УДК 621.396

А.М. Носик

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖАХ АТМ

Проведений аналіз послуг і механізмів захисту інформації при передачі її по каналам за технологією АТМ. Виходячи з аналізу загроз безпеки визначена архітектура об'єктів захисту та загроз безпеки мереж АТМ. Розроблено механізм захисту від несанкціонованого доступу в мережах АТМ. Представлена класифікація загроз захищеності АТМ мережі відповідно до форматів полів заголовків протокольних блоків. Розроблено механізм захисту від несанкціонованого доступу адресних і керуючих полів заголовків АТМ чарунок з метою забезпечення захищеності з'єднань користувачів по цілісності, функціональності й конфіденційності переданої інформації. На основі проведеного аналізу вироблені пропозиції щодо захисту інформації за технологією АТМ.

Ключові слова: *технологія АТМ, захист інформації, загрози безпеки.*

Вступ

Постановка проблеми та аналіз останніх досліджень. У цей час все більше значення в практиці побудови розподілених інформаційних систем отримують питання інтеграції мережних служб у рамках єдиних технологій, що дозволяють уніфікувати засоби побудови мереж передачі даних стосовно до широкого спектра інформаційних. Розробка й впровадження технології асинхронної передачі, заснованої на швидкій пакетній комутації трафіку телекомунікаційних служб, спрямоване на підвищення ефективності використання існуючих високопродуктивних каналів фізичної передачі даних. Мережі з асинхронним режимом передачі (Asynchronous Transfer Mode, ATM), забезпечують універсальні засоби магістральних мереж передачі даних, що дозволяють транспортувати користувальницькі повідомлення в рамках телекомунікаційних служб, які істотно різняться по вимогах семантичної, часової й логічної прозорості.

Основні проблеми сучасного етапу розвитку засобів автоматизації процесів інформаційного обміну, включаючи засоби зв'язку й телекомунікацій, пов'язані із істотним зростанням складності науково-технічних розробок в галузі інформаційних технологій. Внаслідок цього технічні засоби потенційно містять у собі велику кількість помилок і нерегламентованих можливостей, які можуть бути використані зловмисниками [1 – 3]. Отже, будь-які програмно-апаратні рішення повинні ретельно аналізуватися на предмет потенційних загроз безпеки, а адекватний рівень оснащеності засобами захисту – постійно переглядатися [4, 5]. Важлива властивість розподілених інформаційних систем полягає в тому, що ступінь їхньої критичності до зовнішніх і внутрішніх порушень зростає швидше, ніж функціональність, що забезпечується обраним рівнем складності й вартості. Іншими словами, можливі ситуації, коли вартість забезпечення заданого рівня стійкості системи стосовно зовнішніх загроз виявляється порівнянною або навіть вище вартості самої системи.

Метою статті є розробка пропозицій щодо захисту інформації при передачі її по каналам за технологією АТМ виходячи з аналізу загроз безпеки.

Виклад основного матеріалу

Мережі з інтеграцією послуг, які називаються широкосмуговими мережами B-ISDN (Broadband Integrated Service Digital Networks) описують функції АТМ за допомогою багаторівневої еталонної моделі, аналогічної 7-рівневій архітектурі взаємозв'язку відкритих систем (OSI). Еталонна модель протоколу B-ISDN дає нове визначення трьом нижнім рівням: фізичний рівень, рівень АТМ (канальний рівень) і рівень адаптації АТМ (мережевий рівень). Нижні рівні характеризуються більшою інтенсивністю апаратних засобів, тоді як вищі рівні характеризуються вищою інтенсивністю програмного забезпечення і пов'язані з конкретними прикладними системами користувача (на устаткуванні користувача), які обслуговуються рівнями АТМ.

Для аналізу загроз мереж передачі даних, реалізованих з використанням засобів технології АТМ, розглянемо структуру розгалуженої відомчої мережі (ВМ), інтеграція окремих сегментів якої реалізується з використанням технічних засобів АТМ технології (рис. 1).

У рамках структури можуть бути виділені наступні рівні інформаційної взаємодії:

1. Доступ локального сегмента ВМ до транспортної мережі передачі даних у рамках нижніх рівнів протоколів АТМ. Реалізується АТМ комутатором прикордонної ділянки транспортної мережі.

