на основе аналоговых параллельных корреляторов с использованием одного из каналов в целях синхронизации. Данное решение позволит приблизить параметры системы к теоретически достижимому пределу улучшения соотношения Сигнал/Шум. Выбор и построение всей функциональной структуры системы связи на основе шумоподоб- ных сигналов потребует решения множества иных, не менее важных вопросов, среди которых разработка протокола работы системы, организация эфирного трафика, синхронизация работы базовых ретрансляторов, оперативный контроль мощностей пользовательских станций, оптимальное распределение конкретных псевдослучайных последовательностей, а так же многое другое. Следует заметить, что по мнению авторов статьи наиболее соответствующая целям оперативной скрытой подвижной радиосвязи является такая организация системы, при которой имеется возможность проведения сеансов связи как непосредственно напрямую между несколькими мобильными терминалами в режиме симплекса, так и через базовые ретрансляторы в дуплексном режиме. Так же необходимо предусмотреть ситуацию при которой может возникнуть необходимость резкого повышения вероятности получения и передачи информации, к примеру, в случае преднамеренной постановки помех. Для этого в системе связи должна быть предусмотрена возможность передачи текстовых сообщений и специальных команд с относительно невысокой скоростью данных. За счёт использования одной и той же частотной полосы и большей базы сигнала становится возможным без возрастания мощности передачи значительно увеличить дальность связи по сравнению с основным режимом работы. Если же в увеличении дальности нет непосредственной необходимости, то данный режим работы позволит в целях повышения скрытности существенно уменьшить мощность передатчика и, следовательно, его спектральную плотность.

Поступила 29.07.2002
После доработки 3.09.2002

УДК 654.1(045)

*Г.Ф. Конахович, О.М. Сухопара*

## АНАЛІЗ ПРИНЦИПІВ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ПІДСИСТЕМ КЕРУВАННЯ ГЛОБАЛЬНИХ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ

Питання побудови систем керування мультисервісними мережами знаходяться в центрі уваги багатьох компаній, що займаються організацією доступу до всесвітньої мережі Інтернет, наданням послуг передачі даних, а також іншими видами діяльності, так чи інакше пов'язаними з використанням телекомунікаційних технологій.

Поточний стан українського операторського ринку такий, що головну увагу оператори змушені приділяти економічним факторам своєї діяльності поряд з постійним удосконалюванням технологій надання послуг. Гостра конкуренція продовжує залишатися рушійною силою впровадження в існуючі системи прогресивних технічних і технологічних рішень. Саме цим обумовлене підвищення інтересу до складних систем керування розподіленими гетерогенними мережами, зокрема до однієї з найважливіших функцій таких систем – керування безпекою.

У вітчизняних виданнях, присвячених проблемам використання телекомунікаційного обладнання, можна відшукати значну кількість публікацій, що висвітлюють ті чи інші аспекти захисту мереж передачі даних (МПД) від несанкціонованого доступу (НСД). В цих публікаціях розглядаються, як правило, проблеми захисту від НСД локальних

обчислювальних мереж (ЛОМ), що мають у своєму складі відносно невелику кількість вузлів. Проблеми захисту систем керування глобальними МПД національного рівня, які розгортаються останнім часом деякими українськими операторами, на думку авторів, висвітлені недостатньо.

В даній статті запропоновано аналіз принципів захисту від несанкціонованого доступу підсистем керування глобальних мереж передачі даних.

У сучасних телекомунікаційних мережах більшості компаній-операторів використовується відразу кілька телекомунікаційних технологій – IP, X.25, ATM, Frame Relay, SDH, PDH. Крім того, починають застосовуватися технології MPLS, xDSL і DWDM. Широко застосовуються технології конвергенції для передачі через існуючі магістралі голосової і мультимедійної інформації в реальному масштабі часу.

Спектр використовуваного в операторських мережах устаткування сьогодні дуже широкий – це, насамперед, обладнання таких широко відомих компаній як Cisco, Nortel, Lucent, Avaya, Ericsson, Siemens, Alcatel, Newbridge і багатьох інших. Одночасне застосування в складі телекомунікаційної інфраструктури обладнання хоча б кількох з них породжує нетривіальну задачу із створення ефективного механізму керування цим великим і досить різноманітним парком пристроїв.

