https://doi.org/10.31891/2219-9365-2023-74-28
УДК 621.396

ЗАХАРЖЕВСЬКИЙ Андрій
Національний університет оборони України імені Івана Черняховського
https://orcid.org/0000-0001-7019-9949
e-mail: a.zakharzhevskyi12@gmail.com

МОДЕЛЬ РОЗРАХУНКУ КАНАЛЬНОГО РЕСУРСУ АГРЕГОВАНОГО ПОТОКУ ДАНИХ ЗАХИЩЕНОГО КАНАЛУ ПЕРЕДАЧІ ІНФОРМАЦІЇ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В статі вирішується нове актуальне наукове задання щодо оцінки канального ресурсу агрегованого потоку даних для захищеного каналу передачі інформації інфокомунікаційної мережі спеціального призначення.

Розроблено та подано модель розрахунку канального ресурсу агрегованого потоку даних інфокомунікаційної мережі спеціального призначення. Подана модель дозволяє отримати кількісні значення канального ресурсу для різних способів обслуговування в залежності від навантаження агрегованим потоком захищеного каналу інфокомунікаційної мережі спеціального призначення. Відмінністю моделі є можливість до здійснення розрахунків з врахуванням критерію якості обслуговування каналу передачі даних в залежності від обраного способу обслуговування потоку даних захищеного каналу передачі інформації.

Показано, що зростання навантаження на захищений канал передачі даних ріст необхідного канального ресурсу. При цьому, необхідне значення канального ресурсу залежить від способу обслуговування агрегованого потоку даних в захищеному каналі інфокомунікаційної мережі спеціального призначення. Використання способу ізольованого обслуговування дає виграш в необхідному канальному ресурсі від 10 до 20 відсотків в порівнянні з груповим методом обслуговування для IP–телефонії.

Подані результати можуть бути застосовані при розробці нових та удосконалені існуючих телекомунікаційних систем, призначених для передачі конфіденційної інформації захищеними каналами.

Ключові слова:, інфокомунікаційна мережа, захищений канал передачі інформації, агрегований потік даних, канальний ресурс

ZAKHARZHEVSKYI Andrii
The National Defence University of Ukraine named after Ivan Cherniakhovskyi

MODEL FOR CALCULATING THE CHANNEL RESOURCE OF AN AGGREGATE DATA FLOW OF A SECURE INFORMATION TRANSMISSION CHANNEL OF A SPECIAL-PURPOSE INFOCOMMUNICATION NETWORK

In the article, a new topical scientific task is solved regarding the evaluation of the channel resource of the aggregated data flow for the protected information transmission channel of the special purpose information communication network.

A model for calculating the channel resource of the aggregated data flow of a special purpose information communication network has been developed and presented. The presented model makes it possible to obtain quantitative values of the channel resource for various methods of service depending on the load of the aggregated flow of the protected channel of the special purpose information communication network. The difference of the model is the ability to make calculations taking into account the quality criterion of data transmission channel service depending on the selected method of data flow maintenance of the protected information transmission channel.

It is shown that the growth of the load on the protected data transmission channel increases the necessary channel resource. At the same time, the required value of the channel resource depends on the method of servicing the aggregated data flow in the protected channel of the special purpose information communication network. The use of the isolated service method gives a gain in the required channel resource of 10 to 20 percent compared to the group service method for IP telephony.

The presented results can be applied in the development of new and improved existing telecommunication systems intended for the transmission of confidential information through secure channels.

Keywords: information communication network, secure information transmission channel, aggregate flow date, channel resource.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Забезпечення сталого та позитивного розвитку українського суспільства, його економічних та соціально – політичних відносин, досягнення високого рівня захисту територіальної цілісності та незалежності держави Україна вимагає постійного розвитку та удосконалення різних систем та мереж передачі інформації. Одним з типів телекомунікаційних мереж, безпосередньо пов'язаних як з захистом державних так і широкого кола корпоративних інтересів, направлених на захист та збереження інформації є інфокомунікаційні мережі спеціального призначення (ІКМСП) [1,2].

