УДК 004.75

Ю.Р. Гарасим, В.Б. Дудикевич
Національний університет “Львівська політехніка”,
кафедра захисту інформації

ІНФОРМАЦІЙНА БЕЗПЕКА ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖ ЗВ’ЯЗКУ

Розглянуто модель програмно-керованої АТС відповідно до нормативних документів системи ТЗІ в Україні, визначено її недоліки. Запропоновано новий перелік каналів реалізації інформаційних загроз для захищених корпоративних мереж зв’язку, а також модель комплексної системи технічного захисту інформації захищеної корпоративної мережі зв’язку.

This paper is observed a software-programmable PBX model relative to normative documents of information technical security system in Ukraine also its disadvantages are determined. The model propose a new list of information threats realization for secured enterprise telecommunication network and information technical security complex system model for secured enterprise telecommunication network.

Постановка проблеми. В світовому рейтингу з найтехнологічніших напрямів діяльності сучасного суспільства провідне місце посідає галузь телекомунікацій. Світ переживає справжній бум розроблення та впровадження все нових і нових методів та технологій передачі, обробки та зберігання інформації, в результаті чого за останні 10–15 років спостерігається глобалізація телекомунікаційних мереж, стирання національних кордонів та створення єдиного світового інформаційного простору.

Лавиноподібне і революційне впровадження різноманітних технологій в методи та технології передачі, обробки та зберігання інформації в телекомунікаційних мережах змушують принципово по-новому розглядати роль та значення технічного захисту інформації.

Концепція технічного захисту інформації в Україні, затверджена Постановою Кабінету Міністрів України від 8 жовтня 1997 року № 1126, визначає, що об’єктивними підставами такого підходу є зростання загроз інформації, що спричинено лібералізацією суспільних та міждержавних відносин, застосуванням технічних засобів оброблення інформації та засобів зв‘язку іноземного виробництва, поширенням засобів несанкціонованого доступу до інформації та впливу на неї.

За цих умов державні інтереси полягають в технічному захисті інформації, що циркулює в мережах зв‘язку державних відомств та недержавних структур, несанкціонований доступ або пошкодження якої може завдати значних збитків державній та/або економічній безпеці України.

Узагальнюючою назвою таких мереж зв’язку державних відомств та недержавних структур у сучасній термінології є захищені відомчі або корпоративні телекомунікаційні мережі (мережі зв’язку).

Актуальність теми

1. Нормативні документи системи ТЗІ в Україні [1–6], якими визначена методологія створення системи ТЗІ (технічний захист інформації) ЦАТС (цифрова АТС) та оцінки захищеності її інформаційних ресурсів, були впроваджені в 90-х роках минулого століття. Своєю чергою, технології ЦАТС розвивались дуже динамічно, внаслідок чого традиційна АТС перетворилась на комутаційну платформу, на якій формується розгалужений комплекс програмно-апаратних аплікацій і цифрового абонентського сервісу. До таких рішень, які стали складовими компонентами

ЦАТС за цей період, передовсім можна віднести центри обробки викликів (Call Center), системи обробки абонентських голосових, електронних і факсимільних повідомлень, безпровідний абонентський радіодоступ стандарту DECT.

Проте цей розвиток технологій ЦАТС поки що не знайшов свого відображення в НД (нормативний документ) СТЗІ (система ТЗІ) в Україні. Якщо розвиток телекомунікаційних і інформаційних технологій йде у напрямі розробки і впровадження інтегрованих рішень, таких, як аплікації комп'ютерно-телефонної інтеграції (CTI – Computer-Telephone Integration), то в НД СТЗІ ці технології є предметом двох самостійних і несумісних напрямків захисту інформації в комп'ютерному і телекомунікаційному обладнанні.

2. Стан нормативної бази системи ТЗІ в Україні безпосередньо впливає на ефективність державної експертизи СТЗІ ЦАТС та її спроможність забезпечити власників захищених корпоративних мереж зв'язку вичерпною інформацією щодо реалізованої в ЦАТС системи ТЗІ й організаційно-технічними заходами з усунення "слабких місць" у ній, особливо за умов використання різноманітних програмно-апаратних аплікацій ЦАТС.

3. Визначення методів і напрямків технічного захисту ЦАТС часто відокремлюється від телекомунікаційних та інформаційних технологій, з якими вони взаємодіють у корпоративних мережах зв'язку і через які можуть реалізовуватись інформаційні атаки на ЦАТС.