Обмеженість ресурсів не дозволяє на кожному з вузлів мережі тримати персонал, який має потрібні знання та досвід роботи з усіма наявними типами обладнання. З економічної точки зори більш доцільно створити так званий центр керування мережею, в якому розмістити програмно-апаратні засоби централізованої системи управління (ЦСУ) МПД та невелику команду висококваліфікованих фахівців, що виконували б всі функції з експлуатації обладнання вузлів мережі.

У випадку, коли ієрархічна функціонально-організаційна структура МПД налічує відносно велику кількість рівнів вузлів (більше 3), доцільно виконувати централізоване керування лише тими вузлами мережі, які виконують обробку транзитного трафіку користувачів або безпосередньо задіяні у наданні послуг прикладного рівня (служби передача файлів, бази даних, електронна пошта). Керування вузлами мережі, які виконують тільки концентрацію та мультиплексування абонентського трафіку, доцільно здійснювати засобами локальних підсистем управління (ЛПУ) обладнанням, яке встановлене на цих вузлах. Така структура керування МПД забезпечить оптимальне співвідношення між централізацією та децентралізацією функцій управління мережею за критерієм мінімуму затрат на їх реалізацію та експлуатацію.

Очевидно, що віддалене керування обладнанням вузлів мережі має значні переваги з точки зору мінімізації витрат оператора на експлуатацію МПД, але є небажаним з точки зору захисту інформаційних ресурсів систем управління мережею від НСД. Існує протиріччя між необхідністю обмеження доступу до будь-яких підсистем обладнання вузлів мережі до мінімально можливого рівня і повним необмеженим доступом до цього обладнання, чого потребує віддалене централізоване керування. Якщо під час організації віддаленого доступу до елементів МПД не вжити необхідних заходів із забезпечення безпеки інформаційних ресурсів, то в процесі експлуатації мережі можуть бути реалізовані загрози технологічній інформації, яка зберігається в системах керування, в керованих об'єктах та циркулює в каналах зв'язку, тобто може відбутися порушення конфіденційності, цілісності та (або) доступності цієї інформації.

На протязі останніх 10 років відбувається стрімкий розвиток телекомунікаційних мереж і їхніх елементів, який набагато випереджає здатність експлуатаційного програмного забезпечення керувати сучасними глобальними мережами передачі даних. У результаті розробляються тимчасові рішення для функціональних компонентів систем управління, що заміняють в разі потреби застарілі або відсутні блоки. Функціональні модулі, у деяких випадках, розробляються силами самих операторів, що вимагає великих фінансових витрат і безпрецедентної кількості зусиль для їхньої інтеграції.

Використання відкритих програмних інтерфейсів (API) і стандартизація систем не змогли повністю вирішити проблему їхньої взаємодії. Застосування нових технологій, таких як Common Object Request Broker Architecture (CORBA), Distributed Common Object Model (DCOM), Lightweight Directory Access Protocol (LDAP) і Extensible Markup Language (XML), дещо покращило ситуацію але усе ще необхідна "ручна" інтеграція функціональних модулів систем управління. У більшості випадків на практиці після завершення інтеграції додавання нових програмних компонентів без порушення роботи всієї системи усе ще є неможливим.

Така ситуація веде до зменшення прозорості роботи системи управління, зниження ефективності керування мережею і, в решті решт, до виникнення нових загроз інформаційним ресурсам систем управління. Тому під час вибору обладнання вузлів МПД та програмно-апаратних засобів систем управління необхідно звернути особливу увагу на можливість їх "безболісної" інтеграції.

Задачі із керування конфігурацією обладнання вузлів МПД та виявлення спроб НСД до цього обладнання, як правило, вирішуються програмно-апаратними засобами системи централізованого керування мережею та засобами локальних підсистем керування обладнанням вузлів мережі. В багатьох випадках використовують також спеціалізоване позаштатне обладнання, наприклад, міжмережні екрани (Firewalls), системи виявлення вторгнень (Intrusion Detection Systems) і багато іншого.

