УДК 004.056.52: 621.391

МЕТОД АДАПТИВНОЇ ОЦІНКИ URI В КОМПЛЕКСНИХ СИСТЕМАХ ФІЛЬТРАЦІЇ КОНТЕНТУ

Каптур В.А., Князєв О.А.

Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Кузнечна,1.
vadim.kaptur@onat.edu.ua

МЕТОД АДАПТИВНОЙ ОЦЕНКИ URI В КОМПЛЕКСНЫХ СИСТЕМАХ ФИЛЬТРАЦИИ КОНТЕНТА

Каптур В.А., Князєв О.А.

Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная,1.
vadim.kaptur@onat.edu.ua

METHOD OF ADAPTIVE ESTIMATION URI IN COMPLEX SYSTEMS OF THE FILTRATION OF THE CONTENT

Kaptur V.A., Kniaziev A.A.

O.S. Popov Odessa national academy of telecommunications,
1 Kuznechna St., Odessa, 65029, Ukraine.
vadim.kaptur@onat.edu.ua

Анотація. Розглянуто процес аналізу уніфікованого ідентифікатора ресурсу в межах комплексної системи фільтрації контенту, що складається з двох або більше засобів фільтрації. Наведено алгоритм роботи системи фільтрації контенту, робота якої адаптується до характеристик зовнішнього (користувацького) середовища – адаптивної комплексної системи фільтрації контенту. Наведено деталізований опис процесу визначення оптимальної (з точки зору мінімізації часу обробки запиту) послідовності процедур оцінки відповідності URI заданим правилам. Детально розглянуто принцип роботи комплексної системи фільтрації контенту миттєвого прийняття рішення, працює за принципом «все що не дозволено – те заборонено». Запропоновано низку аналітичних виразів для обчислення часу обробки та затримки всередині комплексної системи фільтрації контенту. Розроблено алгоритми вибору найкращої послідовності засобів фільтрації, а також процедур фільтрації в межах засобу.

Ключові слова: захист дітей в мережі Інтернет, адаптивна комплексна система фільтрації контенту, універсальний ідентифікатор ресурсу, небажаний контент, час затримки.

Аннотация. Рассмотрен процесс анализа унифицированного идентификатора ресурса в рамках комплексной системы фильтрации контента, состоящей из двух или более средств фильтрации. Приведен алгоритм работы системы фильтрации контента, работа которой адаптируется к характеристикам внешней (пользовательской) среды – адаптивной комплексной системы фильтрации контента. Приведено детализированное описание процесса определения оптимальной (с точки зрения минимизации времени обработки запроса) последовательности процедур оценки соответствия URI заданным правилам. Детально рассмотрены принципы работы комплексной системы фильтрации контента мгновенного принятия решения, работающая по принципу «всё что не разрешено – то запрещено». Предложен ряд аналитических выражений для вычисления времени обработки и задержки внутри комплексной системы фильтрации контента. Разработаны алгоритмы выбора наилучшей последовательности средств фильтрации, а также процедур фильтрации в пределах средства.

Ключевые слова: защита детей в сети Интернет, адаптивная комплексная система фильтрации контента, универсальный идентификатор ресурса, нежелательный контент, время задержки.

Abstract. The process of analysis of the uniform resource identifier in the integrated content filtering system consisting of two or more filtering systems. An algorithm of the content filtering system, the operation of which is adapted to the characteristics of the external (user) environment – adaptive complex system of content filtering system. Powered by a detailed description of the process of determining the optimal (in terms of minimizing the query processing time) sequence URI conformity assessment procedures specified rules. Considered in detail the principles of integrated content filtering system of instant decision, working on the principle of "everything that is not allowed – it is forbidden". A number of analytical expressions to calculate the processing time and delays within the complex system of content filtering. The algorithms select the best sequence of filtering tools and filtering processes within the facility.

Key words: child online protection, adaptive complex system of content filtering, universal resource identifier inappropriate content, time delay.

Одним із напрямів подальшого розвитку мережі Інтернет є її регулювання з точки зору інформаційного наповнення. Сьогодні Інтернет має тенденцію до майже неконтрольованого наповнення різноманітною інформацією – від наукових статей і літературних творів до ресурсів, які містять пропаганду насильства, нецензурну лексику та/або носять відкритий порнографічний характер. Це обумовлює появу нової наукової та прикладної проблеми, яка полягає у протидії принципово новим ризикам і проблемам. Зокрема, все більшої актуальності набуває необхідність розробки теоретичних основ та формування практичних підходів щодо фільтрації контенту в мережі Інтернет.

Питання фільтрації нецільового контенту як на локальних (підприємства чи окремі користувачі), так і на глобальних рівнях досліджено у працях низки вітчизняних та зарубіжних вчених. Так, в роботах [1-3] висвітлено науково-методичні підходи щодо визначення найбільш ефективного способу організації системи фільтрації нецільового контенту в мережі організації. В працях [4, 6] досліджено світовий досвід управління інформаційною безпекою, її вплив на стабільність держави, сформовано методи захисту дитини в мережі Інтернет, а також наведено класифікацію систем виявлення небажаних втручань.