2. Транспортна мережа передачі даних. Реалізується мережею магістральних АТМ – комутаторів

оператора зв'язку.

3. Сегмент локальної обчислювальної мережі (ЛОМ) ВМ, що підключається до прикордонного комутатора за допомогою мосту АТМ-ЛОМ.

4. Рівень доступу телекомунікаційних служб мережі без встановлення з'єднання.

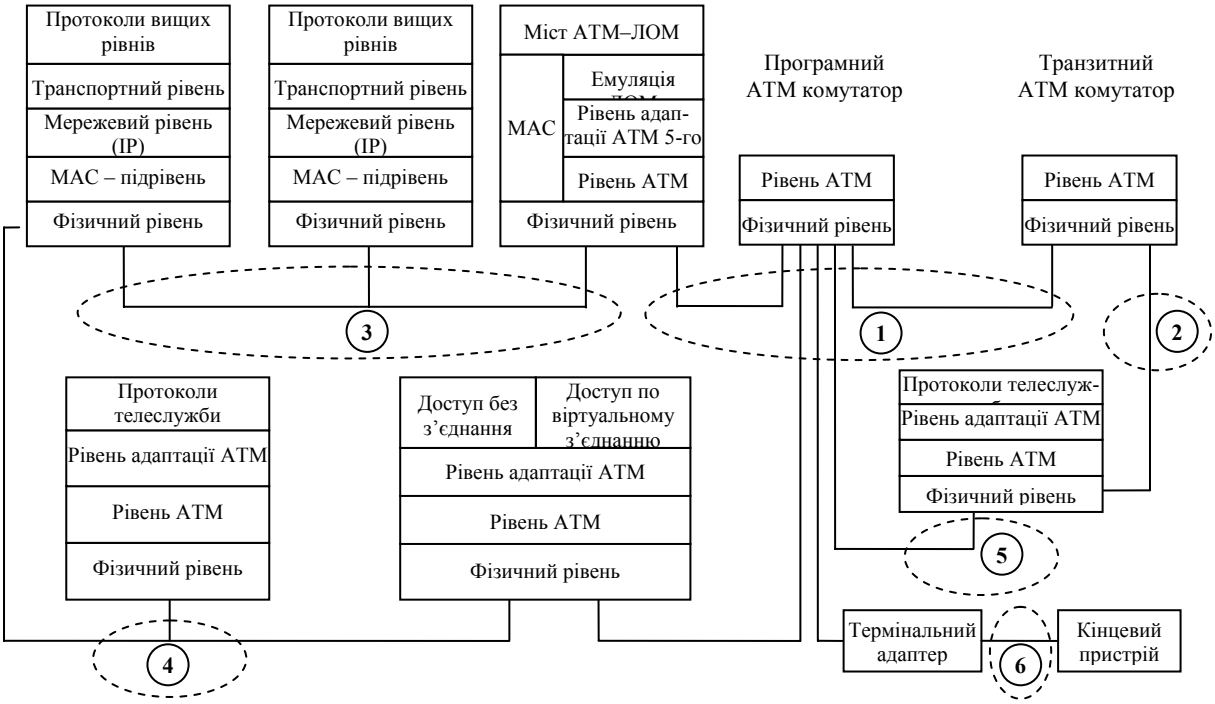

Рис. 1. Архітектура об'єктів захисту в технології АТМ

5. Рівень стандартного широкосмугового стику мережі АТМ. (Служби передачі відео/аудіо в реальному масштабі часу.)

6. Рівень стандартного вузькосмугового стику цифрових синхронних каналів. Реалізується термінальними адаптерами на виході лінійного закінчення середовища передачі мережі АТМ. На даному рівні до ВМ можуть бути підключені стандартні ISDN-сумісні телефонні служби.

Відповідно до точок концентрації інформаційних потоків (рис. 1) на рис. 2. наведено класифікацію суб'єктів загрози [2, 3].

