УДК 621.391

Каптур В.А., Ложковський А.Г., Фурмур М.В., Чумаков Р.В.
Каптур В.А., Ложковский А.Г., Фурмур М.В., Чумаков Р.В.
Kaptur V.A., Lozhkovskiy A.G, Furmur M.V., Chumakov R.V.

СИСТЕМА ФІЛЬТРАЦІЇ SMS-ПОВІДОМЛЕНЬ У МЕРЕЖІ ОПЕРАТОРА МОБІЛЬНОГО ЗВ'ЯЗКУ

СИСТЕМА ФИЛЬТРАЦИИ SMS-СООБЩЕНИЙ В СЕТИ ОПЕРАТОРА МОБИЛЬНОЙ СВЯЗИ

FILTRATION SYSTEM OF SMS-MESSAGES IN THE MOBILE NETWORK

Анотація. Проведено аналіз загальних принципів міжмережної взаємодії операторів мобільного зв'язку при обміні SMS-повідомленнями за допомогою протоколу SMPP. На основі проведеного аналізу розроблено архітектурну модель підсистеми фільтрації, яку інтегровано в архітектуру розробленого авторами статті SMS-комутатора. Розроблена математична модель дозволила провести оцінку впливу базових параметрів роботи комутатора (та підсистеми фільтрації) на тривалість доставки SMS-повідомлень.

Аннотация. Проведен анализ общих принципов межсетевого взаимодействия операторов мобильной связи при обмене SMS-сообщениями с использованием протокола SMPP. На основе проведенного анализа разработана архитектурная модель подсистемы фильтрации, интегрированная в архитектуру разработанного авторами статьи SMS-коммутатора. Разработанная математическая модель позволила провести оценку влияния базовых параметров работы коммутатора (и подсистемы фильтрации) на продолжительность доставки SMS-сообщений.

Summary. The analysis of the general principles of interconnection of mobile operators in the exchange of SMS-messages protocol SMPP. Based on the analysis developed by the architectural model of the filter subsystem integrated into the architecture developed by the authors of SMS-softswitch. A mathematical model that assess the impact of the basic parameters of the switch (and sub-filter) on the duration of delivery of SMS-messages.

Стрімкий розвиток технологій мобільного зв'язку став передумовою появи значної кількості SMS-послуг, які проникли практично в усі сфери життя людини. Сьогодні за допомогою SMS-повідомлень людина може обслуговувати власний банківський рахунок, отримувати новини та повідомлення про стан здоров'я близьких людей, керувати пристроями на відстані, здійснювати покупки в магазинах тощо.

Разом з тим популярність SMS-повідомлень створила проблему появи цілої низки нових загроз, що часто призводять до матеріальних втрат (як для оператора мобільного зв'язку, так і для абонента). Прикладами таких загроз можуть стати:

– DoS атаки безпосередньо на вузол обслуговування коротких повідомлень (Short Message Service Center – SMSC) оператора зв`язку. Керуючись бажанням захистити власні центри обміну повідомленнями від зловмисників, оператори змушені розробляти власні XML – подібні протоколи взаємодії з клієнтськими платформами;

– небажані повідомлення (спам). Особливість SMS-спаму полягає у тому, що абонент не має можливості запобігти надходженню до нього небажаних повідомлень. Тобто кінцевий абонентський термінал у будь-якому разі повинен прийняти повідомлення. Особливо гостро питання спаму постає для абонентів у тих країнах, де повідомлення оплачується обома сторонами;

– підроблення адреси відправника. Маючи складну систему договірних відносин із центрами обміну SMS-навантаженням по всьому світу, оператори мобільного зв'язку практично не мають можливості контролювати достовірність інформації про номер відправника повідомлення, що надходить від посередника;

– SMS-віруси, які, використовуючи вразливість операційних систем сучасних моделей телефонів, можуть призвести до втрат коштів або даних абонентів.

