УДК 004.056.52:621.391

Каптур В.А., Гуляєв К.Д., Поднебесний І.А.
Каптур В.А., Гуляев К.Д., Поднебесный И.А.
Kaptur V.A., Guliaev K.D., Podnebesniy I.A.

МЕТОДИКА ВИБОРУ КОНФІГУРАЦІЇ СИСТЕМ ФІЛЬТРАЦІЇ НЕЦІЛЬОВОГО КОНТЕНТА ДЛЯ КОРПОРАТИВНИХ МЕРЕЖ

МЕТОДИКА ВЫБОРА КОНФИГУРАЦИИ СИСТЕМ ФИЛЬТРАЦИИ НЕЦЕЛЕВОГО КОНТЕНТА ДЛЯ КОРПОРАТИВНЫХ СЕТЕЙ

SELECTION OF THE CONTENT FILTERING SYSTEMS CONFIGURATION FOR CORPORATE NETWORKS

Анотація. Запропоновано модель корпоративної мережі, яка дозволяє систематизувати її ключові характеристики на різних рівнях. Розроблено методику вибору конфігурації систем фільтрації нецільового контента, що базується на покроковому визначенні припустимих конфігурацій на базі висунутих до системи фільтрації вимог. Продемонстровано можливості програмної реалізації методики.

Аннотация. Предложена модель корпоративной сети, которая позволяет систематизировать её ключевые характеристики на различных уровнях. Разработана методика выбора конфигурации систем фильтрации нецелевого контента, базирующаяся на пошаговом определении допустимых конфигураций на основе выдвинутых к системе фильтрации требований. Продемонстрированы возможности программной реализации методики.

Summary. The model of the corporate network, which allows to organize its key characteristics at different levels. The method for selection of the inappropriate content's filtering systems configuration for corporate networks, based on the stepwise determination of allowable configurations on the basis requirements to the filtering system. The possibilities of software implementation techniques are demonstrated.

Зважаючи на бурхливий розвиток мережі Інтернет, який спостерігається в останні роки, все більшої актуальності набуває проблема відсутності потрібної фільтрації контента, під час його передавання від інформаційного ресурсу до споживача. Необхідність вирішення таких завдань, як захист дітей в мережі Інтернет, блокування небажаної реклами та шкідливого програмного забезпечення, дотримання корпоративної політики щодо заборони доступу до розважальних ресурсів у робочий час та навіть цензура (для країн із законодавчо обмеженою свободою слова) створили передумови для розвитку цілої індустрії систем фільтрації контента (СФК). Результатом цього розвитку стала поява значної кількості програмних та програмно-апаратних рішень, призначених для блокування доступу до інформаційних ресурсів мережі Інтернет на різних рівнях (безпосередньо на робочій станції користувача, на боці провайдера, в точках обміну навантаженням операторів телекомунікацій тощо).

Під час попередніх досліджень [1] було розроблено узагальнену модель фільтрації контента в мережі Інтернет, яка дозволила провести класифікацію існуючих засобів, видів, методів та підходів до фільтрації на основі аналізу процесу передавання http-навантаження. Проте навіть поверхневий аналіз різних засобів фільтрації (веб-клієнт, proxy-сервер, DNS-сервер, міжмережний екран) показав наявність переваг і недоліків у кожного з них [1, 2] та дозволив зробити висновок про доцільність створення методики вибору оптимального, як з технічної, так і з економічної точок зору, варіанта конфігурації систем фільтрації нецільового контента для корпоративних мереж різного призначення.

Метою статті є розробка методики вибору конфігурації систем фільтрації контента для корпоративних мереж.

Серед основних факторів, що впливають на вибір конфігурації системи фільтрації контента можна назвати такі, як: масштаб корпоративної мережі; мережна архітектура; спосіб підключення до мережі Інтернет; наявність фахівців для створення або обслуговування СФК; наявність техніки для розгортання СФК; внутрішня політика організації щодо роботи в мережі Інтернет; характер користувачів тощо. На рис. 1 наведено узагальнену модель мережі організації, що відображає зазначені фактори.

