів передачі. В цьому разі буде можливим утворення стандартних аналогових модемних каналів на базі виділених або комутованих телефонних каналів корпоративної АТС для організації обміну сигналами, що відносяться до підсистеми керування корпоративною комп'ютерною мережею. Зрозуміло, що доступ до технологічної інформації за умов її транспортування каналами АТС (особливо, комутованими) буде в значній мірі утруднений.

У випадку організації захисту технологічної інформації в комп'ютерних мережах масштабу міста як середовище транспортування цієї інформації можливо використати виділені або комутовані канали місцевої телефонної мережі загального користування (Public Switched Telephone Network – PSTN) або канали зв'язку відомчих мереж. Це – недороге економічно ефективне рішення, і, в той же час, воно дозволяє суттєво підвищити захист технологічної інформації, оскільки набагато утруднює доступ до неї з боку неавторизованих осіб.

Якщо розглядати шляхи побудови системи захисту підсистеми керування корпоративною мережою глобального рівня, то використання принципу фізичного відокремлення потоків інформації користувачів від потоків технологічної інформації з позицій технічного захисту інформації є безумовно виправданим. Але на практиці в цьому випадку на перший план виступають економічні міркування, оскільки необхідно враховувати суттєву вартість оренди міжміських каналів зв'язку та (або) цифрових систем передачі.

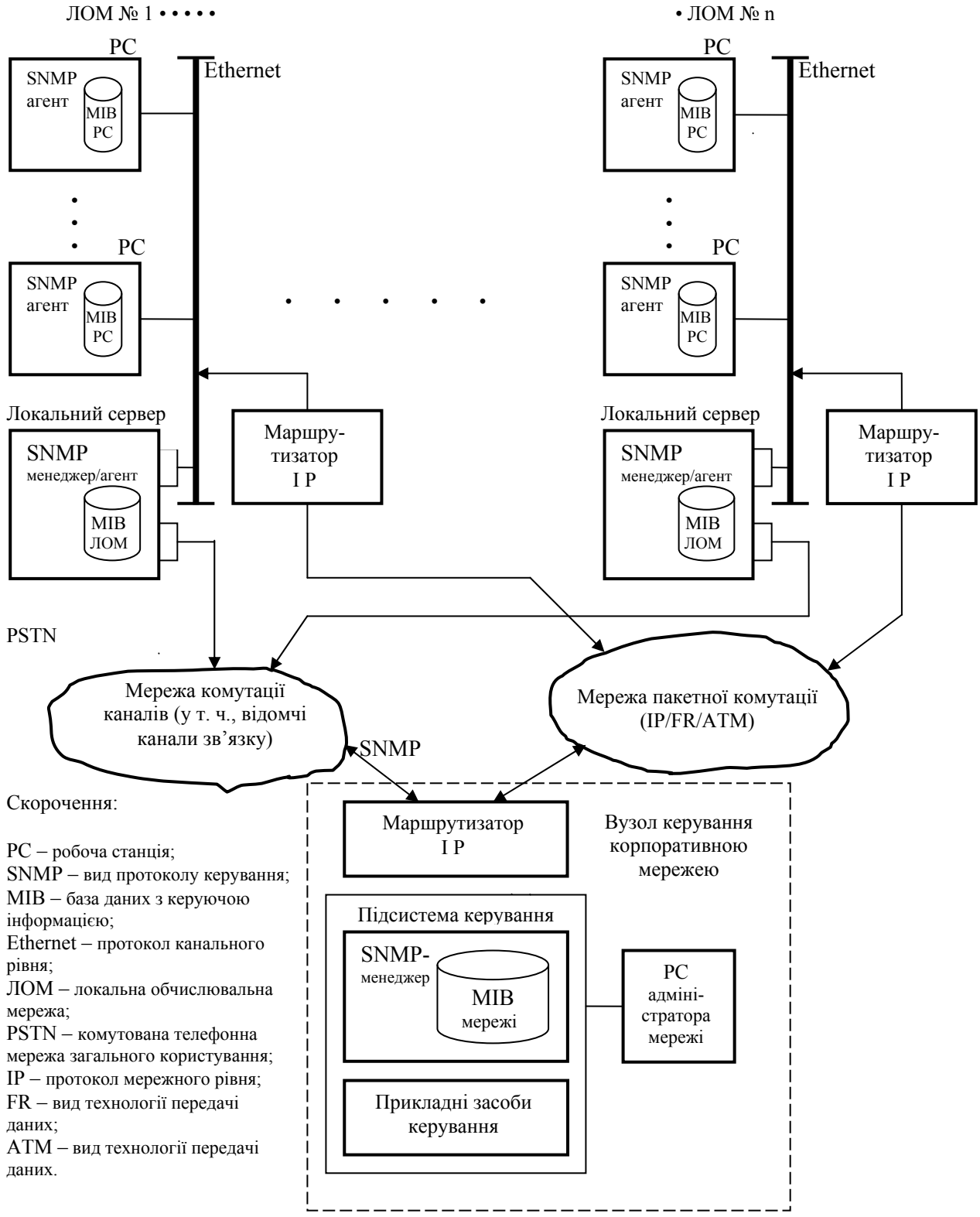

Рисунок 1 – Структура корпоративної комп'ютерної мережі з відокремленими каналами керування

Процес функціонування корпоративної комп'ютерної мережі з відокремленими каналами керування можливо пояснити наступним чином. Робочі станції (PC) користувачів корпорації об'єднані в локальні обчислювальні мережі (ЛОМ), наприклад, за технологією Ethernet (будь-якої версії), тобто маємо *n* фрагментів територіально розосереджених ЛОМ, які, в свою чергу, стандартним шляхом (наприклад, з

використанням IP-маршрутизатора) через канали передачі даних мереж пакетної комутації об'єднані в корпоративну комп'ютерну мережу. В мережах пакетної комутації можуть використовуватися будь-які відомі технології передавання даних: IP (Internet Protocol), FR (Frame Relay) або ATM (Asynchronous Transfer Mode).