Втім, недостатньо дослідженим залишається питання адаптивної оцінки універсальних ідентифікаторів ресурсів (Universal Resource Identifier, URI) з точки зору доцільності їх блокування для конкретного користувача. Це і обумовлює актуальність дослідження цього наукового напряму та визначає **мету роботи**, яка полягає у розробці методу адаптивної оцінки URI в комплексних системах фільтрації контенту (КСФК) [8].

На сьогодні розроблено значну кількість різноманітних підходів до обмеження доступу людини до небажаної інформації. Всі ці підходи можна умовно поділити на нетехнічні та технічні. До нетехнічних підходів відносяться [7, 8]:

- регулювання контенту на рівні інформаційних ресурсів;
- регулювання процесу передавання інформації на рівні телекомунікаційних операторів та Інтернет-провайдерів;
- самоцензура на рівні користувачів (абонентів).

Основним технічним методом захисту людини від негативної інформації в мережі Інтернет є технічна фільтрація інформації, що включає у себе різноманітні засоби фільтрації небажаного контенту. До основних засобів відносяться: фільтрація на базі HTTP проксі-сервера; фільтрація на базі DNS-сервера; фільтрація на базі брандмауера (firewall); фільтрація на базі веб-клієнта [8].

Результатом стрімкого розвитку індустрії систем технічної фільтрації інформації стала поява значної кількості програмних і програмно-апаратних рішень, призначених для блокування доступу до інформаційних ресурсів в комп'ютерних мережах різного типу.

Поодинці існуючі на сьогодні рішення мають низку недоліків, які можуть бути повністю або частково вирішені за рахунок комбінування з іншими. Так, наприклад, одним з суттєвіших недоліків фільтрації на міжмережному екрані є стрімке зростання навантаження на обладнання при збільшенні кількості записів у списках фільтрації [8]. Використовуючи в

якості основного засобу фільтрації веб-клієнта, обмежуючи при цьому використання інших засобів безпосередньо на міжмережному екрані, можна перекласти завдання фільтрації безпосередньо на вбудовані до веб-клієнта механізми та досить надійно обмежити використання інших видів навантаження.

У межах КСФК [8] засоби можуть працювати у послідовному (підсилюючи один одного) або в паралельному (доповнюючи один одного) режимі. В послідовному режимі адреса або контент, що пройшли процедуру фільтрації на одному із засобів – потрапляють на вхід іншого засобу з метою повторного оброблення (наприклад, за допомогою інших методів). У свою чергу, паралельний режим припускає фільтрацію адреси через використання одного засобу фільтрації, а фільтрацію контенту із використанням іншого.

Розглянемо процес аналізу уніфікованого ідентифікатора ресурсу в межах КСФК, що складається з двох або більше засобів фільтрації, кожен з яких включає певні процедури перевірки відповідності URI тим чи іншим правилам (наприклад, на наявність або відсутність у «білому» або «чорному» списку). З погляду системи прийняття рішення про дозвіл або блокування запиту, всі КСФК можна умовно поділити на два типи:

1. Системи миттєвого прийняття рішення. КСФК цього типу базуються на послідовному виконанні процедур перевірки відповідності URI заданими правилами (з урахуванням змісту "білих" та/або "чорних" списків) з можливістю передчасного переривання процесу оцінки в разі позитивного (або негативного) спрацьовування тієї чи іншої процедури.

2. Системи накопиченого аналізу. КСФК цього типу також базуються на послідовному виконанні процедур перевірки відповідності URI заданим правилам, приймаючи рішення про дозвіл або заборону доступу до того чи іншого інформаційного ресурсу на підставі відомостей, що надходять від певної сукупності виконаних процедур (найчастіше – всіх процедур відповідності, що входять до складу КСФК).

Зрозуміло, що зміна послідовності виконання процедур перевірки відповідності URI для КСФК другого типу, як правило, не викликає зміни підсумкового часу обробки запиту і, таким чином, КСФК цього типу не можуть бути оптимізовані за цим параметром. Зважаючи на це, в подальшому, в межах цієї статті, будемо розглядати лише КСФК миттєвого прийняття рішення.

Загальний вигляд алгоритму роботи адаптивної комплексної системи фільтрації контенту (АКСФК), тобто КСФК, робота якої адаптується до характеристик зовнішнього (користувацького) середовища, показано на рис. 1.