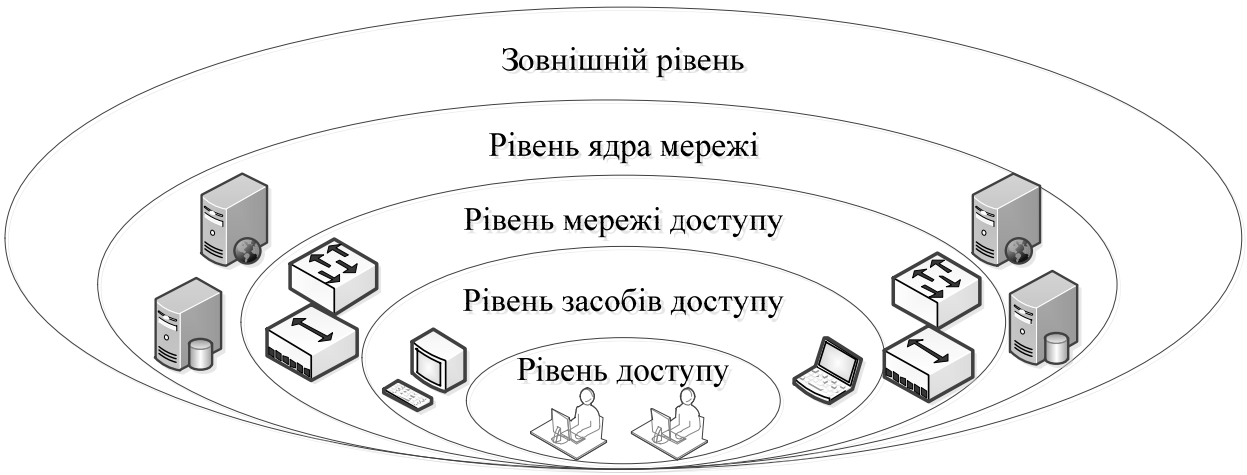

Рисунок 1 – Узагальнена модель мережі організації

Так, наприклад, базовою характеристикою рівня доступу пропонованої моделі (рис. 1) є тип контента, що завантажується із зовнішніх мереж користувачами корпоративної мережі. Зважаючи на те, що в межах однієї організації (установи) можуть бути декілька груп користувачів, що мають різний профіль споживання контента, в межах моделі кожній з таких груп має відповідати перелік певних типів контента та його орієнтовна частка у загальному обсязі інформації, що завантажується через канали зв'язку із зовнішніми мережами.

Крім типу контента важливою характеристикою рівня доступу є мережні сервіси (системи миттєвого передавання повідомлень, системи віддаленого доступу, системи електронного документообігу тощо), що використовуються користувачами корпоративної мережі. Це пояснюється тим, що деякі СФК можуть бути не сумісні зі спеціальними мережними протоколами, які застосовуються у зазначених сервісах (не мають можливості фільтрувати контент, що передається із використанням таких протоколів, або блокуючи один вид навантаження, автоматично блокують й інші).

Також при виборі СФК важливо враховувати частку регулярно відвідуваних користувачами зовнішніх ресурсів по відношенню до загального переліку ресурсів, що зазвичай використовуються користувачами корпоративної мережі. Залежно від цього параметра, можна вибрати одну з політик доступу: «дозволено все, що не заборонено» («чорні списки») або «заборонено все, що не дозволено» («білі списки»).

Також на рівні доступу важливо враховувати, чи використовується в корпоративній мережі доступ до ресурсів по каналах з шифруванням, наприклад, доступ по протоколах HTTPS або SSH, зважаючи на те, що фільтрацію навантаження, що передається з використанням цих протоколів, можуть виконувати лише певні категорії СФК.