Виявлення спроб НСД до ЦСУ МПД, а також до ЛПУ обладнанням, яке розміщене на вузлах мережі, здійснюється шляхом:

- контролю відповідності розподілу прав доступу зареєстрованих суб'єктів до захищених об'єктів, що зафіксовані у вигляді призначених міток доступу або у відповідних матрицях доступу систем управління доступом;
- моніторингу дій користувачів систем управління (тобто, адміністраторів із числа персоналу оператора мережі) і реакції цих систем на нештатні дії суб'єктів доступу.

Правила розподілу прав доступу і фактичний розподіл цих прав між санкціонованими суб'єктами доступу до централізованої системи і локальних підсистем управління обладнанням (тобто, між персоналом оператора мережі, який є користувачем ресурсів цієї системи і цих підсистем управління) визначаються прийнятою політикою безпеки інформаційних ресурсів МПД.

Централізована система управління МПД, а також локальні підсистеми управління обладнанням мережі надають експлуатаційному персоналу оператора послуги із захисту об'єктів від порушень конфіденційності, цілісності та доступності інформаційних ресурсів контрольованого обладнання.

Як ЦСУ, так і ЛПУ контрольованим обладнанням МПД реалізують адміністративний принцип керування, при якому інстальовані засоби захисту дозволяють керувати потоками інформації між суб'єктами та об'єктами тільки спеціально уповноваженим авторизованим користувачам.

В більшості випадків застосовується механізм визначення прав доступу, коли у вигляді атрибутів доступу використовуються мітки, що відображають міру конфіденційності або важливості інформації (об'єкта), з одного боку, і рівень доступу користувача, з другого. Таким чином, на підставі порівняння міток об'єкта і суб'єкта визначається, чи є суб'єкт, що запитує інформацію, авторизованим користувачем.

Інший більш детальний механізм визначення прав доступу базується на використанні концепції матриці доступу. Матриця доступу являє собою паралелепіпед, уздовж кожного виміру котрого відкладені ідентифікатори відповідно суб'єктів доступу, об'єктів і механізмів (засобів) захисту, а в якості елементів матриці виступають дозволені або заборонені режими доступу (наприклад, тільки на читання, на запис і читання і т. ін.). Повна тримірна матриця

доступу дозволяє точно описати, хто (ідентифікатор суб'єкта) через що (ідентифікатор механізму захисту) до чого (ідентифікатор об'єкта захисту) і який режим доступу може одержати.

Система, що заснована на адміністративному принципі керування доступом, дозволяє встановлювати потоки інформації всередині системи тільки уповноваженій особі. Ці потоки не можуть бути змінені без санкції цієї особи. Звичайний користувач не має легальних можливостей ні за яких умов змінювати мітки та інші атрибути доступу об'єктів та суб'єктів. Зона захисту інформаційних ресурсів (або так званий контур безпеки) обладнання, що охоплюється засобами ЦСУ, фактично складається із локальних зон захисту кожного із охоплених маршрутизаторів, комутаторів, серверів тощо.

Об'єктами захисту у кожній із локальних зон захисту є:

- поточна конфігурація програмно-апаратних засобів контрольованого обладнання (у т. ч., штатних засобів захисту);
- інформація, яка міститься в таблицях маршрутизації контрольованого обладнання;
- інформація автентифікації авторизованих суб'єктів доступу (паролі, PIN-коди тощо), ідентифікатори та інші атрибути доступу об'єктів захисту;
- матриця доступу суб'єктів до об'єктів або таблиця з встановленими мітками доступу для суб'єктів та об'єктів;
- правила зміни атрибутів доступу;
- правила створення нових суб'єктів та об'єктів доступу;
- правила експорту та імпорту об'єктів доступу;
- умови реєстрації та генерації контрольованих подій відповідно до визначеної політики безпеки обладнання;
- журнали реєстрації контрольованих подій;
- порогові значення показників, при перевищенні котрих мають надсилатися повідомлення на робочу консоль та до централізованої системи керування про кількість спроб НСД;
- поточні статистичні дані щодо характеристик протокольних блоків, які оброблялись портами контрольованого обладнання, кількість збоїв тощо;
- визначені згідно з політикою безпеки обладнання дані про об'єкти захисту, які необхідно зберігати на протязі певного проміжку часу у так званому "history" файлі.