Незважаючи на таку значну кількість загроз сьогодні практично не існує ефективних рішень фільтрації SMS-повідомлень, що працюють за принципом «фільтруючої хмари». У свою чергу, ті рішення [1], що сьогодні впроваджено на мережах операторів є, як правило, інтегрованими безпосередньо до вузлів обслуговування коротких повідомлень та не можуть бути використані для

побудови сервісів національного або глобального масштабу з охопленням декількох операторів одночасно.

Метою статті є розробка концепції та оцінка ефективності системи фільтрації SMS-повідомлень, що працює за принципом «фільтруючої хмари».

Як відомо, ядром системи обміну SMS-повідомленнями будь-якого оператора мобільного зв'язку є вузол обслуговування коротких повідомлень (SMSC), який використовує для взаємодії із аналогічними вузлами інших операторів мобільного зв'язку протокол піринговых коротких повідомлень (Short Message Peer to Peer (SMPP) protocol) [2].

SMPP – це відкритий протокол передачі повідомлень, що дозволяє об'єктам системи обміну короткими повідомленнями (SMEs) поза мобільною мережою взаємодіяти із SMSC. Немобільні об'єкти, що доставляють повідомлення до SMSC, або отримують їх від нього, відомі як об'єкти зовнішніх коротких повідомлень – ESME (External Short Message Entities).

Відповідно до специфікації [2] протокол SMPP визначає набір операцій для обміну короткими повідомленнями між ESME та SMSC, а також дані, якими ESME повинен обмінятися з SMSC протягом SMPP-операцій. Абоненти SMS можуть отримувати короткі повідомлення від мобільної станції (Mobile Station – MS) через один або більшу кількість ESME.

SMPP базується на обміні протокольних блоків даних (PDUs) запиту та відгуку між ESME та SMSC за допомогою базових мережних з'єднань установлених за допомогою стеків протоколів TCP/IP [3] або X.25 [4]. ESME ініціює сесію SMPP між SMSC та ESME, встановлюючи спочатку мережне з'єднання до SMSC, а далі, надсилаючи запит типу Bind для того, щоб відкрити сесію.

З метою надання можливості ESME передавати та отримувати повідомлення установлюється або два незалежних мережних з'єднання в режимах Transmitter та Receiver, або одне з'єднання в режимі Transceiver.

Протягом сесії SMPP, ESME може відправляти серію запитів до SMSC та повинен отримувати відповіді на кожний запит від SMSC. На додаток, SMSC може відправляти запити SMPP до ESME, на які він повинен відповідати у визначений специфікацією протоколу спосіб.

В основу вирішення проблем, пов'язаних із потенційною небезпечністю, що прихована в неконтрольованому обміні SMS-навантаженням, може буди покладено створення програмного комутатора SMS-повідомлень. Основним призначенням такого комутатора має стати організація безпечного середовища для взаємопідключення SMSC між собою за принципом «фільтруючої хмари», а також забезпечення посередницьких функцій між клієнтським програмним забезпеченням, що знаходиться в зоні, яка не контролюється оператором мобільного зв'язку.

Пропонована архітектурна модель SMS-комутатора наведена на рис. 1.

Основним призначенням базового модуля комутатора (рис. 1) є запуск основного потоку програмного забезпечення. Цей потік утворює усі інші потоки та допоміжні структури, завантажує конфігураційний файл, веде журнальний файл, забезпечує взаємодію із модулем керування (з підтримкою функцій інтерактивного конфігурування та перегляду статистики під час роботи сервісу).

В свою чергу, модуль керування забезпечує зв'язок сервісу з підсистемою керування сервісом за допомогою командного рядка. Модуль обробки SMPP сесії — містить у собі три базових потоки:

– потік ініціалізації підключень – перевіряє внутрішнє сховище, ініціює нові з'єднання до необхідного ESME-об'єкта та запускає новий потік для обробки SMPP сесії;

– потік одержання підключень очікує на TCP-з'єднання від будь-якого ESME-об'єкта, а також ініціює новий потік обробки SMPP сесії;

– потік обробки SMPP сесії здійснює діалог за протоколом SMPP з заданими ESME для отримання, передачі повідомлення або опрацювання службових повідомлень.