На рівні засобів доступу пропонованої моделі (рис. 1) розміщується програмне та апаратне забезпечення, що використовується користувачами для доступу до зовнішніх мереж. Одним із найважливіших параметрів цього рівня є перелік використовуваних в корпоративній мережі операційних систем, оскільки певний клас СФК вимагає установлення на робочу станцію користувача додаткового програмного забезпечення.

Наступним параметром, який потрібно враховувати на рівні засобів доступу, є наявність у корпоративній мережі «тонких» клієнтів. Даний клас персональних комп'ютерів для своєї роботи вимагає певної конфігурації мережі, а отже в установлюваної СФК повинна бути можливість гнучкого налаштування фільтрації мережевих протоколів.

Рівень мережі доступу моделі, зображеної на рис.1, передбачає урахування існуючої мережної інфраструктури (способу адресації, складу мережного обладнання тощо). Так, наприклад, якщо в корпоративній мережі на рівні доступу застосовуються керовані комутатори, частину завдань з фільтрації контента можна перекласти саме на мережне обладнання.

На рівні ядра мережі (рис. 1) розглядається взаємодія користувачів корпоративної мережі із зовнішніми мережами та із серверами внутрішніх мережних сервісів. Аналіз параметрів даного рівня

дуже важливий, оскільки більша частина систем фільтрації передбачає установлення апаратно-програмних засобів саме на рівні ядра мережі.

Одним із найбільш важливих параметрів цього рівня є спосіб підключення корпоративної мережі до зовнішніх мереж, кількість каналів доступу та їх характеристики. Частина СФК базується на використанні таких засобів фільтрації, як DNS та / або proxy-сервери, отже, якщо в корпоративній мережі вони вже установлені, то для організації повноцінної СФК достатньо зробити додаткові налаштування вже функціонуючого засобу і, таким чином, зменшити вартість впровадження СФК.

Останнім рівнем запропонованої моделі (рис. 1) є зовнішній рівень. На даному рівні розглядаються зовнішні мережеві сервіси (наприклад, ті, що надаються провайдером).

На рис. 2 представлений узагальнений алгоритм вибору СФК. Вихідними даними для роботи алгоритму є дані про корпоративну мережу (відповідно до моделі зображеної на рис. 1), інформація про політику обмеження доступу до інформаційних ресурсів, а також економічні показники та база даних, присутніх на ринку СФК.