4. Сьогодні в технічній літературі (у відкритій і спеціальній) практично відсутні публікації з викладенням принципів побудови системи ТЗІ ЦАТС, які були б пов'язані з технічною реалізацією апаратно-програмної побудови конкретних моделей ЦАТС. Це об'єктивно обґрунтовується тим, що виробники ЦАТС практично не поширюють необхідний для цього деталізований опис компонентів ЦАТС, особливо тих, що безпосередньо формують СТЗІ ЦАТС, і не зацікавлені в оприлюдненні у відкритих джерелах інформації їхньої корпоративної політики безпеки, що реалізується в СТЗІ ЦАТС.

Мета і задачі дослідження. Метою дослідження є визначення сучасних інформаційних загроз захищених корпоративних мереж зв'язку, технічну основу яких традиційно становлять комутаційні системи, що реалізовані на виробничо-відомчих АТС, і саме тому вони є однією з основних сфер системи технічного захисту інформації в Україні, а також визначення методів протидії їм.

Для досягнення мети були поставлені такі завдання:

- розробити модель цифрової АТС як програмно-апаратного комплексу;
- запропонувати новий перелік каналів реалізації інформаційних загроз для захищених корпоративних мереж зв'язку;
- розробити модель комплексної СТЗІ захищеної корпоративної мережі зв'язку;

Об'єкт дослідження – безпека захищених корпоративних мереж зв'язку.

Предмет дослідження – методи та засоби захисту корпоративних мереж зв'язку.

Наукова новизна

- розроблено модель цифрової АТС як програмно-апаратного комплексу;
- вдосконалено та доповнено перелік каналів реалізації інформаційних загроз для захищених корпоративних мереж зв'язку;
- розроблено модель комплексної СТЗІ захищеної корпоративної мережі зв'язку.

Модель програмно-керованої АТС відповідно до нормативних документів системи ТЗІ в Україні. Нормативні документи системи ТЗІ України використовують відносно цифрових АТС термін "програмно-керовані АТС", роблячи акцент на метод програмного управління, а не на принцип комутації, за яким традиційно класифікують АТС.

Згідно із цими документами [1–6] з позиції ТЗІ структура програмно-керованої АТС поділяється на дві порівняно незалежні підсистеми: підсистема керування станцією; підсистема комутації абонентських і з'єднувальних ліній зв'язку (КАЗЛ).

Незалежність даних підсистем керування станцією і КАЗЛ розуміють в тому сенсі, що підмножина загроз для інформації, яка характерна для підсистеми керування станцією, не

перетинається з підмножиною загроз, яка характерна для підсистеми КАЗЛ, через відсутність механізмів реалізації загроз на підсистемі керування з боку підсистеми КАЗЛ і, навпаки, – на підсистемі КАЗЛ з боку підсистеми керування станцією.

Відносність незалежності вищезгаданих підсистем полягає в тому, що за певних умов (внаслідок помилок або некоректних/зловмисних дій), які були допущені на стадіях життєвого циклу АТС, що передують експлуатаційним (наприклад, при встановленні програмних закладок або апаратних закладних пристроїв), або внаслідок якісної недостатності АТС можливі реалізації загроз на підсистемі керування з боку підсистеми КАЗЛ, і, навпаки, – на підсистемі КАЗЛ з боку підсистеми керування станцією.

Наведена структурна схема програмно-керованої АТС із позицій ТЗІ, і моделі інформаційних загроз, що визначаються на її основі в нормативних документах СТЗІ, неповною мірою відображають відповідно сучасну програмно-апаратну архітектуру ЦАТС та інформаційні загрози, які можуть виникати, а саме:

1. Комутаційна матриця цифрової АТС реалізована у вигляді просторово-часового комутатора, що реалізує багатостанційний доступ з часовим розподілом каналів, який є розгалуженими по всій просторовій структурі АТС. Управління комутацією здійснюється за рахунок центрального керуючого пристрою і механізму розподілу ресурсів шинної структури.

2. Така архітектура не передбачає поділу системи управління і комутації на визначені в НД СТЗІ підсистеми керування станцією і комутації абонентських і з'єднувальних ліній зв'язку.

3. Система управління цифрової АТС з позицій СТЗІ розглядається як двоєдина, – з одного боку, децентралізованою, тому що елементи програмного управління є в усіх апаратних компонентах АТС, і централізованою, з іншого, тому що всі вони керуються єдиною системою управління і комутації, порушення роботи якої призводить до виходу з ладу всієї АТС чи модифікації реалізованих нею функцій.