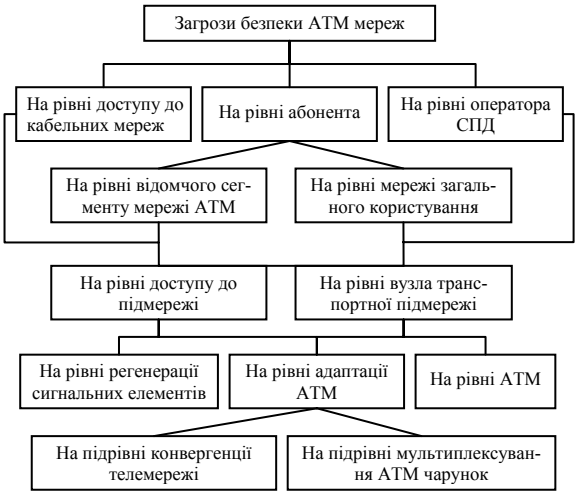

Рис. 2. Класифікація суб'єктів загрози

У загальному випадку точки потенційної загрози класифікуються по просторово-топологічним (горизонтальні зв'язки) і по протокольно-логічним (вертикальні зв'язки) ознакам. Горизонтальна й вертикальна складові загроз взаємозалежні між собою. Наприклад, діючи на вищих рівнях OSI/ISO, порушник із числа абонентів зовнішньої АТМ-підмережі може одержати несанкціонований доступ до мережної станції ВМ, внаслідок чого точка загрози переміститься у вихідну ВМ. З іншого боку, залежно від точки концентрації інформаційних потоків ВМ, що є об'єктом нападу, є можливість використання різних протокольних стеків для одержання доступу до інформаційних ресурсів різних рівнів OSI/ISO.

З огляду на вищесказане, доцільно обмежитися розглядом класифікації загроз і порушників або по просторово-топологічним, або по протокольно-логічним ознакам. Оскільки архітектура корпоративних мереж і окремих транспортних підмереж передачі даних істотно різниться, доцільно розглянути загрози на рівні протоколів АТМ, що є стандартними й незалежними від конкретних мережевих архітектур.

На рис. 3 представлена структура протокольного стеку мережі АТМ.

Як показано на рис. 3, структура протокольного стеку мережі АТМ містить у собі [4, 5]:

– фізичний рівень, на якому визначаються параметри інформаційного потоку, що транспортується безпосередньо через передаюче середовище;

– рівень АТМ на передавальній стороні вико-

ристовується для мультиплексування вихідного потоку чарунок АТМ у єдиний бітовий інформаційний потік, переданий на фізичний рівень. З метою зниження ймовірності перекручування адресних частин АТМ чарунок і запобігання помилок неправильної маршрутизації на прийомній стороні виконується контроль вмісту заголовків АТМ чарунок CRC кодом. У випадку відсутності помилок уміст поля даних передається на рівень адаптації. У противному випадку чарунка знищується;

– рівень АТМ на передавальній стороні використовується для мультиплексування вихідного потоку чарунок АТМ у єдиний бітовий інформаційний потік, переданий на фізичний рівень. З метою зниження ймовірності перекручування адресних частин АТМ чарунок і запобігання помилок неправильної маршрутизації на прийомній стороні виконується контроль вмісту заголовків АТМ чарунок CRC кодом. У випадку відсутності помилок уміст поля даних передається на рівень адаптації. У противному випадку чарунка знищується;