Суть роботи АКСФК полягає в наступному: у систему надходить потік запитів від користувачів (груп користувачів); система визначає тип запиту (URI, IP-адреса тощо); відбувається перевірка на наявність користувача у системі; якщо у базі даних відсутній профіль конкретного користувача, то відбувається його додавання у систему, а також застосування для даного профілю послідовності засобів і процедур фільтрації небажаного контенту за замовчуванням; якщо профіль користувача присутній в базі даних, то для нього буде задіяний механізм, що підбирає найкращу послідовність використання способів і процедур фільтрації таким чином, щоб методи і процедури, які найчастіше спрацьовували, були в пріоритеті і спрацьовували першими. Відбувається це за допомогою підрахунку частоти застосування засобів і процедур для кожного конкретного користувача (або групи користувачів) і процесів блокування, які будуть зберігатися в базі даних.

Далі відбувається перевірка на наявність в обраного профілю рекомендованої послідовності. У разі, якщо послідовність ще не була сформована (наприклад, через недостатність статистичних даних), то в даному випадку буде застосовуватися послідовність за замовчуванням. У разі виявлення такої послідовності її буде взято за основу при прийнятті рішення про блокування або ж надання доступу щодо запитуваного ресурсу.

У процесі роботи АКСФК відбувається оновлення даних для кожного користувацького профілю про прийняті рішення блокування або ж надання доступу. На

основі цієї статичної інформації і буде працювати перебудова послідовності засобів (і процедур усередині кожного засобу) з погляду пріоритетності.

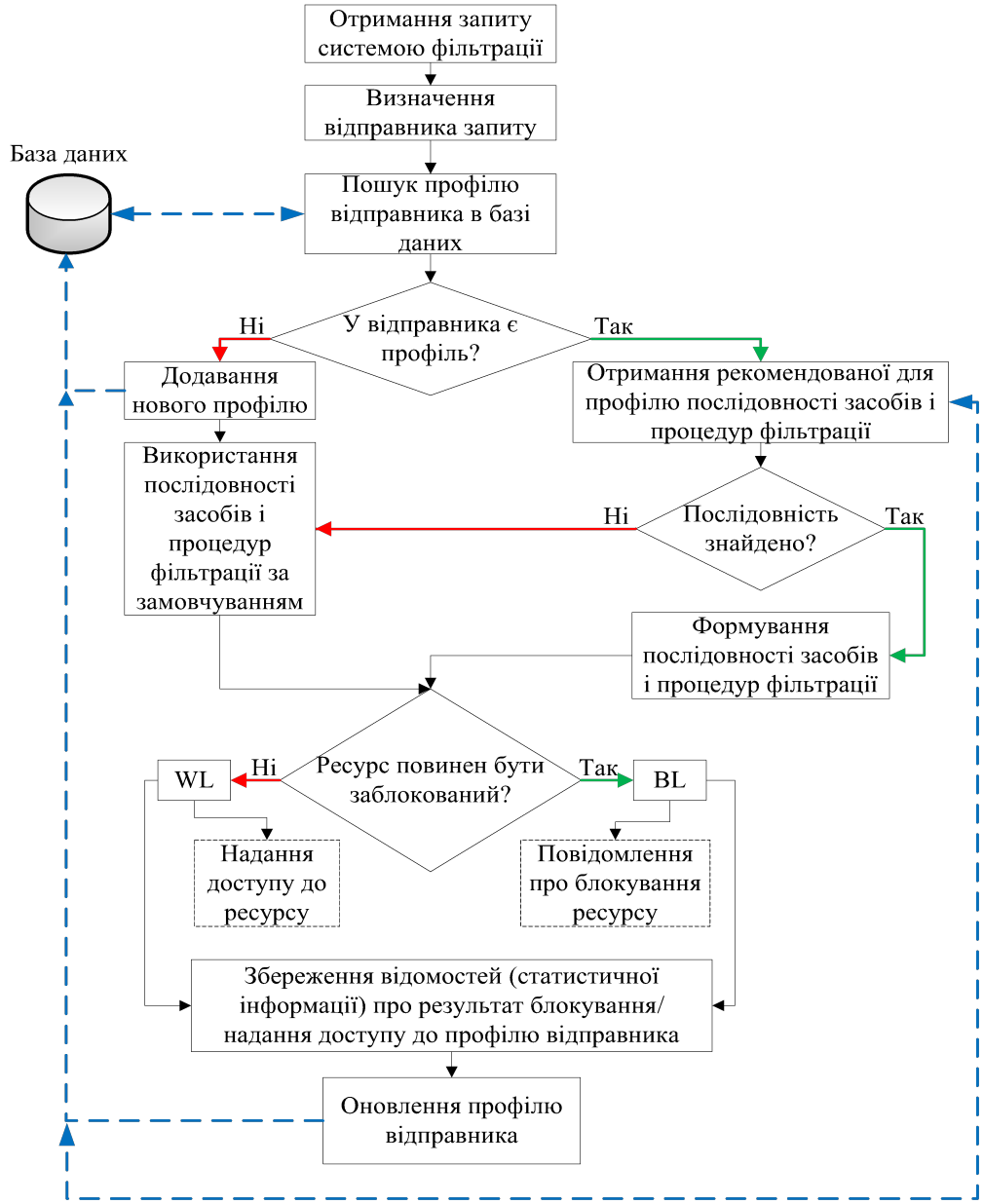

Рисунок 1 – Загальний вигляд алгоритму роботи АКСФК

Розглянемо більш детально процес визначення оптимальної (з точки зору мінімізації часу обробки запиту) послідовності процедур оцінки відповідності URI заданим правилам. Структурно процес аналізу URI в КСФК, який досліджено у низці наукових праць, зокрема [8], складається з таких етапів:

1. Запити (які в нашому випадку представлені у вигляді URI) надходять до КСФК та оброблюються вбудованою системою прийняття рішень, що базується на відомостях про профіль користувача (або групи користувачів) та прийняту для нього (або групи) політику фільтрації.

