Секція: **ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ**
Керівники: **проф. М.Приймак, доц. С.Лупенко, доц. О.Мацюк**
Секретар: **доц. Н. Загородна**

УДК 531.374; 539.213

Е. Довговецький, Р. Жаровський, Л. Щербак
(Тернопільський національний технічний університет імені Івана Пулюя)

ДОСЛІДЖЕННЯ МЕТОДІВ ОПТИМІЗАЦІЇ ПЕРЕДАЧІ ДАНИХ В ПІРИНГОВИХ МЕРЕЖАХ

P2P-мережі засновані на ідеї децентралізації, спільного використання ресурсів по великому числу користувачів. Така децентралізація дозволяє мережі перевершує всі інші технології доставки контенту. У всіх параметрів, таких як загальна сума завантаження, швидкість, доступність, масштабованість і економічність - P2P переваги не має собі рівних. Є багато P2P реалізації в даний час, однак найбільш популярним є протокол BitTorrent з 60-90 відсотків від загального обсягу трафіку P2P.

При передачі інформації протокол Torrent генерує значну кількість службової інформації тому доцільним є дослідження та оптимізація передачі даних в P2P мережах. В доповіді розглянуті методи зменшення об’єму технічних даних між користувачами мережі. Для зменшення об’єму технічної інформації було застосовано відсіювання надмірної (системні команди та биті байти информації) інформації та кешування даних. На графіку (рис. 1) показано, що за рахунок кешування з 150 найпопулярніших торрентів можна заощадити до 20% трафіку BitTorrent.

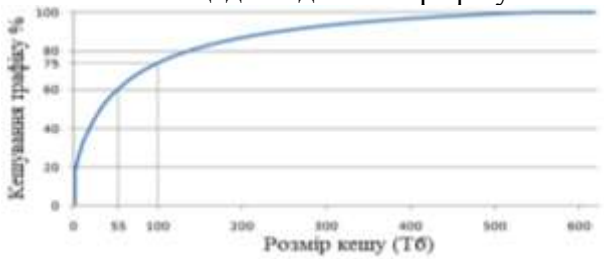

Рис. 1. Об'єм кеш-пам'яті

Простір дискового кеша може бути представлений як принцип Парето. За кешування 20 відсотків активного вмісту BitTorrent до 80 відсотків вірогідність попадання може бути досягнута. Під час тестування в якості сервера було використано стаціонарний комп’ютер з параметрами: процесор – Core2 Duo 2.4 гГц , ОЗП – 8 Гб, HDD – 320 Гб 7200 Об/с. Тестування проводилося на протязі трьох робочих днів за цей період системою проксі-кеш було захоплено 24 міліонна GET запитів розмір журналу склав 18 Гб. Відносно тестування, оптимальний розмір кеша для активних торрентів становить від 55 ТБ до 100 ТБ.

Також розглядався захист мережі від атак зловмисників та закриття доступу для заражених комп’ютерів (додатків), методом фільтрування та обробки даних клієнтів. Захист проводиться методом аналізу та формування білих та чорних списків веб сайтів, та перевірку завантажувальних файлів через бази антивірусних програм. Відносно обробленої інформації в разі знаходження шкідливого файлу (веб сторінки) система повідомляє користувача що дана інформація (веб сторінка) може зашкодити роботі його комп’ютера. У разі якщо комп’ютер користувача вже заражений то система блокує його запити до мережі щоб не було заражена інших користувачів та не булі проведи дії з боку вірусних програм в глобальну мережу.