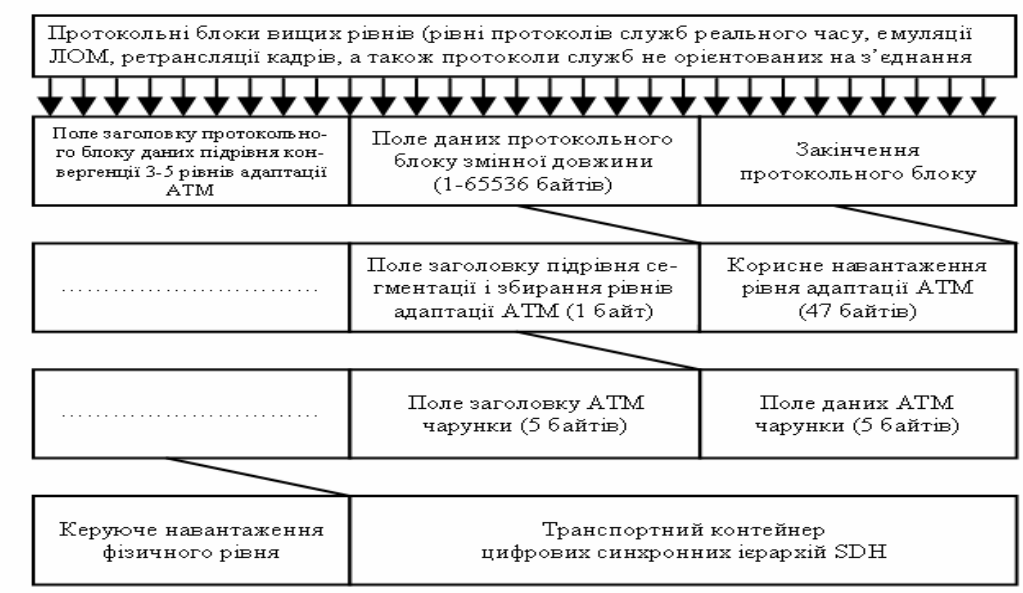

Рис. 3. Рівні інкапсуляції заголовків протокольного стеку мережі АТМ

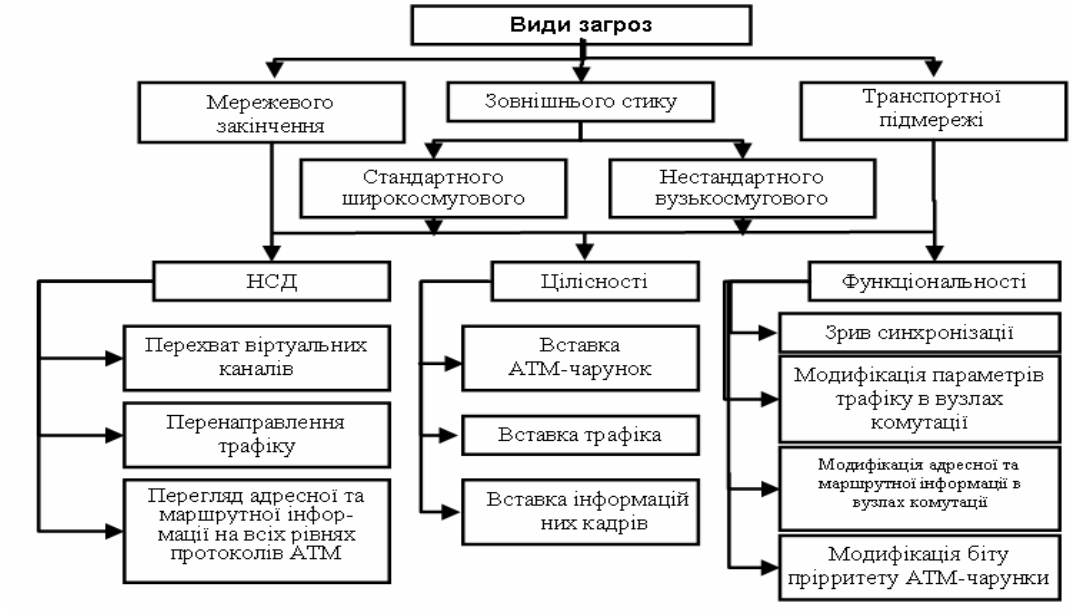

Рис. 4. Класифікація загроз захищеності АТМ

– рівень сегментації й складання підрівня адаптації АТМ сегментує вхідний інформаційний блок рівня конвергенції на фрагменти довжиною 47 байтів і передає їх на рівень АТМ. На прийомній стороні перевіряються ідентифікатори віртуального шляху й віртуального каналу. Якщо вони коректні, то вміст поля даних АТМ чарунки передається на рівень конвергенції телеслужби. У противному випадку чарунка знищується;

– рівень конвергенції телеслужби здійснює пе-

ретворення вхідного трафіку у форму, придатну для використання в конкретній телеслужбі.

На рис. 4 представлена класифікація загроз захищеності АТМ ВМ відповідно до форматів полів заголовків протокольних блоків, наведених у попередньому рисунку [6].

У загальному випадку можуть бути виділені три типи загроз [3]:

– загрози цілісності;

– загрози функціональності;

– загрози несанкціонованого доступу (НСД).