4. На апаратному і програмному рівнях неможливо здійснити інформаційні атаки на визначену НД СТЗІ підсистему комутації абонентських і з'єднувальних ліній зв'язку від атак на систему керування АТС. Тобто інформаційні атаки не можуть поділятися на атаки підсистеми комутації абонентських і з'єднувальних ліній зв'язку й атаки системи керування. Наведені в переліку НД СТЗІ моделі інформаційних загроз стосовно підсистеми комутації абонентських і з'єднувальних ліній зв'язку фактично реалізуються за допомогою атак безпосередньо на/через абонентські та з'єднувальні лінії (на ці лінії – з метою зняття інформації з них, через них – з метою впливу на систему управління та комутації ЦАТС).

5. Модель програмно-керованої АТС не деталізує достатньою мірою види з'єднувальних і абонентських ліній, термінальних пристроїв, тоді як, наприклад, інформаційні загрози, що можуть бути реалізовані через цифрові і аналогові з'єднувальні лінії, аналогові і цифрові, зокрема радіо-, термінали, мають різні механізми і є різними за своєю суттю.

6. Нині перелік каналів реалізації інформаційних загроз є набагато різноманітнішим, ніж визначений нормативними документами СТЗІ і містить, наприклад, системи програмно-апаратних аплікацій, безпроводового радіодоступу, засобів IP-телефонії тощо, які є достатньо небезпечними каналами реалізації інформаційних загроз ЦАТС.

7. Сучасний розвиток телекомунікаційних і інформаційних технологій відбувається у напрямі розробки і впровадження інтегрованих рішень, таких, як аплікації комп'ютерно-телефонної інтеграції, але в НД СТЗІ ці технології, як і раніше, залишаються предметом двох самостійних і несумісних напрямків захисту інформації відповідно в комп'ютерному і телекомунікаційному обладнанні.

8. Реалізація інформаційних атак на систему керування і комутації можлива як на доексплуатаційній (технологічній), так і на експлуатаційній стадіях життєвого циклу АТС. Нормативне унеможливлення атак на систему управління і комутації на експлуатаційній стадії може відповідно деформувати модель системи ТЗІ АТС, що реалізується на цій стадії життєвого циклу.

Така модель не враховує усіх сучасних програмних й апаратних компонентів ЦАТС і не дає змоги ефективно будувати моделі її інформаційних загроз. [7]

Модель цифрової АТС як програмно-апаратного комплексу. Цифрова АТС, що розглядається як програмно-апаратний комплекс на апаратному і програмному рівнях, повинна мати структуру, що наведена на рис. 1 та рис. 2.

