практический сборник, вып. 1 «Технические средства защиты информации», К.: ООО «ТИД «ДС», 2003. ***3.*** *High Precision Cleaning for the Disk Drive Industry. Bill Lambert. Whitepaper, Kerry Ultrasonics Ltd, 2000.* ***4.*** *Методы сканирующей зондовой микроскопии для исследования поверхностей накопителей информации и восстановления данных. С. Коженевский, С. Прокопенко. Информационная безопасность офиса, Научно-практический сборник, вып. 1 «Технические средства защиты информации», К.: ООО «ТИД «ДС», 2003.* ***5.*** *Беседин Д. И., Боборыкин С. Н., Рыжиков С. С. Предотвращение утечки информации, хранящейся в накопителях на жестких магнитных дисках. Специальная техника. №1/2001.* ***6.*** *Жесткий диск – прямой канал утраты информации. С. Коженевский. Информационная безопасность офиса, Научно практический сборник, вып. 1 «Технические средства защиты информации», К.: ООО «ТИД «ДС», 2003.* ***7.*** *Anthony Thornton. End-of-Life Data Security in the Enterprise. Data Security Whitepaper. http://www.redemtech.com/* ***8.*** *Методы визуализации магнитных полей носителей информации. С. Коженевский. Реєстрація, зберігання і обробка даних. 2002, Т. 4, № 4, стр. 48-60.*

УДК 654.1 (045)

ЦЕНТР ОБСЛУГОВУВАННЯ ТЕЛЕФОННИХ ВИКЛИКІВ ЯК ЕКОНОМІЧНО ЕФЕКТИВНА ПЛАТФОРМА ДЛЯ КЕРУВАННЯ КОМПЛЕКСНОЮ СИСТЕМОЮ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Георгій Конахович, Володимир Чуприн
Національний авіаційний університет

Анотація: **Обґрунтовано доцільність використання центрів обслуговування телефонних викликів (Call Centers) як платформ для створення централізованих систем керування територіально розподіленими інформаційними системами.**
Summary: **The expediency of use of the centres of service of telephone calls (Call Centers) as platforms for creation централизованних of control systems is territorial by the allocated information systems.**
Ключові слова: **Інформація, система керування, інформаційна безпека.**

I Вступ

Проектування та створення засобів централізованого керування підсистемами технічного захисту інформації (ТЗІ) (що мають назву відповідно до моделі мережного керування ISO - Security Management) в сучасних складних територіально розподілених інформаційних системах (ІС), наприклад в корпоративних телефонних мережах, побудованих на основі телефонних мереж загального користування (PSTN), як правило, здійснюється в комплексі із засобами керування іншими чотирма підсистемами підтримки функцій експлуатації цих ІС (тобто, у комплексі з Fault, Configuration, Performance and Accounting Management) [1]. Ці засоби у переважній більшості випадків мають унікальну і громіздку логічну структуру, а вартість їхньої реалізації настільки велика, що є “непід’ємною” навіть для найбільших організацій України. Проблема керування розподіленими ІС утруднюється ще й тим, що реально на практиці для побудови мереж керування цими ІС використовуються лише мережі пакетної комутації із застосуванням популярного SNMP-протоколу прикладного рівня, або, в останній час, із застосуванням WEB-технологій (у гетерогенних розподілених середовищах іноді також використовується технологія керування CORBA і ін.) [2]. Звісно, що інформація користувача в загальнодоступних каналах мереж пакетної комутації у порівнянні з каналами мереж комутації каналів є більш уразливою з точки зору ТЗІ, тому що абонентські канали, які утворюються за допомогою засобів мереж пакетної комутації, є логічно (а не фізично) відокремленими і тому доступними для неавторизованих суб’єктів з невеликими ресурсними можливостями. З урахуванням вищезазначеного є доцільним здійснити спроби створення систем керування на основі використання мереж із комутацією каналів, які є менш уразливими з боку неавторизованих користувачів.

II Постановка завдання

Хоча засоби керування, що реалізують універсальну концепцію TMN, підтримувану MCE-T у рамках семирівневої моделі взаємодії відкритих систем [3], могли б знайти застосування в мережах комутації каналів, але внаслідок їхньої особливої складності (і, отже, високої вартості) вони в експлуатаційній практиці, як правило, не використовуються. Найбільш поширені заходи щодо протидії загрозам в мережах з пакетною комутацією – це використання технологій закриття каналів, базованих на криптографічних

методах, та (або) оренда виділених (некомутованих) каналів. Здійснення цих заходів незрівнянно збільшує вартість побудови та експлуатації систем централізованого керування розподіленими ІС. В результаті, більшість організацій – володарів корпоративних розподілених ІС – вимушені утримувати висококваліфікований експлуатаційний персонал майже в кожному вузлі своєї корпоративної ІС, що із зрозумілих причин не є оптимальним рішенням.