Основною особливістю їх побудови є можливість до передачі конфіденційної інформації захищеними від несанкціонованого доступу каналами передачі даних. При цьому такі мережі, як правило, мають закритий корпоративний характер побудови. Тобто обмежені у застосуванні. Особливо в комерційній

та виробничій сфері. Це обмежує сфери їх використання та можливості по ефективному функціонуванню та формує значний недолік у їх застосуванні [3].

Є очевидним, що усунення вказаного недоліку можна вирішити методом захисту конфеденційної інформації, що передається по каналам загального доступу телекомунікаційного мережі загального користування.

Захист інформації в каналах загального доступу здійснюється застосуванням різних технологій та процедур передачі даних. Однією з таких технологій є технологія віртуальної особистої мережі (Virtual Private Network, VPN), заснована на використанні відповідного VPN-шлюзу для захисту трафіку даних в відповідному каналі загального доступу телекомунікаційної мережі [3, 4].

Основою функціонування вузла доступу до транспортної телекомунікаційної мережі під час управління допуском потоків даних є оцінювання необхідного КР для агрегованого потоку даних, що передаються через захищений канал. При цьому КР, що виділяється для обслуговування агрегованого потоку, є найважливішим із ресурсів мережі [4,5].

Однією з особливостей функціонування телекомунікаційних мереж різного призначення є активне циркулювання по їх по каналам загального доступу агрегованих потоків даних. Завданням телекомунікаційної мережі, що передає агрегований потік даних є забезпечення необхідної якості обслуговування трафіку, яке оцінюється часом затримки пакетів даних.

В свою чергу, час затримки пакетів даних в каналі загалом залежить від КР, який виділяються для обслуговування даного трафіку [5,6].

Аналіз досліджень та публікацій

Вирішення наукового задання по підвищенню якості обслуговування агрегованих потоків даних через захищені канали передачі інформації передбачає розвиток та удосконалення методологічного апарату оцінювання необхідного канального ресурсу ІКМСП. Основною метою такої оцінки є розрахунок прогнозованого динамічного резерву канального ресурсу під вхідні агреговані потоки даних. Таке прогнозування потребує окремої процедури, заснованої на відповідній моделі, яка б дозволила однозначно розрахувати КР в відповідності до характеристик даного захищеного каналу передачі даних.

Аналіз публікацій, присвячених оцінці впливу функціонування VPN-шлюзу в каналі передачі інформації показав, що VPN-шлюз чинить вплив на наступні параметри. А саме: пікову (p) і середню (r) швидкість передачі пакетів даних, довжину генерованих пакетів (L) окремо для сервісів відеотелефонії та сервісів IP-телефонії [3,4].

Є очевидним, що процедура розрахунку необхідного канального ресурсу та його динамічного резервування саме для захищених каналів передачі інформації повинна враховувати значення вище поданих параметрів каналу передачі інформації та бути пов’язаною з часом затримки обробки пакетів агрегованого потоку даних у вказаному каналі. Вирішення такого наукового задання вимагає пошуку нових теоретичних та практичних підходів до розвитку нових способів розрахунку канального ресурсу захищених телекомунікаційних мереж та створення на їх основі відповідних моделей.

Формулювання цілей статті

Питання обслуговування агрегованих потоків даних в телекомунікаційних мережах та оцінці канального ресурсу для передачі даних захищеними каналами телекомунікаційних мереж висвітлено в роботах [2,3,7–9].

Основні питання теорії передачі трафіку через канали захищених телекомунікаційних мереж подано в роботах [2,3]. В вказаних роботах розглянуто загальні принципи побудови ефективних захищених телекомунікаційних мереж та реалізація захисту інформації в них за допомогою застосування спеціальних мережевих елементів. В свою чергу, безпосередній розрахунок канального ресурсу та питання визначення його потрібного значення для вхідного агрегованого потоку даних в даних роботах відсутні.

В роботі [7] викладено результати побудови віртуального варіанту окремої, захищеної шлюзом VPN телекомунікаційної мережі. В якості показника оцінки ефективності передачі даних в даній публікації подано затримку часу та пропускну спроможність передачі пакетів даних через захищений канал. При розрахунках визначених показників, кількісні значення необхідного канального ресурсу не розглядались.

