

Оцінка швидкодії мережевих диспетчерів доступу

УДК 004.056.52

Денис Самойленко

*Національний університет кораблебудування імені адмірала Макарова,
DenNikSam@gmail.com*

При проектуванні захищених мережевих інформаційних ресурсів (МІР) з комплексною системою захисту інформації необхідно дотримуватись ряду вимог нормативних документів. Однією з таких вимог є створення диспетчера доступу (ДД) – єдиної точки проходження усіх звернень до МІР, як до інформаційної системи [1-2].

Основні висновки, одержані у попередніх роботах [наприклад, 3], дозволили сформулювати вимоги для коректного складання ДД. Основною з вимог є максимальна відмова від прийняття рішень на етапі серверного оброблення і якнайшвидша передача усіх запитів до МІР. Дані, щодо практичного порівняння різних серверних інструкцій виявлено не було, проте, у неформальному обговоренні (форумах) висловлюються окремі експертні думки без експериментального їх підтвердження.

Метою даної роботи є реалізація та випробування на швидкодію різних реалізацій ДД МІР.

У якості предмета дослідження було складено ДД, що реалізує перевірку трьох «ближчих записів»: головна сторінка (порожній запит - ^\$), запит авторизації (/login), множинний запит (/news/номер), де номер – деяке число. За умови збігу запиту з шаблоном здійснюється перехід на відповідний обробник запиту у окремому файлі (index1-3.php). Інші запити спрямовуються на обробник помилок (error.php). Правила оброблення виглядають наступним чином:

```
RewriteRule ^$ index1.php [L]
RewriteRule ^login$ index2.php [L]
RewriteRule ^news/(d+)$ index3.php?n=$1 [L,QSA]
RewriteRule .* error.php
```

Опція [L] упереджує оброблення подальших правил, [QSA] – зберігає початкові параметри запиту, якщо такі були.

Упередження повторного (циклічного) аналізу правил можна реалізувати двома способами: 1) встановленням опції [END] для інструкцій RewriteRule, 2) контролем значення серверної змінної REDIRECT_STATUS. Останній спосіб є універсальним, перший придатний для серверів Apache починаючи з версії 2.3.

Третій та четвертий варіанти ДД базуються на перенесенні процесу аналізу запитів до самого МІР. Усі запити переводяться до єдиного файлу ДД «main.php».

```
RewriteRule .* main.php
```

У четвертій варіації ДД додано опцію [END] для упередження повторного запуску аналізу через його потенційний вплив на загальну швидкодію ДД. Задля елімінації впливу на результати відмінностей у кодах МІР з різними ДД, у файлі main.php була повністю відновлена функціональність індексних файлів

Результати вимірювання даних щодо часу роботи одного сеансу взаємодії клієнт-сервер зведені до табл.1

Розвиток систем кабельного телебачення (КТБ) бере початок від мереж колективного телевізійного прийому. Система КТБ являє собою сукупність технічних засобів, призначених для формування, обробки та передачі телевізійних сигналів, їх розподілення за допомогою розподільчих кабельних структур і прийому за допомогою індивідуальних абонентських пристроїв.

Таблиця 1

Час одного сеансу клієнт-серверної взаємодії, мс

	/	/login	/news/21	error	середнє	похибка
Варіант 1	9,45	7,92	8,56	7,84	8,44	0,13
Варіант 2	7,88	8,49	8,65	9,06	8,52	0,20
Варіант 3	7,83	8,31	8,22	8,47	8,21	0,36
Варіант 4	8,77	8,53	7,83	8,18	8,33	0,21

Як неважко помітити з наведених результатів, суттєвої відмінності між способами реалізації ДД не спостерігається. З урахуванням похибки вимірювань можна стверджувати про приблизну часову еквівалентність усіх ДД (у межах 5 %).

Тим не менш, найменший час сеансу демонструє ДД, реалізований засобами мови PHP. Одержаний висновок суперечить популярному у мережі Інтернет твердженню щодо повільності PHP у порівнянні з серверними функціями, що додатково свідчить про відсутність попередніх досліджень реальних ситуацій з використанням для його формування лише експертних думок. Додатково можна зауважити, що побудова ДД засобами самого PHP є кращою з точки зору більшої локалізації захисних засобів всупереч їх розподіленості у інших ДД.

Звертає на себе увагу той факт, що використання опції примусової зупинки [END] не покращує швидкодію ДД, реалізованого засобами PHP (рядки 3-4 табл. 1). Це може бути пояснене тим, що процедура оброблення даної опції є більш складною, ніж повторне оброблення одного рядка ДД. Для більш складного ДД з декількома умовами зазначена опція призводить до прискорення роботи (рядки 1-2).

1. Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу: НД ТЗІ 2.5-010-2003. / СБ України. Київ: ДСТСЗІ СБ України, 2003. 20 с.

2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99 / СБ України. Київ: ДСТСЗІ СБ України, 1999. 61 с.

3. Самойленко Д. М., Данильченко С. С. Аналіз способів створення людино-орієнтованих імен з позиції інформаційної безпеки / Матеріали V Всеукраїнської науково-практичної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». – Миколаїв: Вид-во НУК, 2015. – с. 108-109