В той же час на телекомунікаційному ринку України з'явився продукт з поширеною у нашій країні назвою "Центр обслуговування телефонних викликів" (аналог англомовного терміну "Call Center"), який, на наш погляд, доцільно використовувати (безумовно, поряд з іншими сферами застосування) як технічну платформу для керування комплексними системами ТЗІ територіально розподілених ІС, перш за все у корпоративних телефонних системах, що складаються із великої кількості територіально розгалужених місцевих корпоративних телефонних систем, об'єднаних між собою через канали PSTN. У цій роботі висвітлюється один із шляхів використання вищезазначеного продукту в задачах побудови центрів керування розподіленими ІС.

ІІІ Основна частина

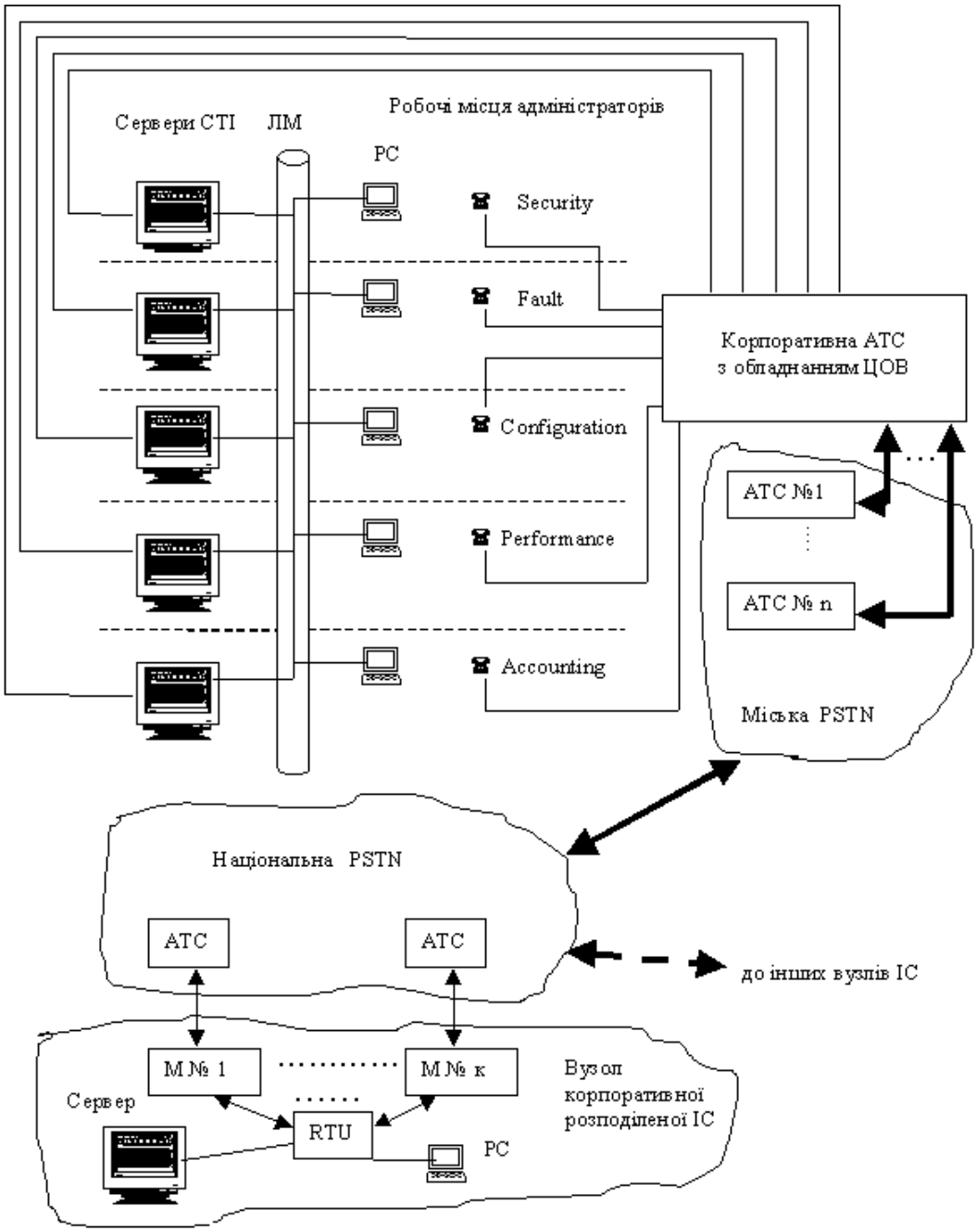
Приклад використання центра обслуговування телефонних викликів (надалі скорочено – ЦОВ) як системи централізованого керування розподіленою корпоративною телефонною системою відображений на рис. 1.