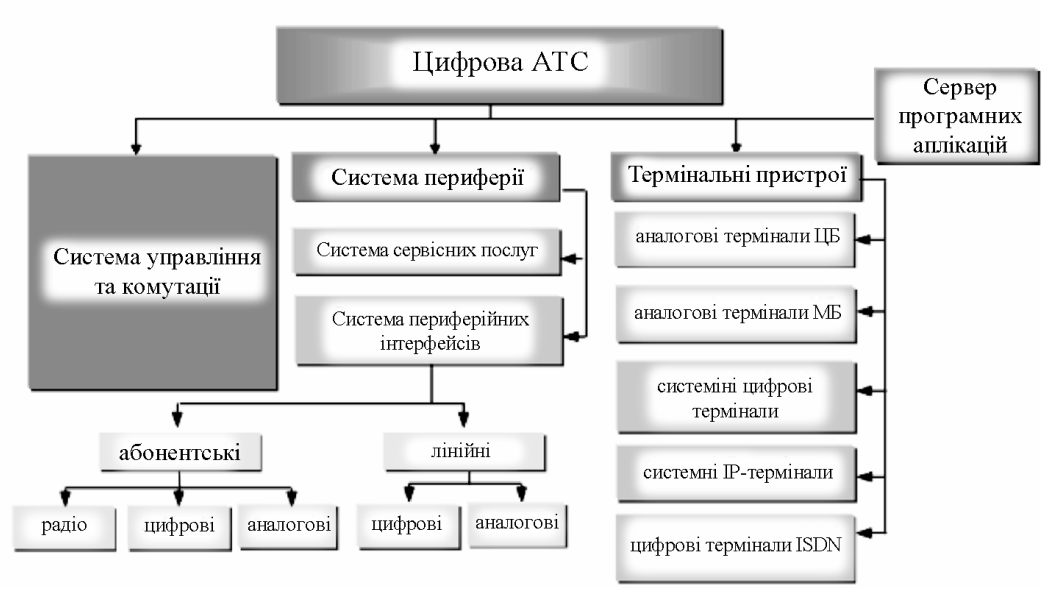

Рис. 1. Апаратна структура цифрової АТС

Рис. 2. Структура програмного забезпечення цифрової АТС

Апаратна структура ЦАТС. Система управління і комутації становить основу ЦАТС і містить комутатор, центральний керуючий пристрій (центральний процесор), пам'ять і порти вводу-виводу (рис. 3).

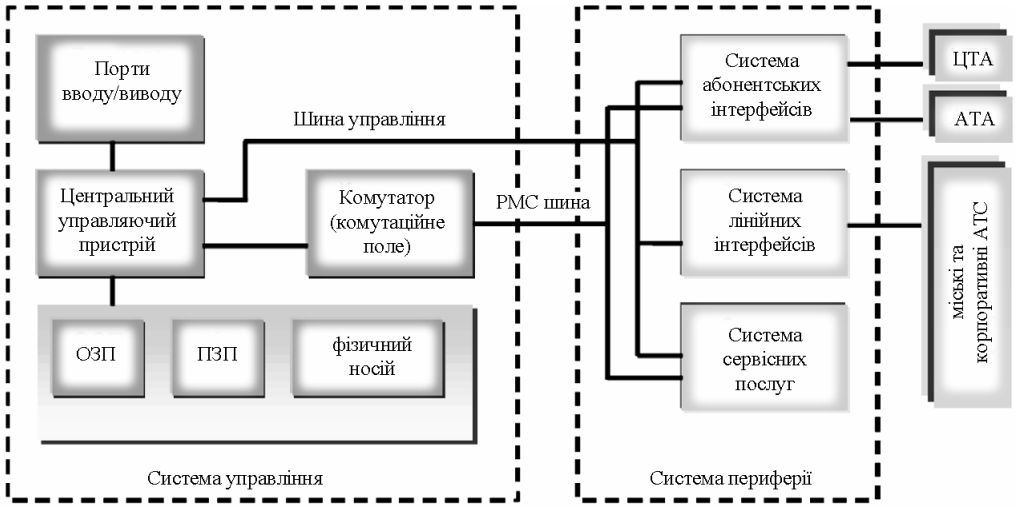

Рис. 3. Система управління і комутації цифрової АТС

Заходи інформаційної безпеки корпоративної мережі на експлуатаційному етапі. Заходи на експлуатаційному етапі виконує безпосередньо персонал власника захищеної корпоративної мережі зв'язку і вони передбачають організаційні, організаційно-технічні і технічні заходи.

До організаційних заходів належить визначення методик і напрямків створення системи інформаційної безпеки захищеної корпоративної мережі зв'язку на експлуатаційному етапі, які передбачають відповідну послідовність дій із забезпечення безпеки захищених корпоративних мереж зв'язку. В узагальненому вигляді вони можуть бути такими: дослідження мережі зв'язку, розроблення концепції її захисту, вибір методів і обладнання захисту, розроблення методики оцінки ефективності захисту, обґрунтування інвестицій в захист (розрахунок економічного ефекту від заходів, що пропонуються), розробка нормативно-методичних документів, створення центру інформаційної безпеки (центру реагування), створення дослідного (сертифікаційного) полігона, створення фрагмента (дослідної зони) захищеної мережі і здійснення натурних іспитів розроблених методів і апаратури, впровадження системи безпеки мережі поетапно відповідно до концепції за "м'яким" та/або "жорстким" сценарієм.

Крім того, нормативними документами забезпечення інформаційної безпеки захищеної корпоративної мережі визначаються функції безпеки, що реалізуються службами інформаційної безпеки організацій, підприємств і установ, до яких можна зарахувати: аутентифікацію (користувачів, об'єктів і джерел даних); контроль доступу; забезпечення цілісності повідомлень; забезпечення конфіденційності; забезпечення доступності; безвідмовність відправки/доставки; локалізація місця ймовірної атаки; моніторинг і аудит; оповіщення про порушення і відновлення функціонування; адаптації до змінних умов функціонування мережі.

