ISSN 1727-1584

ГРОМЫКО И.А., САЙГАК В.Г. РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ ГЕОРАДАРА КАК ПОИСКОВОГО АНТИТЕРРОРИСТИЧЕСКОГО ПРИБОРА
Показано, что при применении георадаров в качестве поисковых антитеррористических приборов необходимо дополнять измерения контрольной проверкой результатов с помощью обычных специализированных устройств механического зондирования.

***

GROMYKO I.A., SAJGAK V.G. RECOMMENDATIONS FOR APPLICATION OF THE GEORADAR AS SEARCH ANTITERRORIST DEVICE
It is shown, that at application of georadars as search antiterrorist devices it is necessary to supplement measurements by control check of results with the help of the usual specialized devices of mechanical sounding.

УДК 681.3

***О.К. ЮДІН,*** *канд. техн. наук, доц.,*
***О.Л. ЯКОВЕНКО***

*Європейський університет*

# АНАЛІЗ ПРОЦЕДУР НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІДКРИТИХ СИСТЕМ ЗГІДНО ЕТАЛОННОЇ МОДЕЛІ ISO/OSI[1]

Розглядаються віддалені атаки згідно рівнів еталонної моделі ISO/OSI, причини успіху їх здійснення на розподілені обчислювальні системи і мережу Internet.

**1. Еталонна модель взаємодії відкритих систем.**

Сучасний ринок комунікаційного устаткування інформаційних систем і мереж є надзвичайно широким і різноманітним. З цієї причини створення сучасних інформаційних систем стало неможливим без використовування загальних підходів при їх розробці, без уніфікації характеристик і параметрів їх складових компонент.

Еталонна модель OSI стала основною архітектурною моделлю для систем передачі повідомлень. При розгляді конкретних прикладних телекомунікаційних систем здійснюється порівняння їх архітектури з моделлю OSI/ISO, яка є найкращим засобом для вивчення сучасної технології зв'язку. Вона описана стандартом ISO 7498. Модель є міжнародним стандартом для передачі даних. Згідно еталонної моделі взаємодії ВВС виділяються сім рівнів, створюючих область взаємодії відкритих систем: 7-Прикладний, 6-Представницький, 5-Сеансовий, 4-Транспортний, 3-Мережний, 2-Канальний, 1-Фізичний.

Основна мета цієї моделі полягає у тому, що кожному рівню відводиться конкретна роль. Завдяки цьому загальна задача передачі даних розщеплюється на окремі конкретні задачі. Кожен рівень визначається групою стандартів, які включають дві специфікації: протокол і забезпечуваний для вищестоящого рівня сервіс. Під протоколом мається на увазі набір правил і форматів, що визначають взаємодію об'єктів одного рівня моделі.

Кожен рівень має наперед заданий набір функцій, які він повинен виконати для проведення зв'язку [1, с.156].

*Прикладний рівень* (рівень 7) - це найближчий до користувача рівень OSI. Він забезпечує послугами прикладні процеси, що лежать за межами масштабу моделі OSI. Прикладний рівень ідентифікує і встановлює наявність передбачуваних партнерів для зв'язку, синхронізує спільно працюючі прикладні процеси, а також встановлює і погоджує процедури усунення викривлень і управління цілісністю інформації.

*Представницький рівень* (рівень 6) відповідає за те, щоб інформація, послана з прикладного рівня однієї системи, була читаною для прикладного рівня іншої системи. Представницький рівень займається синтаксисом даних.

*Сеансовий рівень* (рівень 5) встановлює, управляє і завершує сеанси взаємодії між прикладними задачами. Основні функції: управління черговістю передачі даних і їх пріоритетом, синхронізація окремих подій, вибір форми діалогу користувачів (напівдуплексна, дуплексна передача).

*Транспортний рівень* (рівень 4). Межа між сеансовим і транспортним рівнями може бути представлена як *межа* між протоколами вищих (прикладних) рівнів і протоколами нижчих рівнів. Він забезпечує зв'язок між комунікаційною підмережею і верхніми трьома рівнями, відділяє користувача від фізичних і функціональних аспектів мережі. Головна його задача - управління трафіком (даними користувача) в мережі.

*Мережний рівень* (рівень 3) - це комплексний рівень, який забезпечує можливість з'єднання і вибір маршруту між двома кінцевими системами. Мережний рівень є доменом маршрутизації. Протоколи маршрутизації вибирають оптимальні маршрути через послідовність з'єднаних між собою підмереж.