У свою чергу, модуль фільтрації виконує аналіз та фільтрацію повідомлень, що надходять до сервісу від ESME або інших SMSC. Викликається потоком обробки SMPP сесії у разі надходження повідомлення від ESME (SMSC) та потоком перевірки допоміжної бази даних у разі надходження нових повідомлень до бази даних від веб-сервісу. Модуль здійснює збереження інформації про надходження повідомлень та спрацьовування фільтрів, а також опрацьовує зміни у проміжній базі даних, що забезпечує підтримку веб-інтерфейсу контролю-керування.

Модуль фільтрації має один базовий потік, що викликає певні фільтри у певних комбінаціях в залежності від налаштування. Кожен з фільтрів виконує обробку за власним алгоритмом. Якщо один із фільтрів спрацьовує – подальша перевірка не проводиться. Залежно від налаштування, є можливість використовувати лише обрані фільтри для кожного класу повідомлень. Такий підхід

дозволяє прискорити обробку кожного запиту у тих випадках, коли достатньо часткової перевірки або у певному класі ймовірність спрацьовування певного фільтра за статистикою більша ніж у інших.

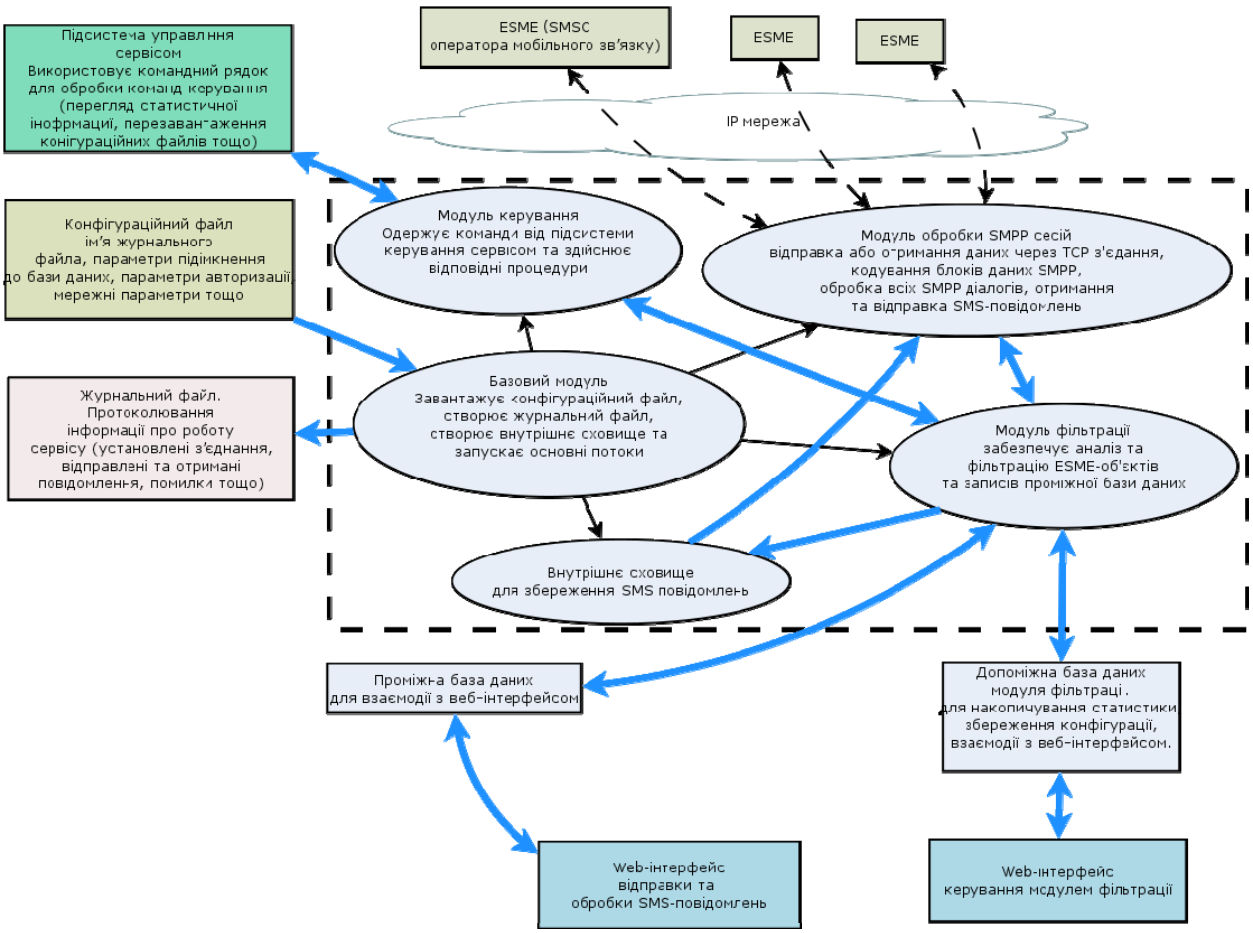

Рисунок 1 – Архітектурна модель SMS-комутатора

Кожне повідомлення за різноманітними ознаками (адреси відправника, одержувача, розмір, цільовий маршрут, зміст тощо) може бути віднесено до певного класу, що ідентифікується унікальним номером. Якщо одне й те саме повідомлення може бути віднесено до декількох класів — воно відноситься до класу, умовам якого воно задовольнило першим. Клас використовується як одна з вхідних умов до фільтра та для збору статистики про повідомлення з певними умовами.

Стандартно комутатор містить у собі такі фільтри:

– перевірка коректності PDU. Перевіряє поля та їх взаємовідносини з PDU, відхиляючи шкідливі, або некоректні запити від ESME (SMSC). Частково керується деякими експертними міркуваннями. У деяких випадках (та при відповідному налаштуванні) виправляє, за можливості, поля, приводячи їх до коректних значень та форми;