Загрози функціональності пов'язані з можливістю втрати необхідного рівня обслуговування клієнта ВМ або повним блокуванням доступу до ресурсу в результаті дії порушника. Подібні дії можуть бути викликані:

– зривом синхронізації бітового потоку на рівні прийомопередаючих пристроїв шляхом руйнування або перекручування прапорів регенераторної й службової секції в кадрах фізичного рівня;

– зривом синхронізації потоку чарунок АТМ шляхом періодичного перекручування значень контрольних сум заголовків чарунок;

– модифікацією маршрутної й адресної інформації в керуючих серверах проміжних комутаційних вузлів. Результатом подібних дій може бути, наприклад, відмова в з'єднанні клієнтові ВМ;

– модифікацією параметрів трафіку в кінцевих вузлах транспортної мережі. Це може негативно позначитися на якості обслуговування клієнтів відомчої мережі;

– модифікацією бітів пріоритету в АТМ чарунках.

Загрози цілісності пов'язані зі зміною інформаційного змісту протокольних блоків даних, переданих по мережі й можуть містити в собі:

– вставку або вилучення АТМ чарунок у вузлах комутації транспортної мережі. При цьому можливі різні варіанти втрат від перекручування інформаційних блоків даних до порушення роботи служб сигналізації й експлуатації мережі;

– вставку трафіку, у результаті якої по обраному віртуальному з'єднанню можлива несанкціонована передача інформації третіми особами.

Загрози НСД пов'язані з можливістю аналізу інформаційного змісту полів даних і керуючих заголовків протокольних блоків, переданих від джерела до приймача [3]. До даної групи можуть бути віднесені:

– перенаправлення трафіку з метою наступного аналізу його інформаційного змісту;

– перехоплення діючого віртуального з'єднання без перехоплення напрямку трафіку;

– несанкціонований перегляд діагностичних повідомлень служб керування й моніторингу мережі з метою аналізу статистики параметрів трафіку або-нентів ВМ.

Беручи до уваги висновки з аналізу загроз безпеки стосовно мереж АТМ, розробимо механізм, що забезпечить захист від НСД адресних і керуючих полів заголовків АТМ чарунок за рахунок чого забезпечимо захищеність з'єднань користувачів по цілісності, функціональності й конфіденційності переданої інформації.

Ефективним механізмом вирішення проблеми захисту від НСД адресних і керуючих полів заголовків АТМ чарунок і в той же час боротьби з пачечністю помилок, що виникають в каналі є перестановочне перетворення. З метою зменшення втрати пакетів за рахунок розсіювання пачок помилок скористаємось елементами теорії захисту інформації, а саме перестановочним перетворенням. Зупинимось на даному механізмі детальніше.

Класична теорія секретних систем оперує симетричними (блоковими і потоковими) криптоалгоритмами [7]. Вони полягають в побудові криптосистеми шляхом комбінування простих і добре вивчених криптографічних перетворень (криптопримітивів).

Як основний примітив, що виконує перестановочне перетворення вхідного вектора для ефективного перемішування оброблюваних даних, використовується блок перестановок (Р-блок), структурна схема якого в загальному вигляді представлена на рис. 5 [8].

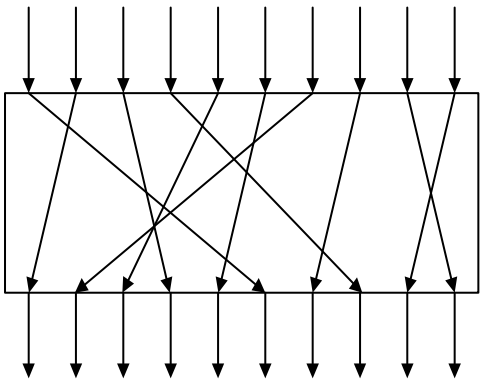

Рис. 5. Структурна схема блоку перестановок

Дослідимо методи побудови і основні властивості перестановочних перетворень. Зміст перестановочного перетворення, як видно з рисунку, полягає в зміні нумерації вхідних символів, тобто вихідний вектор – це перенумерований вхідний.

Припустимо, що $a = \{a_1, a_2, ..., a_n\}$ – вхідний вектор, а $a^* = \{a^*_1, a^*_2, ..., a^*_n\}$ – вихідний вектор, $\forall ai, a^*i \in GF(q)$.

Тоді перестановочне перетворення можна

представити у вигляді

$$a^* = a \cdot P, \qquad (1)$$

де P – перестановочна матриця, тобто квадратна матриця розміром n x n, в кожному рядку і в кожному стовпці якої знаходиться тільки по одній одиниці.