2. Система прийняття рішень, відповідно до результатів проведеного аналізу, а також згідно зі способом отримання запиту (запит надійшов до DNS-сервера, запит надійшов до proxy-сервера тощо), формує послідовність засобів фільтрації (один або більше), що

мають бути задіяні для оцінки доцільності блокування (або надання доступу) до ресурсу, що надано відповідним URI.

3. У свою чергу, кожен із засобів фільтрації (proxy-сервер, DNS-сервер, міжмережевий екран тощо) після отримання для аналізу URI формує послідовність процедур оцінювання відповідності URI заданим правилам з урахуванням доступних конкретному засобу можливостей (аналіз за доменом або доменною зоною, використання регулярних виразів, аналіз за номером порту тощо), а також із використанням відповідних «білих» або «чорних» списків (відповідно до політик фільтрації, що мають застосовуватись до конкретних користувачів).

4. У разі, якщо хоча б одна із процедур підтвердить необхідність блокування ресурсу (або надання доступу до нього), що представлено відповідним URI, КСФК має прийняти відповідне рішення (наприклад, через надсилання у відповідь сторінки із повідомленням про блокування або через надсилання запитаного контенту). У разі, якщо жодна з процедур не підтвердить необхідності блокування ресурсу (або надання доступу до нього), або хоча б одна із них підтвердить його входження до «білого» списку, КСФК має забезпечити доставку запитаного контенту користувачеві.

Очевидно, що при такому процесі тривалість аналізу URI буде безпосередньо залежати від того, яка саме за порядком процедура оцінювання прийме те чи інше рішення. Так, наприклад, у разі позитивного спрацьовування першої ж процедури (наявність ресурсу в «білому» або «чорному» списку) – час обробки запиту буде найменшим, а у разі не відповідності URI жодному з правил жодної з процедур – найбільшим.

Розглядаючи КСФК з миттєвим прийняттям рішення, можна виділити такі основні підходи: "все що не дозволено – те заборонено", "все що не заборонено – те дозволено", а також "гібридний", що працює за принципом першого позитивного, або негативного рішення.

Як приклад, на рис. 2 зображена КСФК, що працює за принципом «все що не дозволено – те заборонено». Вона складається з M засобів фільтрації, кожен з яких здійснює перевірку відповідності URI шляхом застосування N_i процедур, де $i = 1 \ldots M$ – номер засобу фільтрації в межах КСФК.

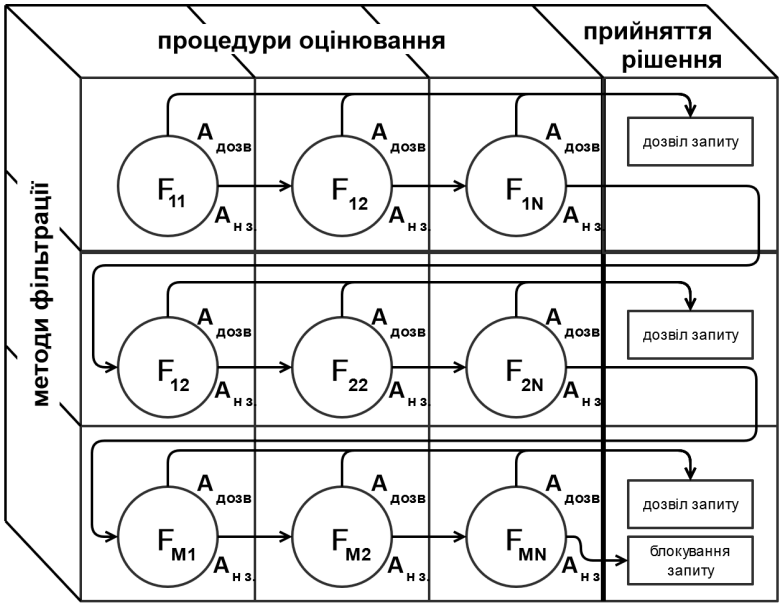

Рисунок 2 – КСФК миттєвого прийняття рішення працює за принципом «все що не дозволено – те заборонено»

Кожну таку процедуру позначено літерою F з індексами i та $j = 1 \ldots N_i$, що розміщено в колі з одним входом та двома виходами. Таким чином F_{ij} позначає процедуру оцінки відповідності URI, що знаходиться на j-му місці в межах i-го засобу фільтрації (згідно з чинним порядком застосування в межах КСФК). Аналіз URI кожною такою процедурою може завершуватись однією з двох подій, що складають собою повну систему $\{A_{дозв}, A_{нз}\}$, де $A_{дозв}$ — подія, що настає у разі виявлення збігу (відповідності) URI правилам спрацьовування процедури з урахуванням наявного "білого" списку, а $A_{нз}$ — подія, що настає у разі не виявлення такого збігу.