– за «чорним» або «білим» списками. Реалізує принципи «усе крім...» та «лише ...» відповідно до обраного режиму. Списки являють собою адреси, шаблони адрес або IMSI (International Mobile Subscriber Identity) відправника чи одержувача;

– за ключовими словами. Аналізує вміст повідомлення на входження до нього певних ключових слів або шаблонів, що установлюються користувачем через веб-інтерфейс;

– евристичний аналізатор. На основі байєсівського [5] класифікатора, що навчається за допомогою зібраної SMS-комутатором статистичної інформації;

– за статистичною інформацією. Рішення приймається на основі зібраної статистики про кількість повідомлень кожного класу, що дозволяє, наприклад, обмежити кількість можливих відправлень одного класу за певний час.

Однією з основних функцій модуля фільтрації є зменшення навантаження на SMSC оператора мобільного зв'язку за рахунок фільтрації, розподілення навантаження між SMSC (у випадку декількох центрів) та захисту SMSC від flood-атак та недобросовісних ESME клієнтів.

Розглянемо поступово обробку повідомлення за допомогою SMS-комутатора (рис. 2). Насамперед вхідне повідомлення від ESME (SMSC) об'єкта буде перевірене на коректність та декодоване у внутрішню структуру за протоколом SMPP. Будемо вважати, що на певному часовому інтервалі сумарний вхідний потік повідомлень має властивості нормального пуассонівського розподілу із параметром інтенсивності λ_1.

Після первинної обробки повідомлення потрапляє до внутрішнього сховища. У разі досягнення максимально можливого значення розміру сховища повідомлення відхиляється (система з кінцевим розміром черги та блокуванням).

Під час вилучення з внутрішнього сховища до SMS-повідомлення додаються певні параметри, що залежать від ESME (SMSC) об'єкта (подальший маршрут повідомлення, клас повідомлення с точки зору системи фільтрації тощо). Разом з цими даними об'єкт буде передано до відповідного набору фільтрів, де його з деякою ймовірністю *P* може бути відхилено.