Робота [8] розкриває сутність оцінки ефективності поданої в статті моделі розрахунку часу затримки, який подано в якості критерію аналізу трафіку в тунелі VPN. При здійснені вказаної оцінки пропонується проводити розподіл захищеного трафіку на різні категорії: перегляд інформації; потокове відео; електронне спілкування, тощо. Подана в даній роботі модель не передбачає проведення оцінки необхідно канального ресурсу агрегованого потоку даних, відповідно якого проводиться оцінка часу затримки. Розрахунки значень канального ресурсу в поданій моделі не взаємопов’язані з часом затримки потоку.

Аналіз публікацій, присвячених розгляду питання обробки агрегованих потоків даних в захищених каналах телекомунікаційних мережах, показав певні невідповідності, які значно впливають на ефективність функціонування ІКМСП та потребують проведення досліджень по їх усуненню.

Постановка задач дослідження

Одним з аспектів підвищення ефективності функціонування ІКМСП є вирішення завдання по динамічному резервуванню канального ресурсу. Вирішення вказаного задання передбачає проведення розрахунку канального ресурсу з врахуванням параметрів захищеного каналу та характристик агрегованого потоку даних.

Метою публікації є удосконалення технології обробки агрегованого потоку даних в захищених каналах ІКМСП методом динамічного резервування канального ресурсу.

Для досягнення мети були поставлені наступні завдання:

– розробка математичних залежностей та на їх основі формування моделі розрахунку канального ресурсу агрегованого потоку даних для захищених каналів ІКМСП;

– оцінку поданої моделі по можливостям розрахунку канального ресурсу та визначення його впливу на критерій якості обслуговування захищеного каналу передачі даних ІКМСП.

Виклад основного матеріалу

Модель розрахунку канального ресурсу агрегованого потоку даних для захищених каналів інфокомунікаційної мережі спеціального призначення.

Для розробки моделі розрахунку канального ресурсу агрегованого потоку даних застосовувалась теорія мережевого обчислення (NC – Network Calculus) [3,10]. Використання вказаної теорії мережевого обчислення дозволяє за відомими кількісними значеннями параметрів формувача трафіку, що притаманні системі управління потоками трафіку по захищеному каналу, розрахувати граничні значення параметрів критерію оцінки якості обслуговування потоку даних в мережі.

Відповідно до цієї теорії, вхідний потік даних, що поступає у формувач трафіку системи управління потоками трафіку захищеного каналу, обмежується детермінованою функцією вхідного потоку. Вихідний потік даних залежить від прийнятої моделі обслуговування, і обмежується функцією обслуговування [4,6]. Детермінований характер прийнятих припущень до розробки математичних залежностей є цілком прийнятним, якщо врахувати, що в реальних мережах трафік завжди обмежений пропускною здатністю каналу зв'язку. Це витікає з необхідності використання механізмів формування навантаження, що реалізуються в архітектурах IntServ і DiffServ [4,6,11].

Опис потоків даних із використанням даного математичного апарату дозволяє звести складні нелінійні системи до лінійних.

Для опису потоків даних, що надходять від джерел у формувач трафіку системи управління потоками захищеного каналу, використаємо кумулятивну функція $A(t)$, що визначає кількість байт даних, які надійшли в систему за інтервал часу $(0, t]$. При цьому приймається, що функція $A(0)=0$. Функція $A(t)$ – завжди зростаюча. Надалі така функцію у роботі приймемо як детерміновану функцію надходження.

Потік А є обмеженим функцією $f(t)$ тоді і лише тоді, коли для всіх $t_1<t_2$ виконується умова [10,11]:

$$A(t_2) - A(t_1) \le f(t_2 - t_1). \tag{1}$$

В якості основних параметрів потоку даних телекомунікаційної мережі приймемо наступні [3,4,10,11].

Максимальний розмірі пакету даних i-го потоку L_i (байт), відому пікові швидкость генерації пакетів p_i (байт/с), середню швидкості генерації пакетів r_i (байт/с) та виділений розмір буфера b_i (байт).