Ці функції планується виконувати за допомогою відповідних механізмів безпеки, в ролі яких можуть бути використані: механізми шифрування; механізми цифрового підпису; механізм обміну інформацією аутентифікації; механізми контролю доступу; механізми цілісності даних; механізм захисту трафіку; механізм управління маршрутизацією; механізм нотаризації тощо.

До організаційно-технічних заходів належать різноманітні заходи з визначення та встановлення контрольованої зони об'єкта, тобто "території, допуск осіб на яку обмежений та яка знаходиться під контролем" [8].

Визначальним для реалізації контрольованої зони є категорія об'єкта, що присвоюється йому за результатом атестації відповідно до Положення про категоріювання об'єктів ТПКО-95. Основ-

ним критерієм присвоєння категорії об'єкту є найвищий рівень таємності інформації, що обробляється та циркулює на об'єкті.

Така контрольована зона може вміщувати декілька концентричних зон, за якими зростають заходи забезпечення інформаційної безпеки відповідно до розміщення компонентів захищеної корпоративної мережі.

Зона безпеки захищеної корпоративної мережі зв'язку (рис. 4) передбачає розташування основних засобів технічного обладнання вторинної корпоративної мережі. Ця зона реалізується як вузол зв'язку з такими елементами: АТС; кросовий зал (крос); лінійно-апаратний зал (з апаратурою каналоутворення); центр електроживлення (у складі блоків живлення та акумуляторних батарей резервного живлення); обладнання технічного захисту інформації (міжмережеві екрани, генератори широкосмугових сигналів тощо); АРМ і ПЕОМ адміністратора захищеної корпоративної мережі; сервер (умовно відокремлений від ПЕОМ адміністратора корпоративної мережі) системи корпоративного аудиту і моніторингу.

Організаційно-технічні і технічні заходи з інформаційного захисту корпоративної мережі реалізуються комплексно.

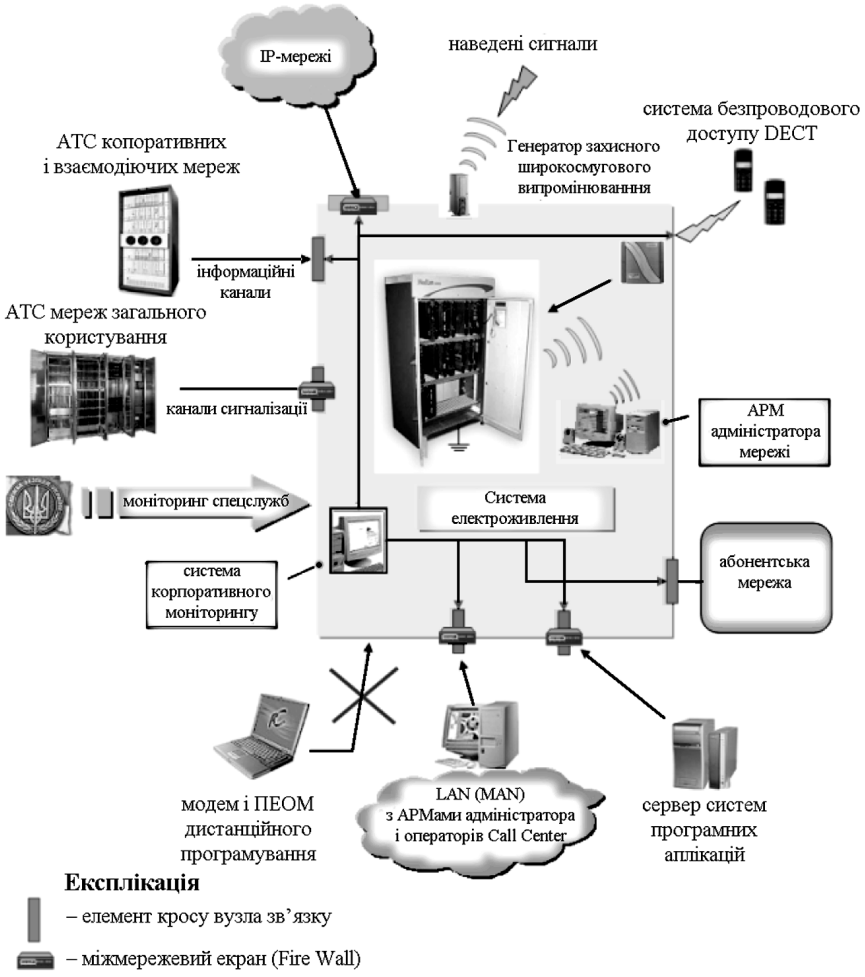

Рис. 4. Модель комплексної СТЗІ захищеної корпоративної мережі зв'язку

Цей комплекс організаційно-технічних і технічних заходів можна зобразити моделлю (рис. 4), де визначені потенційні канали інформаційних атак на ЦАТС. Модель передбачає:

1. Здійснення захисту каналів сигналізації та синхронізації цифрових з'єднувальних ліній із зустрічними АТС із використанням системи моніторингу та технології міжмережевих екранів.