На рис. 1 видно, що як середовище транспортування технологічних сигналів мережі керування використовуються звичайні телефонні канали PSTN. Таке рішення є суттєво простішим і дешевшим, ніж побудова централізованої системи керування на базі засобів мереж пакетної комутації. При цьому найбільш поширена в телекомунікаційних мережах модель керування (згідно рекомендаціям МСЕ-Т Х.701) не порушується, тобто має застосування архітектура менеджер-агент: менеджер надає агентам команди з керуючими впливами, а агент як програмна модель керованого об'єкта виконує керуючі дії і породжує (у випадку виникнення певних подій) повідомлення від його імені. Як протокол керування прикладного рівня можливо застосувати протокол SNMP. При цьому SNMP-пакети з керуючою інформацією у віддалених вузлах вводяться та/або виводяться з аналогових телефонних каналів через стандартні аналогові модеми (М). На вузлі централізованого керування функції модуляції/демодуляції аналогових сигналів під час передавання/приймання SNMP-пакетів виконує обладнання ЦОВ. Оскільки пропускна здатність вузькосмугових аналогових телефонних каналів PSTN не є високою, то для практичного використання пропонується схема, коли кожна із п'яти функціональних підсистем керування має свій окремий канал транспортування технологічної інформації. Для цього на кожному віддаленому вузлі розподіленої ІС необхідно задіяти всього лише п'ять телефонних номерів PSTN. Це, як для задач керування, дуже недорого. Більше того, у разі потреби збільшення технологічного трафіку в цілях керування існує можливість створення додаткових транспортних каналів, якщо мати резерв номерної ємності. Контроль характеристик керованого об'єкту на і-му вузлі розподіленої ІС (у розглянутому випадку, – характеристик всіх п'яти функціональних підсистем керування, включаючи Security Management) здійснює пристрій віддаленого контролю (RTU), який може мати різні варіанти побудови, зокрема мати вигляд багатопортового стаціонарного пристрою з декількома інтерфейсними лінійними модулями (LIM). Останні під'єднуються безпосередньо до точок контролю керованого об'єкту і взаємодіють з вбудованим локальним сервером. Цей сервер виконує задачі автономного збору статистики та даних, обробки накопиченої інформації, взаємодії з іншими елементами системи в і-му вузлі тощо. Робоча станція (РС) RTU і-го вузлу, в свою чергу, вирішує задачі безпосереднього управління пристроєм RTU, візуалізації даних, накопичених в RTU, завантаження необхідних файлів з даними та програмними модулями.

З метою підвищення захищеності каналів керування як модеми RTU, так і порти ЦОВ можуть бути під'єднані паралельно до різних місцевих АТС. У найпростішому випадку, – до двох різних АТС (див. рис. 1). Тоді якщо потрібно підвищити показники цілісності або живучості системи керування, транспортні канали з технологічною інформацією дублюють, тобто одну і ту ж керуючу інформацію транспортують через різні АТС. Якщо ж необхідно підвищити показники конфіденційності технологічної інформації, то поток пакетів з цією інформацією розбивається на два і більше підпотоків, які транспортуються паралельно різними шляхами, тобто через різні АТС.