Тоді у системі керування потоками даних через VPN-шлюз мережі доступу ІКМСП з реалізованою функцією формування трафіку потік даних на виході подамо у вигляді виразу [4,12]:

$$A_i(t) = \begin{cases} L_i + p_i t \;;\; t \le \dfrac{b_i - L_i}{p_i - r_i} \\ b_i + r_i t \;;\; t \ge \dfrac{b_i - L_i}{p_i - r_i} \end{cases}, \tag{2}$$

де $A_i(t)$ – кількість навантаження i-го потоку, що надійшла в систему за період часу $(0, t]$ для найгіршого випадку, коли розмір пакетів дорівнює максимально можливому значенню L_i.

Прийнявши, що потік на виході системи управління потоками захищеного каналу при резервуванні частки канального ресурсу *k*-го каналу зв'язку з пропускною здатністю $R_{КС}$ для *i*-го потоку даних R_i (байт/с) визначається умово $\sum_i^n R_i \le R_{КС}$. Вказаний потік можна описати функцією обслуговування $W_i(t)$, яка визначає мінімальний обсяг даних, переданих у каналі зв'язку за час *t* [11,12]:

$$W_i(t) = R_i\left(t - t_{ЗАПi}\right), \tag{3}$$

де $t_{ЗАПi}$ визначається виразом:

$$t_{ЗАПi} = \frac{L_i}{R_i} + \frac{L_i}{R_{КС}}. \tag{4}$$

Функція обслуговування планувальника WFQ є функцією «швидкість-запізнення» з характеристиками швидкості R_i та запізнення $t_{ЗАПi}$ в секундах.

Приймемо те, що затримка передачі пакета в захищеному канал, викликана наявністю відповідного маршрутизатора захисту на лінії доступу до прикордонного маршрутизатора мережі не враховується. Опис потоків у системі управління потоками захищеного каналу проведемо відносно потоку від вхідного маршрутизатора каналу захисту до формувача трафіку прикордонного маршрутизатора транспортної мережі.

Приймем до уваги, що на вхід планувальника потоку вхідних даних, реалізованого по алгоритму WFQ, подається навантаження, пропущене через формувач трафіку «кошик маркерів», що дозволяє формально описати навантажувальні характеристики потоків зі змінною швидкістю [4, 5].

Вказаний алгоритм WFQ дозволяє застосовувати будь-які дії (скидання або перемаркування) тільки до пакетів, які не відповідають заявленому профілю. Конформні пакети проходять через «кошик з маркерами» без додаткової затримки, пов'язаної з обмеженою інтенсивністю вихідного навантаження [4, 5].

У системах управління допуском потоків даних у мережу важливою перевагою математичного апарату опису параметрів трафіку на виході мережевих пристроїв є мінімальний час обчислення необхідного КР [11, 13].

Забезпечення необхідного рівня критерію якості обслуговування кожного транспортного потоку даних, що надходить у прикордонний маршрутизатор, досягається за допомогою оцінювання часу верхньої затримки обробки пакетів, що проходять крізь нього. Прийнявши умову, що механізм обслуговування реалізований на базі планувальника класу WFQ, визначимо затримку для і-го потоку, яка повинна задовольняти значенню, що розраховується за виразом (5) [11, 13,14]:

$$t_{ПМ} \le \frac{t_{(вим)} - t_{КС} - 2t_{Ш}}{2}. \tag{5}$$

Відповідно до методології розрахунку часу затримки проходження пакетів через канали телекомунікаційної мережі та з врахуванням відомих функцій надходження та обслуговування трафіку визначимо вираз для розрахунку залежності значення часу затримки від керованих параметрів обслуговуючої трафік системи у вигляді [5,13].

$$t_{ПМ} = \begin{cases} \dfrac{(b_i - L_i)(b_i - R_i)}{R_i\left(p_i - r_i\right)} + \dfrac{2L_i}{R_i}; \\ \dfrac{2L_i}{R_i} + \dfrac{L_i}{R_{КС}}, \ R_i > p_i > r_i \end{cases} ; \ p_i > R_i > r_i. \tag{6}$$

В виразі (6) значення $t_{ПМ}$ приймається в якості верхнього граничного значення часу затримки. Це значення може бути забезпечено при резервуванні пропускної здатності R_i (в байтах/сек) в прикордонному маршрутизаторі для подальшого обслуговування вхідного потоку даних.