2. Розміщення ЦАТС і всіх її компонентів у контрольованій зоні (зоні безпеки), де обов'язково реалізуються відповідні організаційно-режимні та обмежувальні заходи.

У приміщенні ЦАТС реалізуються засоби вторинного та резервного електроживлення (під'єднуються в буфері і виконують, крім звичайних, ще й захисні функції). У контрольованих зонах також реалізуються контури захисного заземлення.

3. Використання генераторів шуму для мінімізації загрози використання інформаційних параметрів ПЕМВН для порушення конфіденційності. Отже, можна уникнути загрози використання побічних випромінювань і наведених сигналів від ЦАТС і ЕОМ адміністратора системи.

4. Розміщення базових станцій системи безпровідного доступу стандарту DECT в другій та третій контрольованій зонах (КЗ), що дає змогу забезпечити контроль за їх під'єднанням по провідних каналах через крос до ЦАТС. Однак це не виключає зняття інформації за рахунок випромінювання радіопередавальної частини базових станцій такими засобами, як спеціалізовані сканери та інші аналогічні прилади. Загалом радіус першої КЗ повинен перекривати дальність радіовипромінювання базових станцій.

5. У цій моделі всі інформаційні канали входу в ЦАТС є контрольованими.

Канали під'єднання до ЦАТС за протоколом 10/100BaseT сервера систем програмних аплікацій і локальної LAN (MAN) з АРМами адміністратора і операторів Call Center перебувають під моніторингом міжмережевого екрана Firewall.

Весь трафік, як внутрішній, так і вхідний/вихідний по з'єднувальних лініях, що на схемі зображений як вхід до контрольованої зони з відповідних напрямків (від зустрічних АТС корпоративної мережі, мереж, що взаємодіють, та мереж загального користування), контролює система корпоративного моніторингу й аудиту.

Такі системи моніторингу з генерацією різноманітних звітних форм (як в екранній, так і в документованій формі) є достатньо дієвим механізмом контролю за трафіком, що передається через ЦАТС.

6. Реалізацію в складі захищеної корпоративної мережі ЦАТС послуг IP-телефонії (крім мереж державних структур). Захист IP-шлюзу в ЦАТС забезпечується міжмережевим екраном. Однак заходи інформаційної безпеки не обмежуються лише захистом IP-шлюзу від ЦАТС до мережі Internet або Ethernet. Захист передбачає використання технологій захищених корпоративних мереж зв'язку, таких, як: міжмережеві екрани, системи виявлення/запобігання атакам, системи аутентифікації, технології віртуальних локальних мереж (VLAN), віртуальних приватних мереж (VPN), шифрування трафіку в режимі "end-to-end".

Однак все це не дає змоги запобігати інформаційним атакам перехоплення інформаційних пакетів з визначеними параметрами адресата відправлення або отримання за умов використання як транспортної мережі Internet.

7. Захист програмного забезпечення ЦАТС – найвразливіше місце захищеної корпоративної мережі зв'язку [10]: 1) радикальний метод (повна заміна імпортного фірмового ПЗ математичним забезпеченням власної розробки на підставі захищеної операційної системи); 2) консервативний метод (дослідження фірмового ПЗ на предмет недокументованих можливостей (закладок) і їхнє усунення); прагматичний метод (комбінація наведених вище методів – розробка захисної оболонки (shell) для фірмового ПЗ).

Перший метод є найгроміздкішим, але достатньою мірою гарантує стійкість ПЗ при атаках. Другий метод потребує отримання вихідних текстів від розробника ПЗ. Останній метод – створення захисної оболонки – є доволі складним. Для його реалізації необхідне розроблення спеціальних апаратно-програмних засобів захисту: конверторів і фільтрів сигналізації, фільтрів програмування АТС, кодерів (шифраторів) Е1, використання технологій віртуальних приватних мереж для напрямлення трафіку управління і сигналізації через спеціально організований тунель.