Очевидно, що час аналізу URI T_{ij} процедурою F_{ij} (рис. 2) залежить від виду процедури. Так, наприклад, у випадку лінійного зіставлення (накшталт перевірки запису за шаблоном) такий час буде залежати від двох ключових параметрів: кількості записів у списку відповідної процедури, а також від часу перевірки відповідності одного запису конкретному URI (тобто складності та вибагливості до ресурсів відповідної процедури). В іншому випадку, наприклад, при використанні хеш-таблиць, час пошуку хеш-коду URI по всій таблиці буде, в більшості випадків, близьким до часу перевірки відповідності одного запису.

У свою чергу, при використанні підходу "все що не заборонено – те дозволено" аналіз URI може завершуватись однією з двох подій $\{A_{блок}, A_{нз}\}$, де $A_{блок}$ — подія, що настає у разі виявлення збігу (відповідності) URI правилам спрацьовування процедури з урахуванням наявного "чорного" списку, а $A_{нз}$ – подія, що настає у разі невиявлення такого збігу. Міркування щодо часу аналізу URI T_{ij} процедурою F_{ij} для цього випадку є аналогічними попереднім.

Далі, при використанні підходу «першого позитивного рішення» відбувається перевірка за всіма наявними методами фільтрації. Якщо в процесі перевірки в межах будь-якої процедури фільтрації станеться збіг на наявність запису в «чорному» або «білому» списку, запит буде проходити перевірку наступною процедурою фільтрації на наявність такого збігу. При проходженні процесу на наявність збігу по всіх процедурах фільтрації, в кінцевому підсумку буде прийнято рішення про блокування запитуваного ресурсу або ж про дозвіл на доступ до нього. Як і в попередніх підходах, аналіз URI може завершуватися однією з двох подій: $A_{блок}$ або $A_{нз}$. Дане рішення буде ґрунтуватися на факті наявності першого збігу у «чорному» списку, тобто якщо в процесі оброблення було виявлено перший збіг у «чорному» списку, то буде прийнято рішення про блокування даного запиту.

Аналогічним є підхід «першого негативного рішення», але в процесі аналізу URI, рішення буде ґрунтуватися на факті наявності першого збігу в «білому» списку, тобто, якщо в процесі оброблення було виявлено перший збіг у «білому» списку, то буде прийнято рішення про дозвіл доступу на даний ресурс.

У процесі аналізу, результат обробки URI буде безпосередньо залежати від того, яка саме за порядком процедура оцінювання прийме те чи інше рішення. Так, наприклад, у разі позитивного спрацьовування першої ж процедури (наявність ресурсу в «білому» або «чорному» списку) час обробки запиту буде найменшим, а у разі невідповідності URI жодному з правил жодної з процедур – найбільшим.

Враховуючи той факт, що процедур в конкретному засобі фільтрації може бути досить багато, позначимо як S_{ij} кількість записів у списку, що знаходиться на j-му місці в межах i-го засобу фільтрації (згідно з чинним порядком застосування в межах КСФК). Кожна перевірка списку здійснюється процедурою певного виду $F = \{F_1, F_2, F_3 ... F_k\}$, де k – кількість видів процедур.

У процесі перевірки на збіг у списку процедурою виду F витрачається певний час τ. Відповідно, кожна перевірка процедурами видів $\{F_1, F_2, F_3 ... F_k\}$ буде супроводжуватися конкретним часом $\{\tau_{F1}, \tau_{F2}, \tau_{F3} \ldots \tau_{Fk}\}$.

Зазвичай, для більшості процедур оцінки відповідності час обробки конкретною процедурою безпосередньо залежить від розміру списку, що перевіряється тобто $\tau_{Fk}=\{f(S,\Delta\tau)\}$, де $\Delta\tau$ – час обробки одного запису в списку.

Враховуючи той факт, що в процесі перевірки на збіг URI у різних списках буде витрачатися різний час, що залежить від місцезнаходження URI у самому списку, можна дійти висновку, що чим ближче URI буде перебувати до початку списку, тим менше буде витрачатися час на обробку запиту. Виходячи з цього, проведені в роботі дослідження дозволяють констатувати, що за умов відсутності URI у списку буде витрачатися максимальний час обробки процедури($Sij\,\Delta\tau$), зважаючи на те, що має бути проаналізований весь список на наявність збігу. Відсутність URI у списку є аналогічним місцезнаходженню URI останнім записом у списку, тобто на пошук буде витрачатися максимальний час. Відповідно, мінімальний час обробки процедури ($\Delta\tau$) буде в тому випадку, якщо URI буде знаходитися першим записом у списку, що є часом обробки одного запису, тобто $\Delta\tau$. Якщо ж URI знаходиться у середині списку, то час обробки буде дорівнювати $\frac{Sij}{2}\cdot\Delta\tau$.