Значення $t_{ПМ}$, у свою чергу, залежить від значення виділеної для обслуговування потоку даних смуги пропускання R_i [5,13].

При формуванні моделі розрахунку канального ресурсу та проведенні її оцінки приймемо припущення про те, що буфер прикордонного маршрутизатора має нескінченну довжину. Тобто час затримки пакетів на вході прикордонного маршрутизатора не приймається до уваги.

При використанні мережі зв'язку часто виникає необхідність вирішення оберненої задачі. Її зміст – при заданій необхідної наскрізній затримці пакету *i*-го потоку даних «з кінця в кінець» ($t_{(вимог)}$), потрібно оцінити необхідний канальний ресурс, що запланований до обслуговування трафіку, який прогнозується на вході прикордонного маршрутизатора. Його значення розрахуємо виразом [5,13,14]:

$$R_i = \frac{p_i \frac{b_i - L_i}{p_i - r_i} + 2L_i}{t_{ПМ} + \frac{b_i - L_i}{p_i - r_i} - \frac{L_i}{R_{КС}}}. \quad (7)$$

Значення необхідної наскрізної затримки пакету *i*-го потоку даних $t_{ПМ}$, що подано в (7), визначається виразом (6).

Приймем умову, що значення необхідної наскрізній затримці пакету *i*-го потоку даних «з кінця в кінець» $t_{(вимог)}$ визначається рекомендацією «Міжнародного союзу електрозв'язку», яку подано в Бюлетені «Y.1541» [14, 15].

Для формального опису агрегованого потоку даних, що надходить з вихідного порту мережного елемента, приймемо представлену в «RFC 2216» концепцією характеризації трафіку агрегованих потоків [11,16]. Згідно вказаної концепції сума потоків даних (n), визначених як TSpec, описується сумарною функцією надходження (СФН) $A_{СФН}(t)$:

$$A_{СФН}(t) = \begin{cases} L_i + p_{СФН} t \; ; t < \dfrac{b_i - L_i}{p_{СФН} - r_{СФН}} \\ b_i + p_{СФН} t \; ; t \le \dfrac{b_i - L_i}{p_{СФН} - r_{СФН}} \end{cases}, \quad (8)$$

де L_i – максимальна довжина пакета *i*-го потоку з *n* потоків, що входять до складу агрегованого потоку даних захищеного каналу; $p_{СФН}$ – пікова швидкість генерації пакетів агрегованого потоку захищеного каналу; $r_{СФН}$ – середня швидкість генерації пакетів агрегованого потоку захищеного каналу; b_i (байт) – виділений розмір буфера формувача трафіку агрегованих потоківзахищених каналів, рівний розміру буфера, що виділяється для обслуговування *i*-го потоку з *n* потоків, які входять до складу агрегованого потоку даних каналу.

Вираз (8) дозволяє розрахувати найбільш складний випадок генерації трафіку *n* джерелами, на основі якого стає можливим обчислити необхідний канальний ресурс для *n* потоків з урахуванням забезпечення $t_{ПМ}$ відповідно всіх вимог, що забезпечують необхідну якість обслуговування по часу затримки. При цьому агрегований потік даних обслуговується в маршрутизаторах транспортної мережі при умові ізольованого з'єднання з дисципліною обслуговування FIFO *gj* в окремо зарезервованому буфері прикордонного маршрутизатора [15,18].

Розрахунок необхідного канального ресурсу для агрегованих потоків даних на основі теорії мережевих обчислень обумовлює методи ізольованого та групового обслуговування потоків даних.