Час обробки повідомлення фільтрами є найбільш впливовим фактором на швидкодію системи. Потік обслуговування системи фільтрації матиме експоненціальний розподіл з інтенсивністю μ_1. За рахунок імовірності відхилення повідомлень фільтрами маємо зниження вихідного потоку системи фільтрації $\lambda_2 = \lambda_1(1\text{-}P)$, де *P* – імовірність відхилення повідомлень.

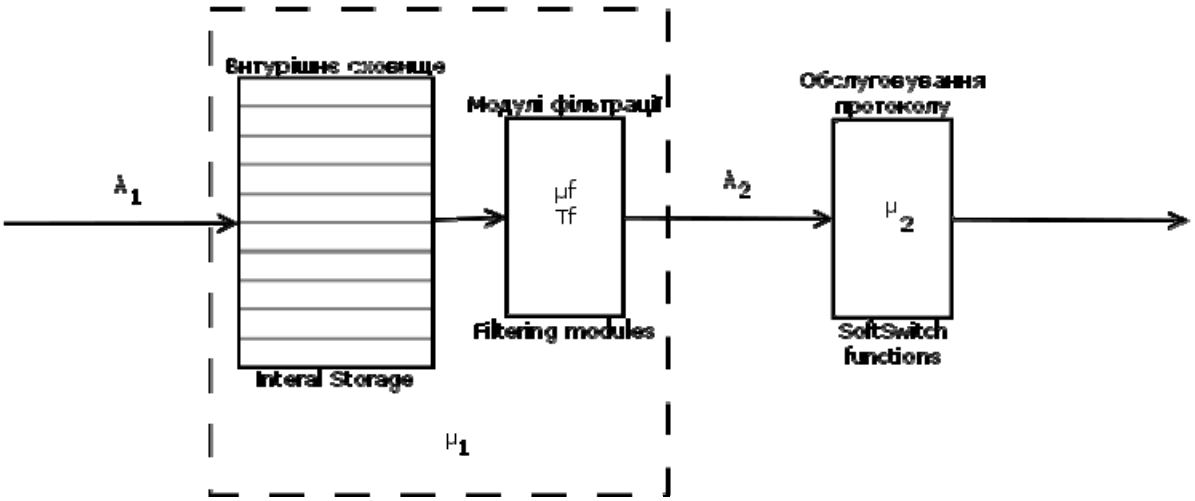

Рисунок 2 – Обробка SMS-повідомлень у модулі фільтрації

Вихідний потік фільтруючої системи (рис. 2), у свою чергу, потрапить до основного модуля (ядра комутації) з інтенсивністю обслуговування μ_2.

Слід зазначити, що кожен з фільтрів має свої власні характеристики, які за певного наближення доцільно представити як два параметри: середній час обробки одного з елементів t_i (наприклад, для фільтрації за списком це буде один елемент «чорного» або «білого» списку, для байєсівського аналізатора — гіпотеза тощо) та кількість цих елементів n_q. Перший параметр може бути визначений шляхом профілювання відповідних функцій обробки, другий є явним значенням кількості записів відповідного списку або структури. За умови лінійної обробки записів, мінімальний час обробки повідомлення дорівнюватиме часу обробки одного елемента $t_{\max} = t_i$, а максимальний відповідно добутку часу обробки одного запису та кількості елементів. При цьому середній час обробки фільтром залежно від кількості елементів та часу обробки одного елемента дорівнюватиме:

$$t_{\text{mid}}(t_i, n_q) = \frac{\sum t_i n_k}{n_q} = \frac{t_i(n_q + 1)}{2}. \qquad (1)$$

Винятком буде лише евристичний аналізатор, зважаючи на те, що для віднесення повідомлення до певного класу необхідно обчислити усі наявні гіпотези. Це призводить наближення середнього часу обробки до максимального значення часу обробки та часу відпрацьовування алгоритму аналізу.

Вочевидь, що середній час відпрацьовування потоку обслуговування буде дорівнювати сумі часів обробки кожного з фільтрів, що застосовуються для даного класу повідомлення, тобто:

$$\mu_f = \frac{1}{\sum t_{k_{\text{mid}}}}, \tag{2}$$

де $t_{k_{\text{mid}}}$ – середній час обробки повідомлення *k*-м фільтром.