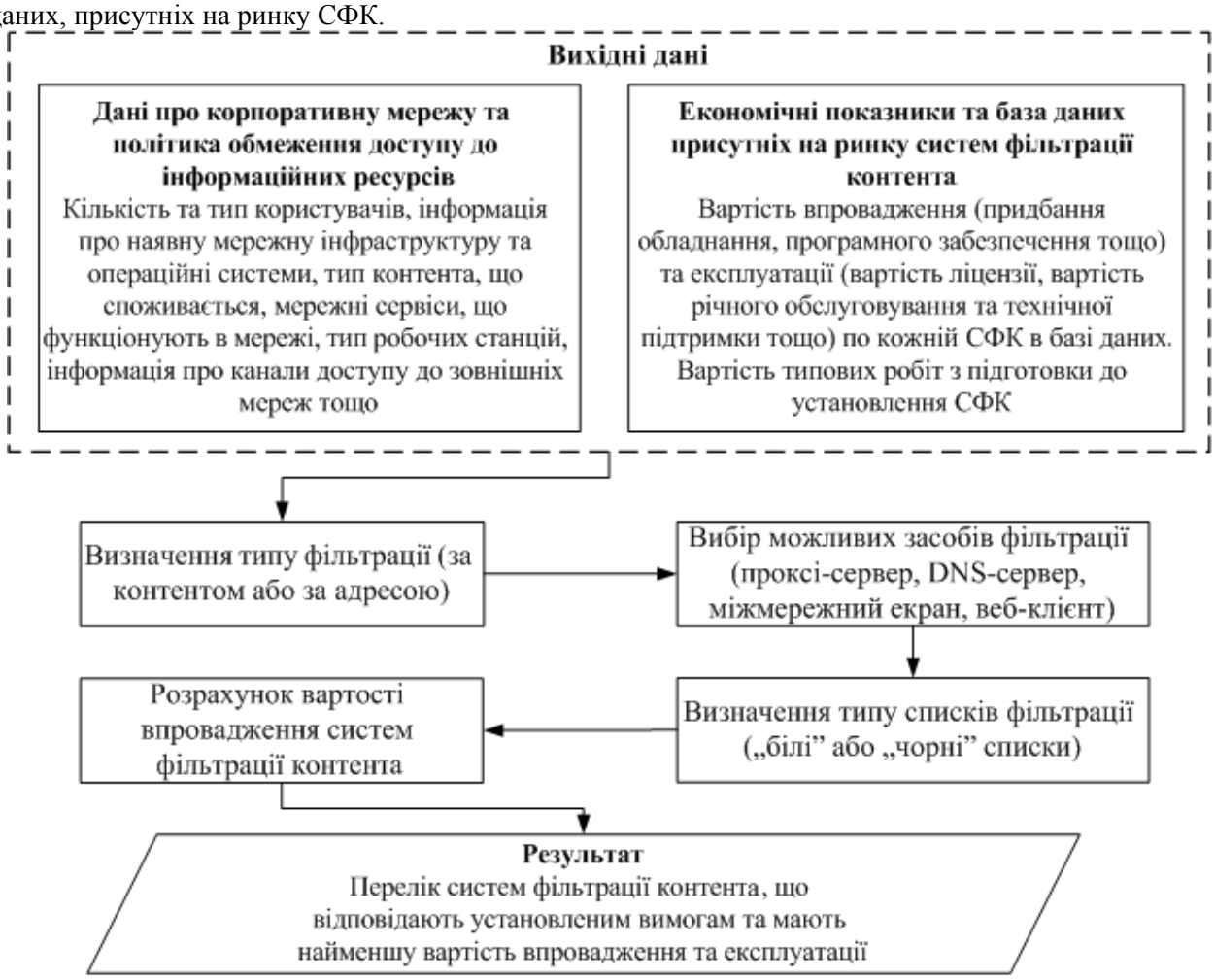

Рисунок 2 – Узагальнений алгоритм вибору системи фільтрації контента

Структурно алгоритм вибору СФК (рис. 2) являє собою послідовність кроків, що призначені для визначення всіх конфігурацій систем фільтрації контента, що відповідають установленим вимогам до типу фільтрації, засобу фільтрації, типів списків фільтрації тощо.

В зв'язку з тим, що більшість ресурсів мережі Інтернет крім корисної інформації містять розважальний контент, необхідно прийняти рішення чи слід блокувати такі ресурси повністю. Системи фільтрації, що використовують для аналізу ресурсу тільки його адресу, не дозволяють гнучко блокувати лише ті фрагменти сторінки, які містять нецільовий контент (за виключенням ситуації, коли ці фрагменти завантажуються з різних вузлів). Це саме стосується і ситуації коли завданням є не блокування нецільового ресурсу в повному обсязі, а лише перешкоджання відображенню його певних елементів (нецензурних фраз, порнографічних зображень тощо). У цьому

випадку необхідно використовувати фільтрацію за контентом, а використання фільтрації за адресами є неприпустимим.

Також потрібно взяти до уваги те, що сервіси з перекладу Інтернет-ресурсів можуть використовуватися для обходу системи фільтрації. Якщо такі сервіси необхідні для роботи підприємства, слід також використовувати фільтрацію по контенту [3, 4].