Як технічну платформу для побудови системи централізованого керування територіально розгалуженою ІС є можливим використати мультимедійний аналог ЦОВ – так званий контакт-центр. Контакт-центр – це є інтегроване прикладне середовище, яке створюється на базі певним шляхом вибраного штатного програмно-апаратного комплексу ЦОВ, що дозволяє забезпечити надання спеціалізованих мультимедійних послуг через різноманітні канали зв'язку (у т. ч., і через канали Інтернет) у реальному часі з використанням єдиної точки стикання потоку викликів з інтелектуальним ресурсом цього центру. Під інтелектуальним ресурсом

розуміються, перш за все, фахові можливості операторів контакт-центру, зміцнені технічними можливостями його програмних та апаратних засобів. Прикладні застосування контакт-центрів використовують, головним чином, гнучку та масштабовану архітектуру "клієнт-сервер", забезпечують комбіновану обробку даних, голосу та відео, у т. ч. і в режимах інтерактивної мультимедійної взаємодії незалежно від географічного розташування клієнтів центру. Контакт-центр є універсальним засобом обробки інформаційних потоків, оскільки:



Позначення : CTI – комп'ютерно- телефонна інтеграція; ЛМ – локальна мережа;
PC- робоча станція; М - модем аналогових ліній;
ЦОВ - центр обслуговування телефонних викликів;
PSTN - телефонна мережа загального користування;
RTU – пристрій віддаленого контролю;

Рисунок 1 – Архітектура централізованого керування через канали PSTN

підтримує стандартні протоколи взаємодії з більшістю видів телекомунікаційних мереж (телефонних, Інтернет, IP-телефонії, ISDN, IN, Frame Relay, ATM, стільникового зв'язку тощо);

надає будь-яку інформацію в межах предметного застосування, на яке він налаштований;

забезпечує незалежність використаних програмно-апаратних рішень від галузі призначення контакт-центру.

Сьогодні пропонується широкий вибір продуктів, призначених для побудови контакт-центрів і їх кількість стрімко зростає.

Вищезазначене дозволяє на базі контакт-центру створювати економічно ефективні рішення, у т. ч. і в сфері керування комплексними системами ТЗІ у розподілених ІС.

IV Висновки

1. На базі програмно-апаратних платформ центрів обслуговування телефонних викликів у багатьох практично важливих застосуваннях можлива економічно обгрунтована побудова центрів керування територіально розподіленими ІС, включаючи побудову підсистем керування комплексними системами ТЗІ.

2. Як канали транспортування технологічної інформації в централізованих системах керування, створюваних на основі ЦОВ, можливо і у багатьох випадках доцільно застосувати стандартні комутовані канали телефонної мережі загального використання. Це спрощує і здешевлює побудову систем керування, а також підвищує захищеність технологічної інформації, що в них циркулює.

3. Шляхом підключення аналогових портів ЦОВ та/або пристроїв віддаленого контролю до різних територіально рознесених АТС забезпечується можливість економічно ефективного внесення апаратної надлишковості з метою адаптивного перерозподілу ресурсів в задачах керування засобами ТЗІ.

4. Для побудови систем централізованого керування складними ІС, створеними на основі гетерогенних мереж, доцільно використовувати мультимедійні програмно-апаратні пристрої обслуговування викликів (так звані контакт-центри).

Література: ***1****. William C. Goers, Michael R. Brenner. Implementing a Management System Architecture Framework / Bell Labs Technical Journal. – October-December, 2000. – 31-43 p.* ***2.*** *International Telecommunication Union, Rec. M.3010. Principles for a Telecommunications Management Network (TMN). – May,1996.* ***3****. Tele-Management Forum, Document GB910, Version 2.1. Telecom Operations Map. – Mart, 2000.*

УДК 004.056.53

ОБ ОДНОМ ПОДХОДЕ К ПОСТРОЕНИЮ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ НА КОМПАКТ-ДИСКАХ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

Виталий Носов, Александр Манжай

Национальный университет внутренних дел, г. Харьков

Анотація: **Пропонується один з підходів до побудови системи захисту компакт-дисків від несанкціонованого копіювання.**

Summary: **One of the approaches to construction the compact discs protection system against the non-authorized copying is offered.**

Ключевые слова: **Система защиты, несанкционированное копирование, компакт-диск.**

I Введение

На современном этапе развития общества, когда информационные отношения формируют, по сути, новую сферу экономики, становится актуальным вопрос об эффективной системе защиты права собственности на информацию.

Принятие в 2001 г. нового Уголовного кодекса Украины стало в нашей стране важным этапом в борьбе с компьютерными преступлениями. Правоохранительными органами был проведен ряд мероприятий по предупреждению, раскрытию и расследованию такого рода преступлений. Однако принятые меры носят, как правило, административный характер, что не позволяет достаточно эффективно противостоять киберпреступности. Вместе с тем кроме организационных мер целесообразно применять и так называемые программно-технические методы и средства защиты с целью повышения защищенности хранимой