Абонентські мережі у плані технічного захисту інформації є одним із найскладніших компонентів захищеної корпоративної телекомунікаційної мережі, що зумовлено різноманітними факторами.

Абонентські мережі в межах території об'єкта (під яким розуміємо офіси установ, відомств, адміністративні і виробничі будівлі підприємств, пункти управління та військові містечка силових та правоохоронних структур тощо) розгортаються відповідно до основного завдання надання послуг зв'язку на робочі місця персоналу. Це визначає структуру, топологію і ємність абонентських ліній, що прокладаються, зокрема через декілька контрольованих зон, внаслідок чого рівень їхньої безпеки відповідно змінюється [9].

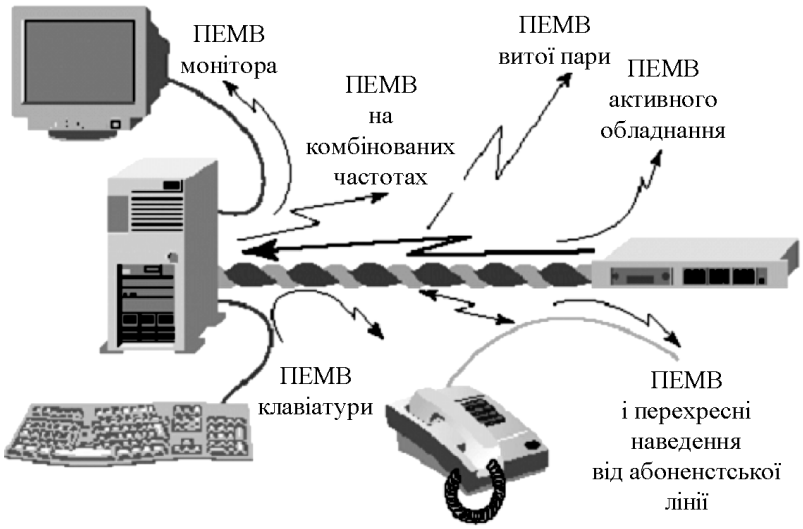

Рис. 5. Джерела ПЕМВН на робочому місці персоналу

Абонентські пристрої розміщуються на робочих місцях персоналу, де, як правило, функціонує різноманітне обладнання (засоби обчислювальної та організаційної техніки, електричні промислові та побутові прилади тощо), що утворює заздалегідь непередбачувану електромагнітну обстановку з ПЕМВН й акустоелектричних перетворень. На рис. 5 зображене робоче місце посадової особи з ПЕОМ, що під'єднане витою парою до ЛОМ та абонентським терміналом до ЦАТС із джерелами ПЕМВН.

Різноманітність побудови і реалізації абонентських мереж, фізичних процесів в них створює потенційну загрозу витоку інформації по технічних каналах такої фізичної природи, як: 1) акустичні (серед них акустоперетворення); 2) електричні; 3) радіо, що можуть мати природу акустичного перетворення, електромагнітного випромінювання і паразитних звуків, наведень, і поширюватись в усіх діапазонах випромінювання (СХ, ДХ, КХ, УКХ). [10]

У сучасних захищених корпоративних мережах зв'язку реалізуються такі абонентські пристрої ЦАТС, як аналогові телефонні апарати системи ЦБ і МБ (до яких можна зарахувати факсимільні апарати), цифрові системні термінали компаній-виробників, цифрові системи ISDN, цифрові телефонні термінали IP-телефонії, комп'ютерні екранні IP-телефони, цифрові радіотермінали систем безпровідного доступу, а також АРМи систем програмно-апаратних аплікацій і адміністрації мереж зв'язку, що реалізуються на базі ПЕОМ.

При захисті телефонних апаратів і телефонних ліній необхідно враховувати декілька аспектів:

− телефонні апарати (й при покладеній МТ трубці) можуть бути використані для перехоплення акустичної голосової інформації з приміщення, в яких вони встановлені, тобто для підслуховування розмов у цих приміщеннях;

− телефонні лінії, що проходять через приміщення, можуть використовуватись як джерела живлення акустичних закладок, що встановлені в них, а також для передавання перехопленої інформації;

− можливим є перехоплення (підслуховування) телефонних розмов за допомогою гальванічного під'єднання або під'єднання через індукційний давач до телефонної лінії закладок (телефонних ретрансляторів), диктофонів та інших засобів несанкціонованого зняття інформації.

