Н.Ф. Казакова, к.т.н., доцент, кафедра інформаційних систем в економіці,
Одеський державний економічний університет (м. Одеса)

МОНІТОРИНГ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Вивчення і аналіз доступних в Internet публікацій з тематики, яка винесена в заголовок, не виявив яких-небудь спроб опису математичних моделей процесу моніторингу інформаційних ресурсів в захищених інформаційних мережах. Під словом «модель» далі будемо мати на увазі аналітичний вираз.

Очевидно, специфіка прикладної області така, що розробникам і дослідникам систем моніторингу захищеного інформаційного поля доступніші та такі, що мають більшу перевагу, моделі виражені алгоритмами. Таким чином, складність завдання порівняння конкуруючих алгоритмів-стратегій реалізації систем моніторингу захищених інформаційних мереж, крім відсутності об'єктивної числової інформації про ефективність кожного варіанту, посилюється відсутністю зручного, одноманітного і строгого (з математичної точки зору) представлення моделей даної проблемної області.

Можна було б припустити, що найбільш використовуваним інструментом дослідження і опису систем моніторингу стануть засоби імітаційного моделювання. Проте для широкого кола читачів доступні всього дві такі роботи ([1, 2]). У них за допомогою імітаційного моделювання досліджуються різні аспекти функціонування системи моніторингу «роботів». Але оскільки результати цих досліджень неможливо застосувати до дослідження стратегій «сенсорів» і «мобільних роботів», то, очевидно, що викладені в даних роботах підходи не застосовні як одноманітний підхід до розгляду ефективності будь-яких систем моніторингу.

Найближче до задачі, яка представлена в доповіді, підійшов McLearn в роботі [1]. Ним була розроблена і застосована програма імітації функціонування модифікованих роботів, які взаємодіють один з одним з тією метою, щоб не переписувати один і той же IP-ресурс зайву кількість разів, тобто для ліквідації перетину сегментів моніторингу. На жаль, в зазначеній роботі зроблений акцент на розгляд ефективності внутрішнього протоколу взаємодії між роботами. Очевидно, цим пояснюється те, що в отриманих результатх відсутні багато елементів, які необхідні для розгляду інших стратегій моніторингу. Так автор обмежився розглядом лише одного критерію ефективності системи моніторингу – «свіжість». Також було зроблено багато припущень про властивості інформаційного поля (наприклад, час скачування одного IP-ресурсу була встановлена в 1 секунду, а сам він характеризується тільки розміром і ознакою стану – «доступний» або «не доступний» для переписування. Іншими словами: не вдалося виявити опис яких-небудь моделей (підходів до їх опису) або спеціальних засобів (зокрема засобів імітаційного моделювання), які допомогли б одержати необхідні дані для самостійного проведення дослідження і порівняння всіх варіантів системи моніторингу.

На перший погляд, найбільш природним в даній ситуації було б використання теорії систем масового обслуговування (ТСМО). Найбільша вигода від викори-

стання ТСМО полягає в можливості отримання аналітичних залежностей характеристик СМО від параметрів вхідного потоку. Проте простота отримання більшості (цей вислів не відноситься до вибраних в доповіді критеріїв ефективності системи моніторингу) аналітичних залежностей обумовлена допущенням про те, що потік заявок є простим, тобто потік володіє властивостями стаціонарності, ординарності і відсутністю наслідку. Для інших видів потоків заявок отримання аналітичних залежностей практично є неможливим. Враховуючи те, що для вирішення основного завдання, переважніше не робити ніяких допущень про характер наявних потоків, оскільки це звужує область застосовності одержуваного результату. Стає зрозумілим, що ТСМО також не може розглядатися як основа для отримання рішення позначеної проблеми.

Таким чином, далі в доповіді показується розв'язання актуального завдання розробки моделей, які можуть служити, по-перше, як приклад зручного (для фахівців в позначеній прикладній області), досить строгого і одноманітного підходу до опису систем моніторингу. А по-друге, ці моделі стануть основою (шаблоном) для реалізації програмних засобів, які необхідні власникам сегментів інформаційних полів для прискорення і здешевлення отримання об'єктивних числових даних при проведенні відносного порівняння вибраних як претенденти на реалізацію варіантів системи моніторингу.

При виборі варіантів системи моніторингу, які необхідно порівняти, орієнтувалися на:

– *потреби і реальну ситуацію (у тому числі і з інформаційним полем), які склалися на момент проведення дослідження;*

– *критерій доступності порівнюваних варіантів для самостійної програмної реалізації і впровадження;*

– *необхідність порівняння варіантів, які належить сенсорній концепції моніторингу з варіантами, які належать іншим концепціям;*

В результаті були вибрані три варіанти в яких відповідно використовуються:

– *один звичайний робот;*

– *один модифікований робот;*

– *сенсори.*

Попереднє уявлення про ці варіанти можна отримати, наприклад, з [3]. Додаткові деталі вибраних варіантів приводяться в доповіді далі по мірі необхідності.

Для створення імітаційної моделі варіанту системи одного робота проведено додаткове вивчення і аналіз публікацій з приводу принципів і алгоритмів функціонування роботів.

У зв'язку з тим, що досліджуваний варіант сенсорної системи ще не реалізовувався на практиці, а є тільки опис зразкового алгоритму реалізації, то при створенні моделі даного варіанту системи моніторингу автори спиралися на ці описи та на дані, які є у [3]. Власне цього було достатньо, щоб перевірити можливість розгляду проектованих варіантів системи моніторингу без їх практичної реалізації.

З причини того, що варіант системи з одним модифікованим роботом має мінімальні відмінності від варіанту системи з одним звичайним роботом, тут не

приводиться опис імітаційної моделі такого варіанту системи. В доповіді зроблене обмеження стосовно розгляду відповідних відмінностей при подальшому описі її програмної реалізації.

Щоб уникнути невиправданого ускладнення моделей і порівняти за умовами розгляду варіанти системи, в принципі, вважали, що пропускна спроможність каналів, через які система моніторингу і інформаційні джерела підключені до Internet, мають максимально можливий розмір, щоб мінімізувати час передачі будь-якого, окремо взятого IP-ресурсу. Крім того, при дослідженні відмовилися від розгляду функції пошуку нових IP-ресурсів.

На основі викладеного, як результат, в доповіді представлена *системна модель процедури моніторингу інформаційних ресурсів в захищених мережах*.

Література

1. McLearn G. L. Autonomous Cooperating Web Crawlers / Master's thesis // [Electronic resource]: Mode of access: http://citeseer.nj.nec.com/mclearn02autonomo-us.html.

2. Melnik S., Raghavan S., Yang B., Garcia-Molina H. Building a Distributed Full-Text Index for the Web // [Electronic resource]: Mode of access: http://www-db.s-tanford.edu/~rsram/pubs/www10/www10paper.pdf.

3. Земсков И.А. Моделирование мониторинга информационного поля Internet. – Дис. … канд. техн. наук: 05.13.11: Москва. – М.: РГБ. – 2000 (Из фондов Российской государственной библиотеки).

4. Казакова Н.Ф. моніторинг інформаційних ресурсів в захищених інформаційних мережах // Матеріали VII Міжнар. наук.-техн. конф. студентства та молоді «Світ інформації та телекомунікацій», Київ, 15-16 квітня 2010 р. – Київ: Державний університет інформаційно-комунікаційних технологій, 2010. – С.165-168.