Наприклад, для перших восьми символів вхідної послідовності на рис. 5 перестановочне перетворення може бути задане у вигляді виразу (1), де

$$P = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Дійсно, підставивши матрицю у вираз (1) і виконавши матричне множення, отримаємо

$$a^* = \{a^*_1 = a_2, a^*_2 = a_7, a^*_3 = a_5, a^*_4 = \\ = a_3, a^*_5 = a_6, a^*_6 = a_1, a^*_7 = a_8, a^*_8 = a_4\}.$$

На практиці перестановочне перетворення простіше задавати вектором перестановок $p = \{p_1, p_2 ., p_n\}$, координати компонент якого відповідають індексам вхідного вектора, а власні значення компонент – індексам вихідного вектора. Наприклад, для розглянутого прикладу вектор перестановок рівний p = {6, 1, 4, 8, 3, 5, 2, 7}.

Для зручності матрицею P (або, відповідно, вектором p) позначатимемо надалі деяке фіксоване перестановочне перетворення. Таким чином за рахунок використання перестановочного перетворення заголовку АТМ чарунки можливо підвищити захищеність мережі зв'язку з використанням АТМ технології.

В цілях забезпечення часової прозорості мережі АТМ для зменшення часу затримки пакету у вузлах комутації функції заголовку пакету АТМ значно обмежені. Основною функцією заголовка є ідентифікація віртуального з'єднання за допомогою ідентифікатора і забезпечення гарантії правильної маршрутизації. Помилка в заголовку може привести до неправильної маршрутизації.

Це обумовлює ефект розмноження помилок: один спотворений біт в заголовку може привести і до втрати пакету, і до його доставки не за адресою. З метою зменшення ефекту розмноження помилок із-за неправильної маршрутизації в заголовку пакету АТМ передбачається виявлення помилок і їх виправлення. Як відомо помилки в каналі зв'язку мають властивість групуватися.

З урахуванням того, що поле управління помилками в заголовку АТМ чарунки (HEC) виправляє тільки одноразові помилки, при високому рівні завад чарунки знищуватимуться, що в свою чергу може призвести до різкого погіршення якості зв'язку [9].

Припустимо, що інформаційний вектор $a = \{a_1, a_2, ..., a_n\}$ піддається впливу помилок, в результаті чого спотворюються елементи a1÷a3 інформаційного вектору. За рахунок перестановочного перетворення можливо досягти ефекту розсіювання помилок і отримати блоки помилок меншої кратності. На рис. 6. представлений варіант розсіювання блоку помилок за допомогою блоку перестановок.

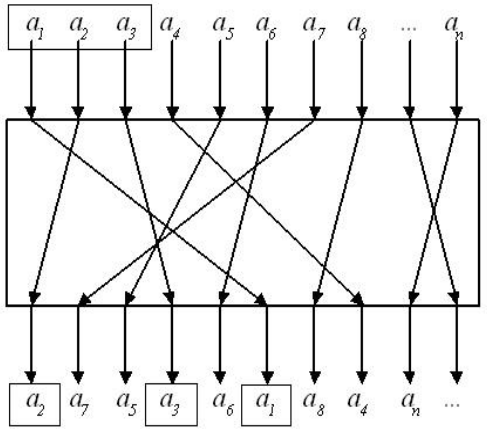

Рис. 6. Варіант розсіювання блоку помилок

Таким чином використання перестановочного перетворення заголовку АТМ чарунок дозволяє не тільки підвищити захищеність інформації в АТМ мережах, але і забезпечити можливість виправлення помилок на прийомній стороні та суттєво зменшити втрати АТМ чарунок.

Висновки

З погляду забезпечення безпеки і обмеження доступу до конфіденційної інформації мережі АТМ, які орієнтовані на з'єднання типу крапка-крапка, є набагато захищенішими, ніж мережі, засновані на принципах загального використання середовища Ethernet або Fast Ethernet, де інформація доступна в будь-якій точці сегменту мережі.

Це означає, що дані, що передаються в мережі АТМ по віртуальному каналу між двома клієнтами, доступні тільки їм і нікому більш, і виконується це на апаратному рівні. Але існуюча інфраструктура і наявне програмного забезпечення примушує використовувати режим емуляції ЛВС (LANE), при якому доводиться імітувати широкомовні повідомлення шляхом їх розсилки від сервера Broadcast and Unknow Server (BUS) до кожної станції, що знаходиться в мережі. Проте всі станції, що належать цій

віртуальній мережі, строго регламентовані.