*Канальний рівень* (рівень 2) забезпечує надійний транзит даних через фізичний канал. Виконуючи цю задачу, канальний рівень вирішує питання фізичної адресації, топології мережі, впорядкованої доставки блоків даних і управління потоком інформації. Канальний рівень - визначає правила сумісного використовування фізичного

[1] Публікується в авторській редакції.

ISSN 1727-1584

рівня вузлами зв'язку.

*Фізичний рівень* (рівень 1) визначає електротехнічні, механічні, процедурні і функціональні характеристики встановлення, підтримки і роз'єднання фізичного каналу між кінцевими системами. Фізичний рівень виконує три основні функції: встановлення і роз'єднання з'єднань; перетворення сигналів і реалізація інтерфейсу. Фізичним середовищем в різних телекомунікаційних системах можуть бути найрізноманітніші засоби від простої пари дротів до складної системи передачі синхронної цифрової ієрархії.

Вдосконалення еталонної моделі ВВС для ЛОМ привело до декомпозиції рівнів 1 і 2. Канальний рівень розділений на два підрівні: підрівень управління логічним каналом (передача кадрів між РС, включаючи виправлення викривлень, діагностика працездатності вузлів мережі) і підрівень управління доступом до передаючого середовища (реалізація алгоритму доступу до середовища і адресація станцій мережі). Фізичний рівень ділиться на три підрівні: передачі фізичних сигналів, інтерфейсу з пристроєм доступу і підключення до фізичного середовища.

*Організація обміну даними в обчислювальних мережах* може здійснюватися двома різними способами: без встановлення логічного з'єднання між передаючим і приймаючим вузлами обчислювальної мережі та зі встановленням логічного з'єднання (зі встановленням сеансу зв'язку).

Спосіб зв'язку без встановлення логічного з'єднання характеризується наступним:

- він використовується в мережах з комутацією пакетів, причому кожен пакет розглядається як індивідуальний об'єкт, незалежна одиниця передачі інформації;
- пакети від відправника можна передавати в довільні моменти, одночасно множині адресатів по різних маршрутах;
- перед передачею даних крізний зв'язок між відправником і одержувачем наперед не встановлюється, не вимагається також синхронізації апаратури зв'язку на передаючому і приймальному пунктах;
- через зайнятість окремих ділянок маршруту може здійснюватися буферизація пакетів у проміжних вузлах зв'язку;
- передача сигналу від адресата до відправника, підтверджуючого отримання інформації, не здійснюється.

Це один з перших і простих способів обміну даними в комунікаційній технології. Він широко використовується в дейтаграмних мережах, в яких реалізуються дейтаграмні протоколи інформаційного обміну. Спосіб зв'язку (або режим зв'язку), орієнтований на логічне з'єднання, відноситься до пізнішої технології. Він забезпечує вищий рівень сервісу в порівнянні з дейтаграмним зв'язком.

Особливості організації обміну даними зі встановленням логічного з'єднання:

- перед передачею інформації між взаємодіючими абонентами (відправником і одержувачем) встановлюється логічний (віртуальний) канал, причому технологія створення (встановлення) каналу така: відправник посилає запит на з'єднання видаленому адресату через ряд проміжних вузлів зв'язку; адресат, одержавши цей запит, у разі «згоди» на встановлення логічного каналу посилає відправнику сигнал підтвердження; після отримання сигналу підтвердження відправником починається обмін даними з управлінням потоком, сегментацією і виправленням помилок;
- після завершення обміну даними адресат посилає пакет підтвердження цієї події відправнику (клієнту - ініціатору встановлення логічного каналу), який сприймається як сигнал для роз'єднання каналу. Отже, при використовуванні цього способу зв'язку виділяються три етапи: встановлення каналу, обмін даними, роз'єднання каналу.

Зв'язок зі встановленням логічного каналу застосовується у віртуальних мережах, де використовуються протоколи інформаційного обміну типу віртуального з'єднання. До них відносяться протоколи: управління передачею TCP, послідовних пакетів SPP, транзакції ATP і ін. [2, с.452].

Перший з розглянутих способів організації обміну даними у мережах відрізняється простотою у реалізації і порівняно невеликими накладними витратами. Другий спосіб, навпаки, характеризується високими накладними витратами, проте, він надає абонентам істотно великі зручності, забезпечує необхідну оперативність в обміні даними (в ідеальному випадку переповнювання з'єднань у проміжних вузлах зв'язку повністю виключається) і гарантовану надійність доставки інформації абонентам.