Відтепер, враховуючи внутрішнє сховище з обмеженим розміром та відкиданням повідомлень за умови переповнення, система фільтрації може розглядатися за Кендалом [6] як СМО M/M/1:IS, де *IS* — загальна кількість місць обслуговування та очікування у системі, що на одиницю більше ніж розмір внутрішнього сховища програмного комутатора. Тоді згідно з [6] імовірність блокування за переповненням черги може бути визначена як:

$$P_b = \frac{(1-\rho)\rho^{IS}}{1-\rho^{IS+1}}, \tag{3}$$

де ρ – коефіцієнт завантаженості системи.

У цьому випадку $\lambda_2 = \lambda_1(1-P_b)(1-P)$, середня кількість заявок у системі:

$$\overline{N} = \frac{\rho}{1-\rho} - \frac{(IS+1)\rho^{IS+1}}{1-\rho^{IS+1}}. \tag{4}$$

За формулою Літтла [6, 7] середній час перебування у фільтруючій системі $\overline{T}_f = \frac{1}{\lambda}\overline{N}$, а час перебування у головному модулі ($\overline{T}_m$) відповідно:

$$\overline{T}_m = \frac{\overline{N}_m}{\lambda} = \left(\frac{\rho_2}{1-\rho_2}\right)\left(\frac{1}{\lambda_2}\right),$$

$$\rho_2 = \frac{\lambda_2}{\mu_2} = \frac{\lambda_1\rho_b}{\mu_2}. \tag{5}$$

При цьому загальний час обслуговування системою становитиме $\overline{T} = \overline{T}_f + \overline{T}_m$.

Зрозуміло, що визначення базових параметрів та їх оптимальних значень дозволяє підвищити ефективність функціонування будь-якого програмного комплексу, обрати для цього апаратне забезпечення бажаної швидкодії, установити можливі ролі використання тощо.

Параметрами, що найбільшим чином впливають на загальний час обробки повідомлення в пропонованій системі, є параметри підсистеми фільтрації та характеристики вхідного потоку.

Складність оцінювання полягає у щільній взаємодії всіх параметрів та необхідності під час аналізу впливу одного параметра на систему фіксувати інші значення згідно з певною метою. У нашому випадку метою є простежити за роботою системи за умов максимально можливого часу роботи підсистеми фільтрації та при значному навантажені. Для цього будемо використовувати фільтри з максимальним часом обробки повідомлень: евристичний аналізатор, фільтри за чорним списком та ключовими словами. Швидкодію кожного модуля було установлено шляхом вимірювання середніх значень для середньостатистичної серверної платформи.

На рис. 3 наведено графік залежності загального часу обробки від кількості слів-гіпотез у евристичному аналізаторі та окремо від кількості номерів у списку небажаних номерів фільтра за чорним списком. Відповідні залежності було розраховано із використанням формул (1…5) для досить значної кількості гіпотез та номерів з метою максимального наближення до умов реальної експлуатації.

З рис. 3 видно, що за умови, коли інші параметри близькі до граничних значень та під час обробки, що дорівнює 0,8 секунди, кращий результат даватиме евристичний фільтр, що оперує двома тисячами гіпотез, та фільтр за чорним списком, що використовує базу з 20-ма тисячами записів.

Такі результати свідчать про можливість застосування пропонованої моделі комутатора без суттєвого збільшення часу надходження SMS-повідомлення від відправника до одержувача.

На рис. 4 зображено типову схему взаємодії пропонованої платформи у вигляді «фільтруючої хмари» з мережами існуючих операторів мобільного зв'язку.

Відповідно до пропонованої моделі (рис. 4) весь трафік від абонентів, що надходить від ESME (SMSC) або Web-шлюзу, буде оброблятися SMS-SoftSwitch. При цьому кожен користувач має змогу у певних межах керувати своїми правилами фільтрації за допомогою спеціального Web-інтерфейсу.