Процес прийняття рішення про вихід із засобу фільтрації надамо у вигляді системи подій $\Omega_{\text{проц}}=\{A_1, A_2, A_3 ... A_n\}$, де A_n – подія виходу із засобу фільтрації після *n*-ї процедури (наприклад, прийнято рішення фільтрувати вхідний запит).

Зважаючи на те, що СФК не може наперед визначити, яка саме подія настане, ці події можна вважати випадковими з відповідними ймовірностями $P(A_1, A_2, A_3 ... A_n)$[9]. При цьому $\sum_{i=1}^{Sij} P(Ai) = 1$.

Таким чином, при настанні події A_1 час обробки запиту буде дорівнювати $\Delta\tau$. У свою чергу, при настанні події A_2, він буде дорівнювати $2\cdot\Delta\tau$, а при настанні події A_n, він буде дорівнювати $S_{ij}\cdot\Delta\tau$.

Порядок проходження можна вважати оптимальним у тому випадку, якщо середній час обробки запиту до прийняття того чи іншого рішення буде мінімальним. Приймаючи, що середній час порівняння URI запиту із записом у списку блокування і середній час тестування URI регулярним виразом є величини постійні і приблизно еквівалентні, а середній час обробки запиту залежить від кількості записів у списках фільтрації або кількості регулярних виразів, отримаємо формулу для визначення «загального часу обробки вхідного запиту»:

$$T^{ij}_{\text{обробки}} = \sum_{v=1}^{Sij} (P(Av)\cdot v\cdot\Delta\tau)\ , \qquad (1)$$

де *v* – кількість записів у списку; $\Delta\tau$ – час обробки одного запису у списку (із застосуванням відповідної процедури); $P(A_v)$ – ймовірність позитивного спрацьовування процедури на позиції *v* чинного списку.

Час обробки вхідного запиту всіма процедурами відповідності в межах однієї СФК можна визначити за формулою:

$$T^{i}_{\text{обробки}} = \sum\nolimits_{j=1}^{Mi} T_{ij}\,, \qquad (2)$$

де M_i – кількість процедур відповідності в межах однієї СФК.

Процес прийняття рішення в процесі роботи всього алгоритму також може бути описано за допомогою системи подій $\Omega_{\text{зас}} = \{A_1^{\text{вих}}, A_2^{\text{вих}}, A_3^{\text{вих}} ... A_{M_i}^{\text{вих}}\}$ При цьому процес виходу з алгоритму характеризується ймовірностями $P(A_1^{\text{вих}}, A_2^{\text{вих}}, A_3^{\text{вих}} ... A_{M_i}^{\text{вих}})$. Зважаючи на це, формула для обчислення часу середньої затримки буде мати вигляд:

$$T^{i}_{\text{обробки}} = \sum_{j=1}^{Mi}(P(A_j^{\text{вих}}) \cdot \left\lfloor \sum_{v=1}^{S_{ij}}(P(A_v) \cdot v \cdot \Delta\tau) \right\rfloor). \quad (3)$$

На основі цієї формули складемо алгоритм, що відповідає за підбір найкращої послідовності засобів і процедур фільтрації небажаного контенту в рамках АКСФК (рис. 3).