Таким чином, кожний з режимів зв'язку має свої особливості, а значить, і області застосування.

Протоколи обміну даними, або протоколи верхнього рівня (вірніше, середнього, оскільки вони виконуються на 4-5-у рівнях моделі ВВС), служать для управління обміном даних. Кожен протокол має засоби для ідентифікації будь-якої робочої станції мережі по імені, мережній адресі або по обох цих атрибутах. Активізація обміну інформацією між взаємодіючими вузлами починається після ідентифікації вузла адресата вузлом, що ініціює обмін даними. Ініціююча станція встановлює один з методів організації обміну даними: метод дейтаграм або метод сеансів зв'язку. Протокол надає засоби для прийому/передачі повідомлень адресатом і джерелом. При цьому звичайно накладаються обмеження на довжину повідомлень.

**2. Віддалені атаки згідно рівнів еталонної моделі ISO/OSI.**

Міжнародна Організація по Стандартизації (ISO) прийняла стандарт ISO 7498, описуючий взаємодію відкритих систем (OSI). Розподілені ОС так же являються відкритими системами. Любий мережний протокол обміну, як і любу мережну програму, можливо с тією чи іншою степеню точності спроектувати на еталонну, сімерівньову модель OSI. Така многорівньова проекція дозволить описати в термінах моделі OSI функції, закладені у мережний протокол або програму. Віддалена атака також є мережною програмою. У зв'язку з цим є логічним розглядати віддалені атаки на РОС, проектуючи їх на еталонну модель ISO/OSI [2, с.369].

*Причини успіху здійснення віддалених атак на розподілені обчислювальні системи і мережу Internet:*

- Відсутність у РОС повної інформації про її об'єкти.
- Відсутність у РОС криптозахисту повідомлень.
- Відсутність виділеного каналу зв'язку між об'єктами мережі Internet.
- Недостатня ідентифікація й аутентифікація об'єктів і суб'єктів мережі Internet.

ISSN 1727-1584

- Взаємодія в мережі Internet об'єктів без установлення віртуального каналу.

- Використання нестійких алгоритмів ідентифікації об'єктів при створенні віртуального TCP-з'єднання.

- Неможливість контролю за віртуальними каналами зв'язку між об'єктами мережі Internet.

- Відсутність у Internet можливості контролю за маршрутом повідомлень.

- Відсутність у Internet повної інформації про її об'єкти і, отже, вимушене використання алгоритмів віддаленого пошуку.

- Відсутність у базових протоколах Internet криптозахисту повідомлень.

*Переваги розподіленої ОС із виділеними каналами зв'язку між об'єктами полягають у наступному:*

- передача повідомлень здійснюється прямо між джерелом і приймачем, минаючи інші об'єкти системи. У такій системі у випадку відсутності доступу до об'єктів, через які здійснюється передача повідомлення, не існує програмної можливості для аналізу мережного трафіка;

- є можливість ідентифікувати об'єкти розподіленої системи на канальному рівні за їхніми адресами без використання спеціальних криптоалгоритмів шифрування трафіка. Це можливо, оскільки система побудована так, що по даному виділеному каналу здійсненний зв'язок тільки з одним визначеним об'єктом. Поява в такій розподіленій системі помилкового об'єкта неможлива без апаратного втручання (підключення додаткового пристрою до каналу зв'язку);

- система з виділеними каналами зв'язку - це система, у якій відсутня невизначеність з інформацією про її об'єкти. Кожен об'єкт у такій системі споконвічно однозначно ідентифікується і має повну інформацію про інші об'єкти системи.

*До недоліків РОС із виділеними каналами відносяться:*

- складність реалізації і високих витрат на створення системи;

- обмежене число об'єктів системи (залежить від числа входів у концентратора);

- складність внесення в систему нового об'єкта.

**3. Програмно-апаратні методи захисту від віддалених атак у мережі Internet:**

1. Апаратні шифратори мережного трафіка.

2. Методика Firewall, реалізована на базі програмно-апаратних засобів, таких як:

2.1. Багаторівнева фільтрація мережного трафіка.

Фільтрація звичайно здійснюється на трьох рівнях OSI:

- мережному (IP);

- транспортному (TCP, UDP);

- прикладному (FTP, TELNET, HTTP, SMTP і т.д.).

