

АНАЛІЗ МЕТОДІВ БЛОКУВАННЯ РЕСУРСІВ ІНТЕРНЕТ

Колтун Ю.М., Тройно Т.В.

Харківський національний університет радіоелектроніки, Харків, Україна

Інтернет забезпечує зв'язок різних інформаційних мереж, які належать різним установам у всьому світі. Якщо раніше мережа використовувалася винятково в якості передачі файлів і повідомлень електронної пошти, то сьогодні за її допомогою вирішуються значно складніші задачі – розподіленого доступу до ресурсів і надання персоналізованих послуг. Однак робота з Інтернет супроводжується також безліччю проблем, серед яких найбільш важливі полягають в забезпеченні безпечного публічного використання мережі і у визначенні підходів, що забезпечують управління доступом до Інтернет-ресурсів [1]. Метою доповіді є порівняльний аналіз методів блокування протиправного контенту в мережі Інтернет і формування пропозицій щодо використання найбільш ефективних з них (або їх комбінацій) на основі набору відібраних критеріїв якості технологічного та економічного характеру. Зокрема у доповіді аналізуються наступні методи блокування: за IP-адресою, за DNS, за URL та поглиблений аналіз пакетів за їх вмістом (DPI) [2]. В процесі проведення аналізу цих методів значна увага приділяється потенційній точності цих методів, надана оцінка можливостям щодо їх обходу, а також проаналізовано наявність в арсеналі Інтернет-операторів заходів, що перешкоджають їх обходу [3]. Аналіз цих методів блокування дозволив зробити такі висновки. Найкращим методом блокування є комбіноване блокування з попереднім виділенням за IP адресами та подальшою фільтрацією за URL (IP + URL). Його можна рекомендувати у якості основного методу для вирішення поставлених задач. Зокрема на підставі цього методу у доповіді пропонується послідовність дій щодо організації блокування шкідливих Інтернет-ресурсів в Україні. Реалізація блокування на основі комбінованого методу IP + URL або на основі поглибленого аналізу пакетів, забезпечує достатню точність, щоб уникнути надмірного блокування, має мінімальний вплив на інфраструктуру мережі Інтернет, не знижує її стійкість в цілому і не порушує працездатності інших сервісів і додатків.

Список літератури

1. Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей (издание II) [Електронний ресурс] / Cisco Systems©. – 2003. – Режим доступу до ресурсу: <https://docplayer.ru/28292846-Resheniya-kompanii-cisco-systems-po-obespecheniyu-bezopasnosti-korporativnyh-setey-izdanie-ii.html>
2. Барнс Р. Технические вопросы блокировки сервисов Интернет [Електронний ресурс] / Р. Барнс, А. Купер, О. Колкм // Инженерный совет интернет (Internet Engineering Task Force, IETF). – 2012. – Режим доступу до ресурсу: http://raec.ru/upload/files/ietf_block_internet_tech_2012.pdf
3. Как обойти блокировку запрещенных сайтов [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: <http://ntv.livejournal.com/272969.html>