Через те, що адміністратори мають привілейований доступ до керованого ними обладнання вузлів МПД, надзвичайно важливо, щоб було проведено організаційно-технічні заходи із захисту всього обладнання, яке використовується впродовж сесії віддаленого керування. Захисту потребує не лише кероване обладнання МПД, але й інформаційні ресурси станцій керування ЦСУ і ЛПУ та технологічна інформація керування, яка передається через канали зв'язку. Захист інформації абонентів мережі у каналах зв'язку, як правило, не здійснюється.

Для захисту технологічної інформації, яка передається між контрольованим обладнанням вузлів мережі та програмно-апаратними засобами ЦСУ через відкриті канали

впродовж сесії віддаленого керування, можуть використовуватися різні механізми, наприклад шифрування даних у каналі засобами протоколу SSL (Secure Socket Layer), фільтрація IP-пакетів, виявлення спроб здійснення атак та блокування IP-адрес порушників тощо. Останнім часом поширюється використання технологій побудови віртуальних приватних мереж (Virtual Private Networks – VPN) з використанням протоколів IPSec, L2TP, PPTP.

Призначенням протоколу SSL є забезпечення захисту інформації керування під час її передачі між контрольованим обладнанням вузлів МПД та ЦСУ. Протокол розділений на два рівні (підпротоколи). На нижчому рівні, розташованому над певним орієнтованим на з'єднання протоколом транспортного рівня (наприклад, TCP), використовується так званий SSL Record Protocol. Він призначений для інкапсуляції даних протоколів прикладного рівня, таких як HTTP, SMTP, POP тощо. Одним з таких протоколів, що інкапсулюються в SSL Record Protocol є SSL Handshake Protocol. Він дозволяє виконувати взаємну автентифікацію сторін, що приймають участь у створенні захищеного каналу та узгоджувати алгоритми шифрування та криптографічні ключі, які будуть використовуватися впродовж сеансу зв'язку. Для шифрації даних протоколом SSL можуть використовуватися різні симетричні криптоалгоритми, наприклад AES, DES, RC4. Автентифікація сторін виконується засобами асиметричних криптоалгоритмів (RSA, DSS). Цілісність даних під час їхньої передачі через мережі загального користування забезпечується шляхом використання хеш-функцій, наприклад SHA, MD5.

Протокол PPTP дозволяє створювати захищені канали для обміну даними через мережі, що створені з використанням різних протоколів – IP, IPX або NetBEUI. Дані цих протоколів інкапсулюються за допомогою протоколу PPTP у пакети протоколу мережного рівня, наприклад IP, за допомогою якого ці пакети переносяться у зашифрованому виді через будь-яку мережу TCP/IP. Як правило, інкапсулюється вихідний кадр PPP, тому протокол PPTP можна віднести до класу протоколів інкапсуляції канального рівня в мережний.
Багатопротокольність – основна перевага інкапсулюючих протоколів канального рівня, до яких відноситься протокол PPTP. Протокол SSL орієнтується на протокол тільки мережного рівня – IP. До того ж розміщення протоколу захищеного каналу безпосередньо під прикладним рівнем (за моделлю OSI) вимагає модифікації програмного забезпечення. Захист даних на канальному рівні робить засоби захисту прозорими як для протоколів прикладного рівня, так і для протоколів мережного рівня.

Існують також і варіанти вбудовування засобів створення захищеного каналу на мережному рівні. Мається кілька протоколів цього типу, що використовують шифрування й інкапсуляцію протоколу мережного рівня в мережний. Для захисту даних у IP-мережах розроблена захищена версія протоколу IP, що найчастіше називають IPSec. Цей протокол підтримує автентифікацію на мережному рівні, а також може виконувати шифрування даних користувача. Протокол IPSec не визначає жорстко, які методи шифрування повинні використовуватися для автентифікації і створення захищеного каналу, хоча для перших реалізацій визначений варіант IPSec, що використовує хеш-функцію MD5 для автентифікації й алгоритм шифрування DES для утворення захищеного каналу. Недоліком протоколу IPSec є те, що він працює тільки в IP-мережах і не визначає спосіб захищеного транспортування пакетів інших протоколів. Цей недолік усувають такі протоколи, як PPTP або L2F.