2.2. Proxy-схема з додатковою ідентифікацією й аутентифікацією користувачів на Firewall-хості.

2.3. Створення приватних мереж (Private Virtual Network - PVN) з «віртуальними» IP-адресами (NAT - Network Address Translation).

3. Захищені мережні криптопротоколи.

4. Програмно-апаратні аналізатори мережного трафіка.

5. Захищені мережні ОС.

Складна структура атак не дозволяє використовувати лише один принцип забезпечення безпеки. Багатогранність різновидів проведення віддаленої атаки потребує комплексного захисту як окремого хоста, так і цілих РОС.

Сама система захисту Firewall є звичайним фільтром, тільки комп'ютерна програма в поєднанні з купою заліза. Отже не факт, що розум людини може обійти різноманітні захисти при проведенні атаки, але це не значить, що система Firewall нікому не потрібна. Адже Firewall у поєднанні з мережним монітором безпеки IP Alert-1, та досвідченим спеціалістом з галузі інформаційної безпеки, можуть гарантувати, що, принаймі, 99 % атак на Вашу РОС буде відбито, а зловмисника покарано відповідно до Закону.

Розглянемо на прикладі спрощену схему повнофункціонального хоста Firewall (рис.).

**4. Мережний сервер безпеки.**

*Процедура запитів зв'язку :*

1. Хост з IP адресою 120.22.100.01 зв'язується з хостом № 3.

2. Виконання процедури архівного запису як відповідь на запит про встановлення зв'язку.

3. Перевірка Firewall-хостом на наявність атаки.

4. Виконуються процедури аутентифікації і встановлення зв'язку хостів. Надається дозвіл на передачу даних.

При виявленні атаки, повідомлення відкидається Firewall-хостом.

Наприклад, хост атакуючого з IP адресою 190.13.250.28 (схема рисунку), зібравши достатньо інформації під час мережного аналізу, від імені IP адреси інших хостів мережі хоче провести DOS-атаку. Звісно, що Firewall-захист пропустив би цю атаку як би не мережний монітор безпеки IP Alert-1, яким цілодобово керують професіонали комп'ютерної безпеки.

Вирахувавши справжній IP-адрес зловмисника, йому посилають RST-біт, що розриває зв'язок його хоста з даним доменом. Його IP-адрес заноситься до списку адресів Firewall-захисту, які в наступному автоматично відфільтровуються.

Знаючи справжній IP-адрес зловмисника можна легко вирахувати його місце знаходження, структуру або організацію до якої відноситься хост зловмисника, та вжити подальших заходів, щодо запобігання злочинних дій збоку цієї особи або групи осіб.

Отже для забезпечення безпеки потрібний комплекс програмно-технічних засобів, та спеціалісти для стеження за роботою цього комплексу.

**Висновки.**

1. Вибір безпечної топології РОС є необхідною, але аж ніяк не достатньою умовою для створення захищених систем зв'язку між об'єктами розподілених ОС.

2. Найкраща, з погляду безпеки, взаємодія об'єктів у розподіленій ОС можливо тільки по фізично виділеному каналі.

3. При побудові захищеної системи зв'язку у розподіленій ОС необхідно виходити з того, що всі повідомлення, передані по каналу зв'язку, можуть бути перехоплені, але це не повинно спричинити за собою порушення безпеки системи в цілому.

4. Будь-яка взаємодія двох об'єктів у розподіленій ОС повинна проходити по віртуальному каналу зв'язку.

5. Для забезпечення надійної ідентифікації об'єктів розподіленої ОС при створенні віртуального каналу необ-

ISSN 1727-1584

хідно використовувати криптоалгоритми з відкритим ключем.

6. Забезпечення цифрового підпису повідомлень.

7. Необхідно забезпечити можливість шифрування повідомлень.

8. Для забезпечення доступності ресурсів розподіленої ОС необхідний контроль за віртуальними з'єднаннями між її об'єктами.

9. Забезпечення контролю за встановленням з'єднання, ввівши обмеження на число оброблюваних за секунду запитів з однієї підмережі.

10. Необхідно забезпечити контроль за використанням з'єднання, розриваючи його за тайм-аутом у випадку відсутності повідомлень.

11. Найбільш безпечно розподіленою ОС є та система, у якій інформація про її об'єкти споконвічно цілком визначена, й у якій не використовуються алгоритми віддаленого пошуку.