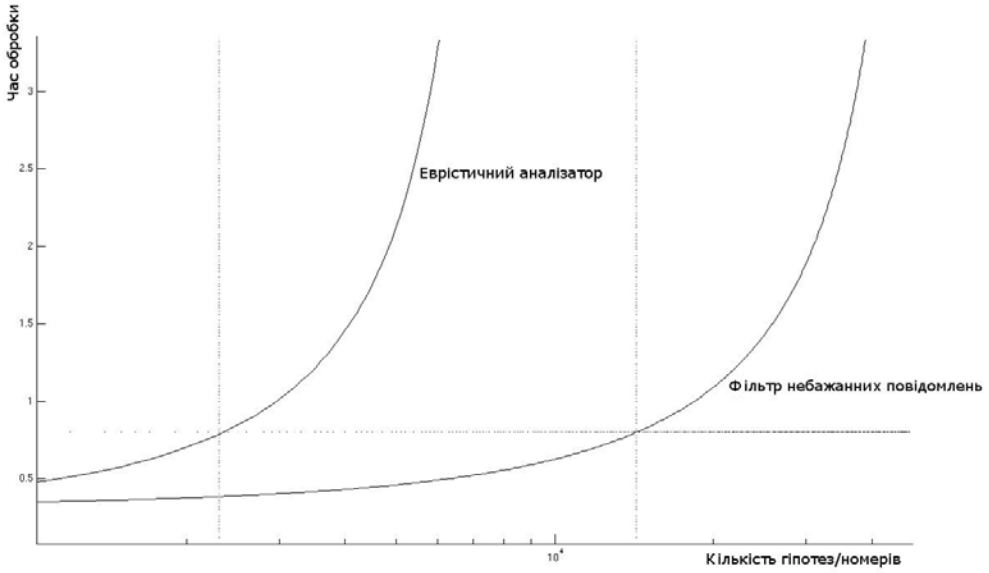

Рисунок 3 – Залежність середнього часу обробки залежно від параметрів фільтрів

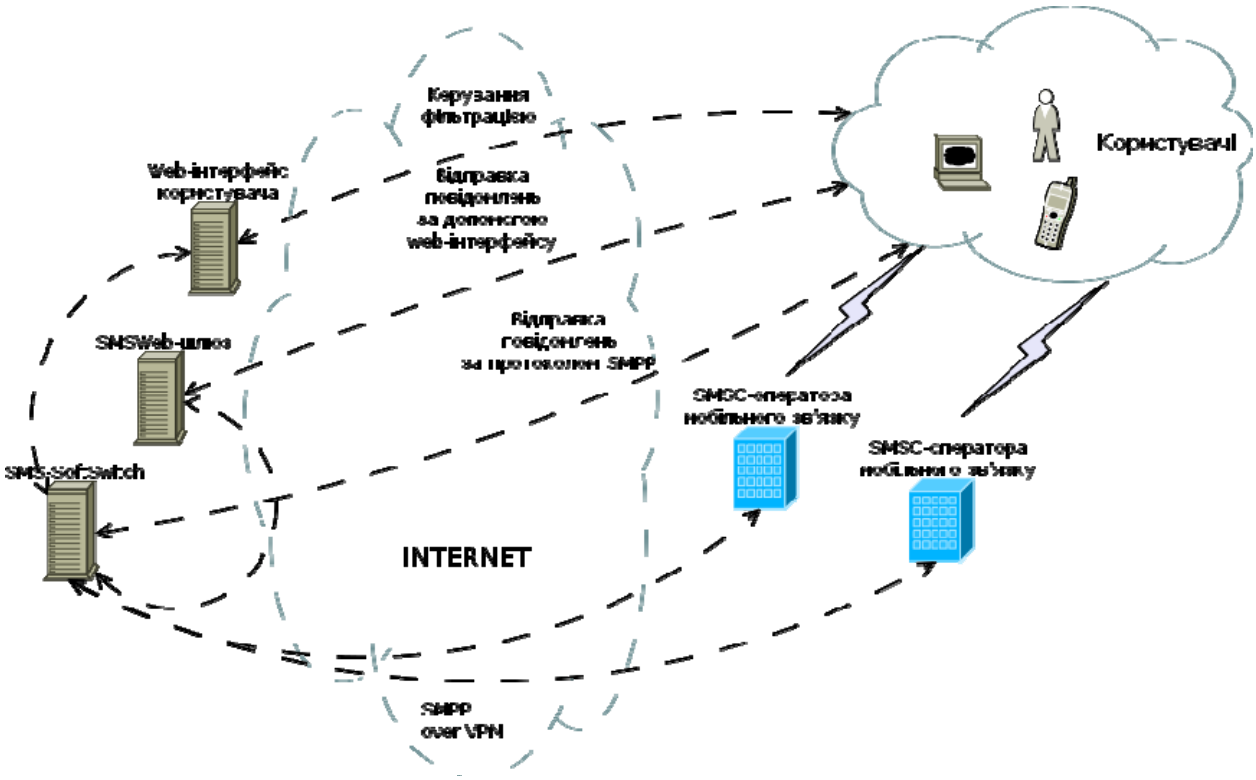

Рисунок 4 – Схема інтеграції SMS-SoftSwitch до мережі оператора

Зважаючи на те, що одним із найбільш впливових на роботу системи параметрів є “чистота” потоку, яка характеризує кількість повідомлень, що будуть відкинуті системою (на скільки буде зменшено інтенсивність подальшого потоку), в рамках подальших досліджень доцільно сконцентруватися на розробці методів оптимізації роботи фільтрів. Одним із можливих напрямів оптимізації може стати статистична оцінка частоти спрацьовування повільних (евристичних) фільтрів для повідомлень певного класу з подальшим розподілом таких повідомлень по інших фільтрах з більшою швидкодією.

На завершення можна зробити такі висновки:

1. Зростаюча популярність SMS-повідомлень призвела до появи цілої низки нових загроз, що часто призводять до матеріальних втрат, як для оператора мобільного зв'язку, так і для абонента.

2. У рамках статті було запропоновано архітектурну модель системи фільтрації SMS-повідомлень на базі розробленої авторами платформи SMS-SoftSwitch та концепцію використання цієї платформи як «фільтруючої хмари».

3. Розроблено математичну модель системи фільтрації у вигляді многофазової СМО з обмеженою чергою та отримано низку аналітичних виразів, що дозволяють визначити основні фактори, які впливають на якість обслуговування системи.