Тому при інтеграції мереж Ethernet або Fast Ethernet в мережу АТМ з'являються додаткові можливості по підвищенню рівня їх безпеки за рахунок можливості будувати віртуальні мережі, причому не на рівні портів комутатора, а на рівні МАС-адрес робочих станцій.

За всіма цими складними процесами, характерними для сучасних мережевих технологій, дозволяє стежити єдина система управління. Вона допускає виконання цих функцій, як з одного центрального місця головного адміністратора (що зручніше з погляду забезпечення безпеки), так і з декількох територіально розподілених місць (що зручніше для оперативного вирішення поточних проблем).

Таким чином виходячи з аналізу загроз безпеки можна запропонувати наступні основні пропозиції щодо захисту інформації при передачі її по каналам за технологією АТМ:

1. У рамках транспортної мережі передачі даних повинна бути забезпечена захищеність з'єднань користувачів по цілісності, функціональності й конфіденційності переданої інформації.

2. Захист інформаційних потоків від НСД повинен бути забезпечений засобами телеслужб на рівні прикладних протоколів OSI/ISO.

3. Захист від НСД адресних і керуючих полів заголовків АТМ чарунок повинен забезпечуватись технічними засобами й устаткуванням оператора зв'язку.

4. Контроль цілісності з'єднань і підтримка функціональності транспортної мережі АТМ повинні забезпечуватися операторами зв'язку при наявності спеціалізованих засобів захисту керуючих серверів у вузлах транзитної комутації.

Список літератури

1. Оборудование для сетей АТМ технологии. – [Електронний ресурс]. – Режим доступу до документу: http://www.citforum.ru/ nets/lsok/devices.shtml.

2. Назаров А.Н. Модели и методы расчета структурно-сетевых параметров АТМ сетей / А.Н. Назаров. – М.: Горячая линия – Телеком, 2002. – 256 с.

3. Соколов А. Защита от компьютерного терроризма / А. Соколов, Б. Степанюк. – СПб.: БХВ – Петербург, 2002. – 496 с.

4. Бакланов И.Г. Технологии измерений первичной сети. Часть 2. Системы синхронизации, B-ISDN, АТМ / И.Г. Бакланов. – М.: Эко-Трендз, 2002. – 150 с.

5. АТМ-Форум. – [Електронний ресурс]. – Режим доступу до док.: http://www.atmforum.com.

6. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

7. Аграновский А.В. Практическая криптография / А.В. Аграновский, Р.А. Хади. – М.: Солон-Пресс, 2002. – 255 с.

8. Онучин С.В. Устройства защиты информации. Критерии выбора / С.В. Онучин // Мир связи. – 1998. – № 11. – С. 104-114.

9. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2003. – 1104 с.

Надійшла до редколегії 18.03.2009

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ АТМ

А.М. Носик

Проведен анализ услуг и механизмов защиты информации при передаче ее по каналам по технологи АТМ. Исходя из анализа угроз безопасности определена архитектура объектов защиты и угроз безопасности сетей АТМ. Представлена классификация угроз безопасности АТМ сети в соответствии к форматам полей заголовков протокольных блоков. Разработан механизм защиты от несанкционированного доступа адресных и управляющих полей заголовков АТМ ячеек с целью обеспечения защищенности соединений пользователей по целостности и конфиденциальности переданной информации. На основе проведенного анализа разработаны предложения по защите информации в АТМ сетях.

Ключевые слова: *технология АТМ, защита информации, угрозы безопасности.*

INFORMATION PROTECTION ON CHANNELS BY ATM

A.M. Nosyk

The analysis of services and mechanisms of information protection during transmission by channels with ATM technology was made. Based on safety threats analysis the architecture of objects protection and safety threats of ATM networks was defined. Classification of safety threats of ATM networks according to formats of protocol blocks header fields is presented. The mechanism of protection against unauthorized access to address and control fields of ATM cells for the purpose of user connection security support by integrity and confidentiality of the transferred information is developed. As the result of analysis the propositions on information protection by ATM technology were developed.

Keywords: *ATM technology, information protection, safety threats.*