Найбільш складним з алгоритмів першої групи є алгоритм вибору засобів фільтрації (рис. 3). Перед застосуванням цього алгоритму адміністратор корпоративної мережі має відповісти на низку питань щодо бажаної архітектури СФК та її властивостей (можливість роботи у разі відмови центрального сервера, необхідність блокування окремих типів навантаження, необхідність блокування по сигнатурах протоколів або по порту призначення тощо). Також на цьому кроці використовуються відомості про обраний тип фільтрації (за контентом або за адресою).

В основу вибору оптимальної (з технічної та економічної точок зору) конфігурації СФК для певної організації покладено принцип порівняння обсягу капітальних і експлуатаційних витрат на основі показника "чистого грошового потоку", який розраховується лише з урахуванням витратної частини.

З цією метою скористаємося методом приведеної вартості (чиста поточна вартість від англ. Net Present Value – NPV) [5]. Загальна формула розрахунку якої, має такий вигляд:

$$\mathrm{NPV} = (\sum_{\mathrm{i}=0}^{\mathrm{t_{ok}}} PV_i) - S_{\text{кап}}\,, \tag{1}$$

де $\mathrm{t_{ok}}$ – період урахування експлуатаційних витрат, роки; PV – поточна вартість, грн. (дисконтований чистий грошовий потік, спричинений інвестиціями, який може бути визначений як $\mathrm{PV_i} = CF_i \times Kd_i$); $\overline{CF}$ – середньорічна сума чистого грошового потоку за період експлуатації системи, що для нашого випадку має негативне значення та визначається виключно експлуатаційними витратами, грн; Kd_i - коефіцієнт дисконтування, що визнається як $Kd_i = \dfrac{1}{(1+t_x)^i}$, де t_x – ставка дисконтування, що може бути прийнята за індекс інфляції; i – індекс періоду (року); $S_{\text{нап}}$ – обсяг капітальних інвестицій може бути визначений, як сума одноразових витрат на модернізацію необхідної для роботи СФК мережної інфраструктури ($S_{\text{інфл}}$) та обсягу витрат безпосередньо на впровадження СФК ($S_{\text{впров}}$), грн.

Вартість модернізації необхідної для роботи СФК мережної інфраструктури розраховується в такий спосіб:

$$S_{\text{інфр}} = N_{\text{серв}} \cdot S_{\text{серв}} + \sum_i N_{\text{акт.}} \cdot S_{\text{акт.}i} + L \cdot S_{\text{скс}}\,, \tag{2}$$

де $N_{\text{серв}}$ – кількість установлюваних серверів; $S_{\text{серв}}$ – вартість одного сервера, грн.; $N_{\text{акт.}}$ – кількість одиниць активного мережного обладнання *i*-го типу, що необхідно додатково установити в мережі; $S_{\text{акт.}i}$ – вартість одиниці активного мережного обладнання *i*-того типу, грн.; $S_{\text{скс}}$ – вартість побудови або модифікації існуючої структурованої кабельної системи (СКС) із розрахунку за один метр, грн.; *L* – довжина СКС, що потребує будівництва (модернізації), м.

В свою чергу вартість впровадження системи фільтрації $S_{\text{впров}}$ може бути розрахована, як:

$$S_{\text{впров}} = S_{\text{ліцензії}} + S_{\text{год}} \cdot \sum_i N \cdot T_{\text{налашт}} + S_{\text{відр}}\,, \tag{3}$$

де $S_{\text{ліцензії}}$ – загальна вартість ліцензії на використання СФК, грн.; $S_{\text{год}}$ – вартість години роботи з інсталяції необхідного апаратного та програмного забезпечення, грн.; *N* – кількість одиниць обладнання *i*-го типу, що необхідно налаштувати; $T_{\text{налашт}}$ – час налаштування обладнання *i*-го типу, год., $S_{\text{відр}}$ – вартість відрядження працівників, грн.