4. Установлено критичні значення базових параметрів за умови використовування системи в режимі «без оптимізації». За результатами дослідження установлено, що використовування SMS-SoftSwitch дійсно дозволяє зменшити навантаження та поліпшити надійність системи передавання SMS-повідомлень не збільшуючи суттєво час обробки повідомлень.

Література

1. *Гвинель Ле-Бодик.* Мобильные сообщения. Службы и технологии SMS, EMS, MMS. – Издательство Кудиц-Образ, 2005. – 448 с.
2. Short Message Peer to Peer Protocol Specification v3.4 [Електронний ресурс]. – Режим доступу: http://www.smsforum.net/ . – Назва з екрана.
3. RFC 793. TRANSMISSION CONTROL PROTOCOL [Електронний ресурс]. – Режим доступу: http://www.faqs.org/rfcs/rfc793.html. – Назва з екрана.
4. RFC 877. A Standard for the Transmission of IP Datagrams Over Public Data Networks [Електронний ресурс]. – Режим доступу: http://tools.ietf.org/html/rfc877. – Назва з екрана.
5. Better Bayesian filtering [Електронний ресурс]. – Режим доступу: http://paulgraham.com/better.html . – Назва з екрана.
6. *Крылов В.В.* Теория телетрафика и ее приложения / В. В. Крылов, С. С. Самохвалова. – СПб.: БХВ-Петербург, 2005. – 288 с.; іл.
7. *Бочаров П.П.* Теория массового обслуживания [учебник] / П.П. Бочаров, А.В. Печинкин. – М:. Изд-во «РУДН», 1995. – 529 с.; іл.