Телефонний апарат має декілька елементів, що здатні перетворювати акустичні коливання на електричні ("мікрофонний ефект"). До них належать дзвінковий ланцюг в аналоговому ТА, телефонний і мікрофонний капсулі. За рахунок електроакустичних перетворень в цих елементах виникають інформаційно небезпечні сигнали.

При покладеній мікротелефонній трубці телефонний і мікрофонний капсулі гальванічно від'єднані від телефонної лінії і при під'єднанні до неї спеціальних високочутливих низькочастотних підсилювачів є можливим перехоплення небезпечних сигналів, що виникають в елементах тільки дзвінкового ланцюга. Амплітуда цих сигналів, як правило, не перевищує часток мВ.

При використанні для зняття інформації методу "високочастотного нав’язування", незважаючи на гальванічне від’єднання мікрофона від телефонної лінії, сигнал нав‘язування завдяки високій частоті потрапляє в мікрофонний ланцюг і модулюється за амплітудою інформаційним сигналом.

Отже, в телефонному апараті є необхідним захищати як дзвінкове, так і мікрофонне коло.

Для захисту телефонного апарату від витоку акустичної (голосової) інформації по електро-акустичному каналу використовуються як пасивні, так і активні методи і засоби [9, 10].

Серед пасивних методів захисту найефективнішими є: обмеження небезпечних сигналів; фільтрація небезпечних сигналів; від’єднання джерел (перетворювачів) небезпечних сигналів.

До основних активних методів належать: подавання під час розмови в телефонну лінію синфазного маскуючого низькочастотного (мовного діапазону) сигналу (метод синфазної низько-частотної маскуючої перешкоди); подавання під час розмови в телефонну лінію високочастотного маскуючого сигналу звукового діапазону (метод високочастотної маскуючої перешкоди); пода-вання під час розмови в телефонну лінію високочастотного маскуючого ультразвукового сигналу (метод маскуючої ультразвукової перешкоди); підняття напруги в телефонній лінії під час розмови (метод підвищення напруги); подавання під час розмови в лінію напруги, що компенсує постійну складову телефонного сигналу (метод "обнулення"); подавання в лінію при покладеній МТ трубці маскуючого низькочастотного (мовного діапазону) сигналу (метод маскуючої низькочастотної перешкоди); подавання в лінію при прийомі повідомлень маскуючого низькочастотного (мовного діапазону) з відомим спектром (компенсаційний метод); подавання в телефонну лінію високо-вольтних імпульсів (метод "випалювання").

Висновки. Забезпечення інформаційної безпеки держави, всіх її інститутів є актуальним питанням і технічний захист інформації виступає практичним механізмом її реалізації.

Робота акцентує увагу на тому, що в реалізації системи ТЗІ цифрових АТС на всіх стадіях життєвого циклу важливими є всі взаємопов’язані і синхронізовані заходи виробників обладнання, державних органів СТЗІ в Україні і власників захищених корпоративних мереж зв’язку.

Наявність слабких місць в будь-якій ланці цього єдиного технологічного процесу, як показано в роботі на прикладі об‘єктивного відставання методологій і нормативної бази СТЗІ в Україні від темпів розвитку телекомунікаційних технологій, як і їхня недосконаліть, негативно впливають на ефективність комплексного захисту інформаційних і системних ресурсів захищених корпоративних мереж зв’язку.

1. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. – введ. 1999-05-28. – К.: ДСТСЗІ СБ України. 2. НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова). – введ. 1999-05-28. – К.: ДСТСЗІ СБ України. 3. НД ТЗІ 2. 5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту. – введ. 1999-07-01. – К.: ДСТСЗІ СБ України. 4. НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту. – введ. 1999-05-28. – К.: ДСТСЗІ СБ України. 5. НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту. – введ. 1999-05-28. – К.: ДСТСЗІ СБ України. 6. НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. – введ. 1999-05-28. – К.: ДСТСЗІ СБ України. 7. Ярмухаметов А. Информационная безопасность корпоративных (ведомственных) сетей связи / Ярмухаметов А. – Информост: радиоэлектронника и телекоммуникации. – 2002. – № 3. 8. Гончарок М.Х. Информа-ционная безопасность в телефонных сетях. – ЛОНИИС. – 2002. 9. Иванова Т.И. Корпаративные сети связи. – М.: Эко – Трендз. – 2001. 10. Гольдштейн Б.С. Мониторинг и предотвращение атак / Б.С. Гольдштейн, И.М. Ехриель, Р.Д. Рерле. – 2006.