Керування мережним обладнанням (наприклад, маршрутизаторами, комутаторами, серверами, DSU/CSU тощо), яке розташоване у віддалених вузлах МПД і від працездатності якого залежить коректність роботи мережі, є ключовим елементом експлуатації сучасних мультисервісних мереж. Для віддаленого доступу, як правило, використовуються системи управління, що ґрунтуються на протоколі SNMP та (або) інших протоколах стеку із TCP/IP. В цьому випадку технологічна інформація керування передається через ті ж самі канали зв'язку, що й інформація абонентів МПД. Такий тип керування має назву In-band керування.

В разі виходу з ладу каналу зв'язку між керованим вузлом МПД та ЦСУ або при виникненні порушення доступності керованого обладнання з інших причин персонал центра керування втрачає контроль над цим обладнанням. Для запобігання таким ситуаціям доцільно використовувати системи управління типу Out-of-band.

Система управління типу Out-of-band дозволяє персоналу оператора мережі отримувати віддалений доступ до системних консолей (портів RS-232, AUX тощо) критичного обладнання вузлів МПД через виділені канали зв'язку, які призначені виключно для цілей керування. Крім підвищення надійності мережі та ефективності її експлуатації такий підхід дозволяє збільшити захищеність інформаційних ресурсів підсистем керування МПД від НСД, оскільки технологічна інформація керування фізично відокремлена від інформації абонентів.

Проаналізувавши особливості захисту від несанкціонованого доступу інформаційних ресурсів глобальних мультисервісних мереж національного рівня, можна зробити висновок, що внаслідок широкого застосування персоналом операторів МПД віддаленого керування обладнанням вузлів цих мереж можуть бути реалізовані специфічні загрози технологічній інформації керування, яка обробляється та зберігається в системах управління, в керованих об'єктах та циркулює в каналах зв'язку. Для запобігання порушенням конфіденційності, цілісності та (або) доступності інформації через реалізацію цих загроз необхідно у повній мірі використовувати можливості штатних систем ТЗІ обладнання вузів мережі, можливості позаштатного обладнання, а також тісно інтегрувати ці засоби у єдину підсистему керування безпекою. Особливу увагу слід звернути на коректність роботи механізмів розподілу прав доступу до систем управління. При передачі технологічної інформації між контрольованим обладнанням вузлів мережі та програмно-апаратними засобами ЦСУ впродовж сесії віддаленого керування необхідно використовувати захищені канали зв'язку. В особливих випадках для підвищення надійності мережі та збільшення захищеності інформаційних ресурсів підсистем керування МПД від НСД слід використовувати системи керування типу Out-of-band.

## ЛІТЕРАТУРА

1. Компьютерные сети. Принципы, технологии, протоколы. *Олифер В.Г., Олифер Н.А.* – СПб: Питер, 2001. – 672 с.: ил.

2. Атака на Internet – 3-е изд., стер. *Медведовский И.Д., Семьянов П.В., Леонов Д.Г.* – М.: ДМК, 2000. – 336 с.: ил.

3. *Stephen L. Packard, Archie D. Andrews*, "Remote System Administration", ATI IPT Special Report, April 2000, <http://ips.aticorp.org>.

Надійшла 10.07.2002

УДК 004.56.021.2: 510.22 (045)

А.Г. Корченко, к.т.н., В.В. Душеба, к.т.н., В.А. Рындюк, Е.В. Пацира

## ИССЛЕДОВАНИЕ МЕТОДОВ ОБРАБОТКИ ТОЛЕРАНТНЫХ НЕЧЕТКИХ ЧИСЕЛ ДЛЯ ПРИМЕНЕНИЯ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Определение состояния безопасности информационной системы в настоящее время является одним из наиболее распространенных классов задач, в которых немаловажное место уделяется проблеммам принятия решений. На практике часто принятие решений