Керування корпоративною мережею здійснюється згідно з моделлю взаємодії "агент – менеджер". Програмне застосування, яке ініціює команди керування і приймає повідомлення від керованих об'єктів, називається програмою-менеджером, а програмне застосування, що встановлюється на керованих об'єктах і виконує команди керування, зокрема надсилає повідомлення від імені керованих об'єктів, називається програмою-агентом. В нашому випадку програми – менеджери проміжного рівня встановлюються на локальних серверах фрагментів ЛОМ. Вони виконують функції безпосереднього керування всіма елементами фрагментів ЛОМ, в першу чергу робочими станціями користувачів. Для цього на кожній РС інсталюється відповідна програма-агент. Менеджер фрагменту ЛОМ (в нашому випадку він інсталюється на локальному сервері фрагменту корпоративної мережі) встановлює взаємозв'язок з усіма агентами цього фрагменту за протоколом SNMP, після чого починається процес обміну технологічною інформацією. Програма-агент здійснює посередницькі функції між менеджером та керованими ресурсами РС. Взаємодія агента з цими ресурсами здійснюється через уніфіковані на міжнародному рівні [1 – 3] функціональні інтерфейси. База даних з характеристиками стану елементів РС зветься базою інформації керування SNMP (Management Information Base, MIB) цієї РС. MIB – це віртуальний інформаційний масив, що містить в упорядкованому вигляді вичерпні дані щодо стану керованої РС, тобто фактично є інформаційною моделлю керованого об'єкту. В цій моделі відображені робочі характеристики РС, на котрі є можливим здійснювати вплив або котрі можливо контролювати в процесі керування. Програма-агент підтримує у реальному часі актуальність MIB керованого об'єкту, нормалізує (тобто, упорядковує і фільтрує) дані цієї MIB і транслює "очищені" дані з неї до MIB менеджера. Для поновлення своєї бази менеджер з необхідною періодичністю запитує агента. Таким чином, MIB менеджера містить відфільтровані дані з усіх MIB РС фрагменту ЛОМ і, отже, має повну інформацію щодо поточних характеристик усіх керованих об'єктів цього фрагменту мережі. Аналогічна схема "агент – менеджер" діє і на більш високому рівні ієрархії управління – на рівні управління всією корпоративною мережею. Тільки в цьому випадку програми-агенти розміщуються на локальних серверах фрагментів ЛОМ (поряд з SNMP-менеджерами цих фрагментів), а програма-менеджер вищого рівня інсталюється безпосередньо на вузлі керування корпоративною мережею. Іншими словами, маємо дворівневу схему керування.

В типовій ситуації PDU з упакованими SNMP-командами разом з PDU, що містять інформацію користувачів, циркулюють каналами мереж пакетної комутації і відносно легко можуть бути перехоплені зловмисниками. В нашому випадку, як це витікає із рис. 1, ці команди відокремлюються від загального потоку даних на рівні прикладних систем і передаються через інше фізичне середовище, за яке в багатьох практичних застосуваннях можливо і доцільно вибрати канали мереж комутації каналів або магістральних систем передачі.

IV Висновки

1. Фізичне відокремлення каналів керування від каналів, через які здійснюється передача інформації користувачів корпоративних комп'ютерних мереж, дозволяє суттєво підвищити рівень захищеності інформаційних ресурсів підсистем керування цими мережами.

2. Фізичне розмежування потоків інформації користувачів і потоків технологічної інформації підсистем керування під час створення невеликих корпоративних мереж в межах однієї локальної території корпорації не потребує значних витрат ресурсів і, тому, з позицій технічного захисту інформації є можливим і доцільним способом організації захисту.

3. В корпоративних мережах, середніх за масштабами розповсюдженості, також доцільно застосування схем фізичного відокремлення потоків технологічної інформації від загальних потоків даних з інформацією користувачів. Як альтернативне середовище передачі можливо використати канали абонентського доступу власної корпоративної АТС (якщо її зона обслуговування співпадає із зоною обслуговування комп'ютерної мережі) і навіть відносно недорогих каналів PSTN.

4. У великих корпоративних комп'ютерних мережах під час створення системи захисту інформаційних ресурсів підсистеми керування слід брати до уваги можливість організації обміну керуючою інформацією через фізично відокремлене середовище розповсюдження сигналів. В деяких випадках така організація захисту може бути економічно виправданою.

Література: ***1.*** *Harrington D., Presuhn R., Wijnen B. An Architecture for Describing SNMP Management*