Якщо виконати попередню вимогу неможливо, необхідно в розподіленої ОС використовувати тільки алгоритм віддаленого пошуку з віддаленим інформаційно-пошуковим сервером, і при цьому взаємодія об'єктів системи з даним сервером повинна здійснюватися тільки по віртуальному каналу з застосуванням надійних алгоритмів захисту з'єднання з обов'язковим використанням статичної ключової інформації.

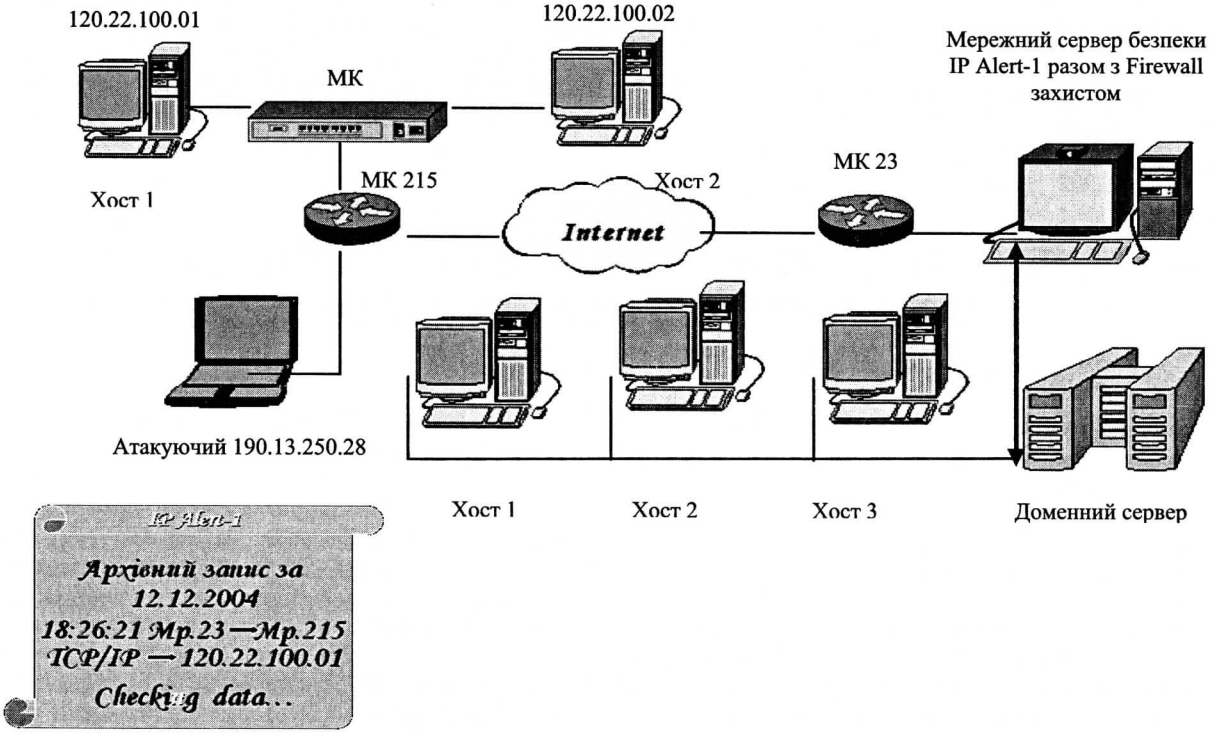


**Рисунок - Спрощена схема повнофункціонального хоста Firewall**

## ЛІТЕРАТУРА

1. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. -СПб.: БХВ-Петербург, 2000. -320 с.

2. Конеев В.Р., Беляев А.В. Информационная безопасность предприятия. -СПб.: БХВ - Петербург, 2003. -752 с.

*Надійшла до редколегії 22.06.2005*

ЮДИН О.К., ЯКОВЕНКО О.Л. АНАЛИЗ ПРОЦЕДУР НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ ОТКРЫТЫХ СИСТЕМ ПО ЭТАЛОННОЙ МОДЕЛИ ISO/OSI
Рассматриваются отдаленные атаки по уровням эталонной модели ISO/OSI, причины успеха их осуществления на распределенные вычислительные системы и сеть Internet.

***

JUDIN O.K., JAKOVENKO O.L. THE ANALYSIS OF PROCEDURES IN THE NON-AUTHORIZED ACCESS TO INFORMATION RESOURCES OF OPEN SYSTEMS ON REFERENCE MODEL ISO/OSI
The remote attacks on levels of reference model ISO/OS I, the reasons in success of their realization on the distributed computing systems and a network Internet are considered.