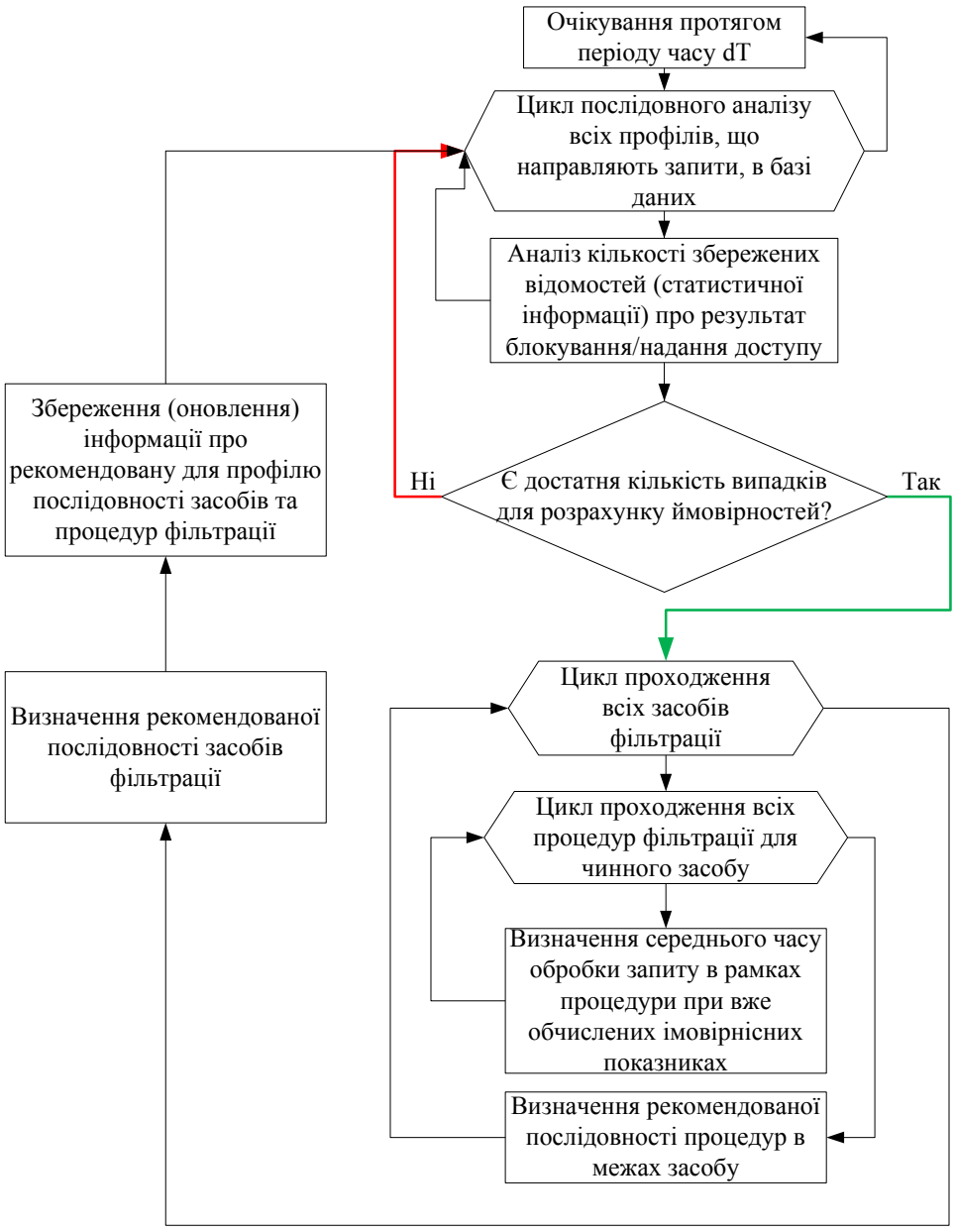

Рисунок 3 – Алгоритм вибору найкращої послідовності

В процесі роботи алгоритму відбувається створення рекомендованої послідовності способів і процедур фільтрації небажаного контенту. Даний алгоритм працює паралельно з загальним алгоритмом роботи АКСФК (рис. 1). Визначення статистичних показників ґрунтується на результаті ухвалення рішення (блокування або надання доступу до запитуваного ресурсу). Наприклад, якщо для певного користувача більшість запитів блокувалося за результатами спрацьовування п’ятої за порядком процедури, то система має перемістити його на початкову позицію та, тим самим, прискорити загальний час обробки запиту в АКСФК.

Результатом роботи даного алгоритму має стати рекомендована послідовність засобів (та процедур) фільтрації для конкретного профілю користувача з подальшим збереженням (оновленням) інформації для профілю користувача.

В процесі роботи алгоритму підбирання найкращої послідовності, відбувається визначення рекомендованої послідовності процедур у межах засобу фільтрації (рис. 4).

Переміщення процедури в позиції може відбуватись за рахунок сортування простими обмінами, іншими словами сортування бульбашкою, алгоритм якої докладно описано у [10].

Проведений аналіз існуючих систем фільтрації контенту продемонстрував наявність переваг та недоліків у кожного із них та підтвердив доцільність застосування комплексних систем фільтрації контенту як основи для сучасних рішень у сфері захисту людини від небажаної інформації.

Рисунок 4 – Визначення рекомендованої послідовності фільтрації процедур у межах засобу

Запропонований метод адаптивної оцінки URI в комплексних системах фільтрації контенту дозволяє будувати принципово нові типи КСФК, у яких послідовність виклику процедур оцінки відповідності формується відповідно до статистичних показників, накопичених системою протягом певного часу. Цей підхід відрізняється від існуючих тим, що в процесі роботи адаптивної комплексної системи фільтрації контенту відбувається адаптація до користувача (груп користувачів), яка виражається у вигляді підстроювання параметрів системи таким чином, що процедура фільтрації, яка застосовується частіше всіх, буде в пріоритеті над іншими, та буде спрацьовувати першою.

Також одержані аналітичні вирази дозволяють визначити середній час затримки запиту в межах КСФК, що дозволяє в майбутньому створити імітаційну модель роботи адаптивної комплексної системи фільтрації контенту та виконати її програмну реалізацію.