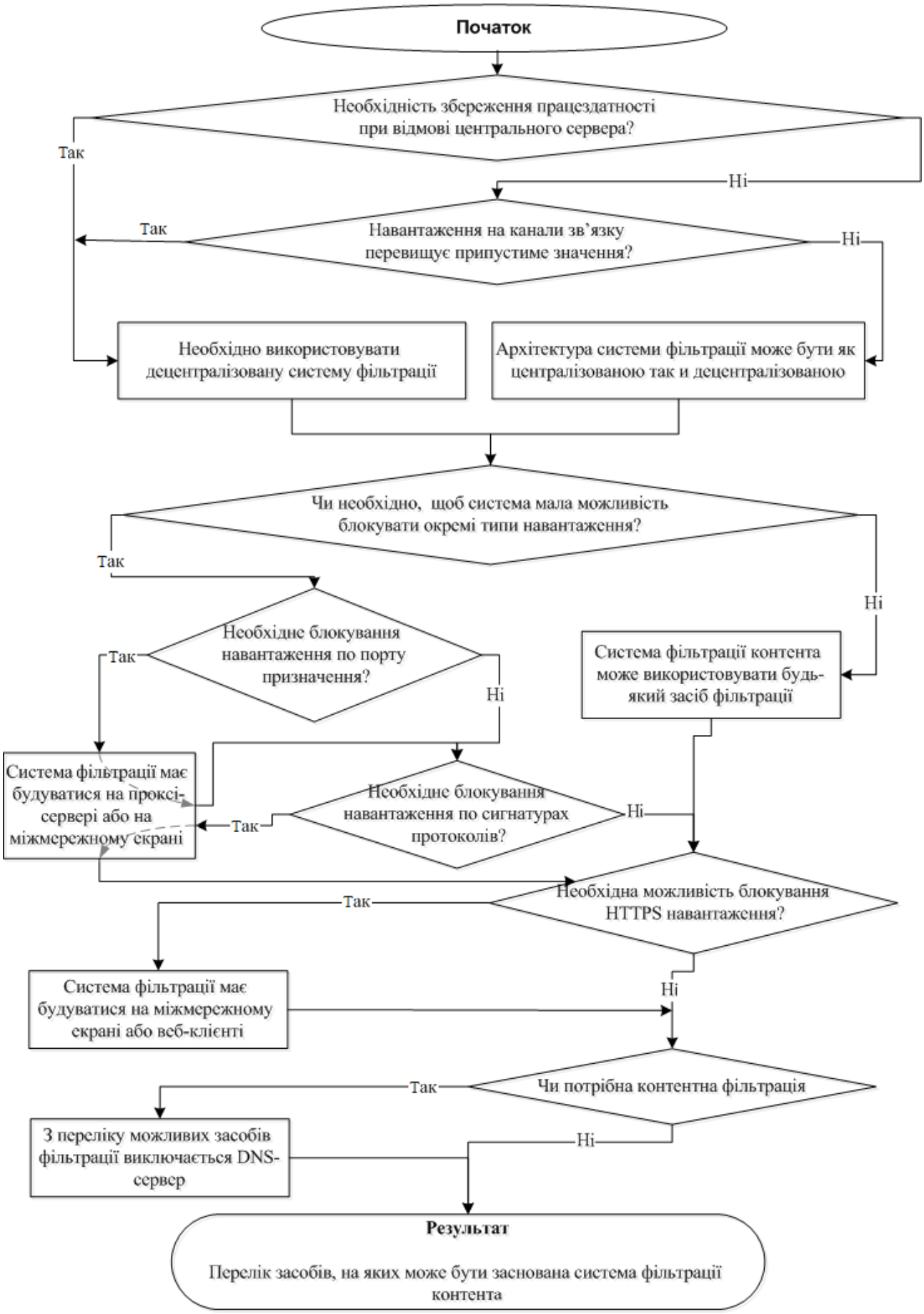

Рисунок 3 – Алгоритм вибору засобів фільтрації

Вартість експлуатації СФК протягом одного року може бути визначена за наступною формулою:

$$\overline{CF} = S_{\text{експл}} = N_{\text{корист}} \cdot C_{\text{кор.ліц}} + C_{\text{обсл.сист}} + C_{\text{підтр}}\ , \qquad (4)$$

де $N_{\text{корист}}$ – кількість користувачів СФК; $S_{\text{кор.ліц}}$ – вартість ліцензії на одного користувача, грн.; $S_{\text{обсл.сист}}$ – вартість обслуговування системи (наприклад, частка річного фонду оплати праці мережного адміністратора), грн.; $S_{\text{підтр}}$ – вартість технічної підтримки системи її розробником, грн.