ЛІТЕРАТУРА:

1. Воробієнко П.П. Єдина система обмеження доступу до нецільових ресурсів мережі Інтернет в освітніх закладах України / П.П. Воробієнко, В.А. Каптур, В.А Коляденко, В.О. Самодід // Комп'ютер у школі та сім'ї. – 2009. – № 8. – С. 30-34.
2. Kaptur V. Current status and prospects of the content filtering methods in the telecommunication networks // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, P. 113-119.
3. Каптур В.А. Система фільтрації SMS-повідомлень в мережі оператора мобільного зв'язку / В.А. Каптур, А.Г. Ложковський, М.В. Фурмур, Р.В. Чумаков // Наукові праці ОНАЗ ім. О.С. Попова. – 2011. – № 2. – С. 19-24.
4. Баранов А.А. Региональная инициатива «Создание центра по защите детей в сети Интернет для региона СНГ» / А.А. Баранов, В.А. Каптур // Региональное подготовительное собрание для стран СНГ к ВКРЭ-14, (Кишинёв, Молдова, 19-21 февраля 2013). Документ RPM-CIS13/08.
5. Шевченко В.Л. Лучшие мировые практики управления информационной безопасностью и их влияние на экономическую стабильность государства / В.Л. Шевченко // Сучасні інформаційно-телекомунікаційні технології: матеріали науково-технічної конф., (м. Київ, 17-20 листопада 2015 р.). У 5 томах. – Т. IV. Сучасні технології інформаційної безпеки. – К.: ДУТ, 2015. – С. 5-7.
6. Корченко А.А. Базовые признаки классификации систем обнаружения вторжений / С.Т. Ахметова, Корченко А.А. // Сучасні інформаційно-телекомунікаційні технології: матеріали науково-технічної конф, (м. Київ, 17-20 листопада 2015 р.). У 5 томах. – Т. IV. Сучасні технології інформаційної безпеки. – К.: ДУТ, 2015. – С. 25-27.
7. Каптур В.А. Визначення умов доцільності застосування комплексних систем фільтрації контенту / В.А. Каптур, І.А. Поднебесний // Наукові праці ОНАЗ ім. О. С. Попова. - 2014. - № 2. - С. 64-70.
8. Каптур В.А. Комплексні системи фільтрації контенту в мережі Інтернет / В.А. Каптур // Наукові праці ОНАЗ ім. О.С. Попова. – 2013. – № 1. – С. 16-21.
9. Зайцев Д.А. Моделирование телекоммуникационных систем в CPN Tools / Д.А. Зайцев, Т.Р. Шмелева. – Одесса: ОНАС, 2008. – С. 68.
10. Интернет-библиотека. Сортировка пузырьком [Електронний ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Сортировка_пузырьком.

REFERENCES:

1. Vorobiyenko P., Kaptur V., Kolyadenko V., and Samodid V. "Unified Limit Access to Inappropriate Internet in Educational Institutions of Ukraine."The Computer in the School and the Family 8th ser. (2009): 30-34. Web.
2. Kaptur V. "Current Status and Prospects of the Content Filtering Methods in the Telecommunication Networks." Ukrainian Scientific Journal of Information Security 8th ser. 20.2 (2014): 113-19. Web.
3. Kaptur V., Lozhkovskyy A., Furmur M., and Chumakov R. "Filtration System SMS-messages on the Network of Mobile Operator." Proceedings of the O.S. Popov ONAT 2nd ser. (2011): 19-24.
4. Baranov A., and Kaptur V. "Regional Initiative "Creating the Child Protection Centre in the Internet for the CIS Region." Regional Preparatory Meeting for the CIS Countries to WTDC-14, Kishinev, Moldova: 19-20 Feb. 2013. Document RPM-CIS13/08.

5. Shevchenko V. "The World's Best Practice Information Security Management and Their Impact on the Economic Stability of the State."Modern Information and Telecommunication Technologies: Materials Science Conference (Kyiv, 17-20 November 2015) 5.4 (2013): 5-7. Web. 17-20 Nov. 2015.
6. Korchenko A., and Akhmetova S. "Basic Features of the Classification of Intrusion-detection Systems." Modern Information and Telecommunication Technologies: Materials Science Conference (Kyiv, 17-20 November 2015) 5.4 (2015): 25-27. Web.
7. Kaptur V., and Podnebesny I. "Determination the Feasibility of Using Integrated Content Filtering Systems." Proceedings of the O.S. Popov ONAT 2 (2014): 64-70. Web.
8. Kaptur V. "Integrated Filtering Content Systems in the Internet." Proceedings of the O.S. Popov ONAT 1 (2013): 16-21. Web.
9. Zaitsev D., and Shmeleva T. "Simulating Telecommunication Systems with CPN Tools." Students' Book. – Odessa: ONAT (n.d.): 68. Web.
10. Bubble sort – Available at: https://en.wikipedia.org/wiki/Bubble_sort.