Останнім кроком роботи узагальненого алгоритму (рис. 2) є виведення переліку СФК, що відповідають установленим вимогам та мають найбільше значення NPV (потребує найменшого обсягу витрат за зваженим показником за установлений термін).

Для спрощення користування розробленою методикою було розроблено спеціальне програмне забезпечення (ПЗ). Дане ПЗ має в собі програмну реалізацію запропонованої методики, базу даних з існуючими на ринку системами фільтрації контента, а також інструмент для простого наповнення бази даних. Для розробки ПЗ були використані мова програмування PHP та система управління базами даних MySQL.

Під час роботи з ПЗ користувачу пропонується заповнити анкету, на підставі якої будується модель корпоративної мережі і визначаються основні технічні вимоги до систем фільтрації контента. Приклад результатів розрахунку виведених за допомогою розробленого ПЗ наведено на рис. 4.

додавання систем перегляд систем редагування змінних анкета

Назва системи	Розробник	Web адреса	Вартість підготовки мережевої інфраструктури	Вартість встановлення та налаштування системи	Вартість річного обслуговування системи	Загальний фінансовий показник за перші 3 роки експлуатації системи
Всеукраїнська система обмеження доступу до нецільових ресурсів мережі Інтернет	ОНАЗ ім. О.С. Попова	http://copworldwide.org/ua/	400	200	100	**900**
NetPolice Child	NetPolice	http://netpolice.ru	0	0	2500	**7500**
NetPolice Pro	NetPolice	http://netpolice.ru	0	0	5000	**15000**

Одеська національна академія зв'язку імені О. С. Попова
podnebesny.igor@onat.edu.ua

Рисунок 4 – Результати розрахунків

На завершення можна зробити такі висновки:

1. Запропонована модель є універсальною для корпоративних мереж будь-якого рівня і дозволяє сформувати технічні вимоги до СФК без необхідності ознайомлення з принципами їх роботи. Це особливо актуально для невеликих організацій в штаті яких відсутній мережний адміністратор (наприклад, для загальноосвітніх навчальних закладів).
2. Запропонована методика дозволяє адміністрації установи або організації вибрати найбільш оптимальний з економічної і технічної точок зору спосіб підключення корпоративної мережі до системи фільтрації контента.
3. Розроблене ПЗ дозволяє значно зменшити трудовитрати користувача на вибір системи фільтрації контента, оскільки воно виконує порівняння технічних параметрів систем з побажаннями користувачів та розрахунок економічних параметрів впровадження та експлуатації систем фільтрації контента в автоматичному режимі.

Література

1. Каптур В.А. Узагальнена класифікаційна модель фільтрації контента в мережі Інтернет / В.А. Каптур // Зб. наук. праць Військового інституту телекомунікацій та інформатизації НТУУ "КПІ". – 2011. – №1. – С. 65 – 70.
2. 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.
3. Как сидеть ВКонтакте в школе на уроках информатики? [Електронний ресурс]. – Режим доступу: http://www.simpletutorials.ru/internet/kak-sidet-vkontakte-v-shkole-na-urokax-informatiki.php.
4. Интернет Цензор, [Електронний ресурс]. – Режим доступу: http://www.icensor.ru/soft/.
5. Виленский П.Л. Оценка эффективности инвестиционных проектов. Теория и практика / Виленский П.Л., Лившиц В.Н., Смоляк С.А. – М.: Дело, 2008. – 1104 с.