Розрахунок канального ресурсу методом ізольованого обслуговування потоків при умові відсутності впливу маршрутизатора захищеного каналу даних подамо в вигляді [15,18]:

$$R_{ізол}(n) = \sum_{i=1}^{n} \frac{p_i \frac{(b_i - L_i)}{(p_i - r_i)} + 2L_i}{t_{ПМ} + \frac{(b_i - L_i)}{(p_i - r_i)} - \frac{L_i}{R_{КС}}}, \quad (9)$$

Розрахунок канального ресурсу методом групового обслуговування потоків даних на основі сумарної функції надходження (СФН) при умові відсутності впливу маршрутизатора захищеного каналу подамо в вигляді [15,18]:

$$R_{СФН}(n)=\frac{\sum_{i=1}^{n}\frac{\sum_{i=1}^{n}(b_i-L_i)}{\sum_{i=1}^{n}(p_i-r_i)}+2L_i}{t_{ПМ}+\frac{\sum_{i=1}^{n}(b_i-L_i)}{\sum_{i=1}^{n}(p_i-r_i)}-\frac{L_i}{R_{КС}}}, \quad (10)$$

В поданих виразах (9) і (10) прийнято [18,19,20]:

n – кількість потоків у складі агрегованого потоку даних;

i – порядковий номер потоку, що входить до складу агрегованого потоку даних;

L_i – максимальний розмір пакету даних i-го потоку, вибраний з усіх потоків n агрегованого потоку даних,

$t_{ПМ}$ – мінімально необхідна затримка до обробки пакета в ПМ серед n потоків даних,

$R_{КС}$ – пропускна здатність каналу зв'язку,

p_i – пікова швидкість генерації пакетів i-го потоку,

r_i – середня швидкість генерації пакетів i-го потоку,

b_i – виділений розмір буфера формувача трафіку для i-го потоку.

Таким чином, запропонована в роботі модель розрахунку канального ресурсу агрегованого потоку даних для захищених каналів інфокомунікаційної мережі спеціального призначення включає вирази окремих розрахунків канального ресурсу при ізольованому (9) та груповому (10) методі обробки пакетів даних. Розрахунковим параметрами даної моделі є директивно встановлений час затримки обробки пакетів та параметри захищеного каналу передачі даних інфокомунікаційної мережі спеціального призначення. Модель дозволяє визначити співзалежність розрахованого канального ресурсу від для прогнозованих значень потоків даних відповідно параметрів трафіку даного захищеного каналу.

Оцінка впливу канального ресурсу на час затримки обробки пакетів в захищеному каналі інфокомунікаційної мережі спеціального призначення

Для оцінки застосовності моделі розрахунку канального ресурсу агрегованого потоку даних захищених каналів ІКМСП проведено математичне моделювання по виразам (9) та (10) з урахуванням виразів (6), (7), (8).

При проведені розрахунків були використані значення характеристик потоків даних, які генеруються термінальним обладнанням, задіяним в стандартній структурі телекомунікаційної мережі з захищеним каналом передачі даних IP-телефонії [19, 20]. Пропускна здатність каналів $R_{КС}$ в розрахунках мала значення 100 Мбіт/сек.

Одержані в процесі моделювання кількісні значення канального ресурсу в залежності від кількості потоків IP-телефонії в загальному навантаженні на вході захищеного каналу для ізольованого обслуговування потоків даних – (9) і групового обслуговування потоків даних на основі СФН – (10), подано і на рис.1.

На рис.1 для порівняння подано значення резервованого канального ресурсу ($R_{еф}$) для n потоків сервісів реального часу, отримане на основі розрахунку ефективної швидкості передачі інформаційного потоку IP-телефонії [5, 21].

При його розрахунках коефіцієнт втрати пакетів для нульового (0) – класу якості обслуговування приймався в значені $P_{loss}=10^{-3}$ [19, 20].

Подані на рис.1 залежності дозволяють оцінити можливість розробленої моделі щодо розрахунків значення необхідного канального ресурсу в залежності від навантаження на захищений канал [22, 23] передачі даних ІКМСП.

Отримані розрахункові данні показують їх спів падіння з даними, одержаними на основі розрахунку ефективної швидкості передачі інформаційного потоку по запропонованим альтернативним моделям з різницею до 15 – 18 відсотків в залежності від навантаження на канал.

При цьому метод ізольованого обслуговування агрегованого потоку даних в порівнянні з груповим показав біль ефективні результати по виділеним обсягам канального ресурсу з ростом навантаження на канал.

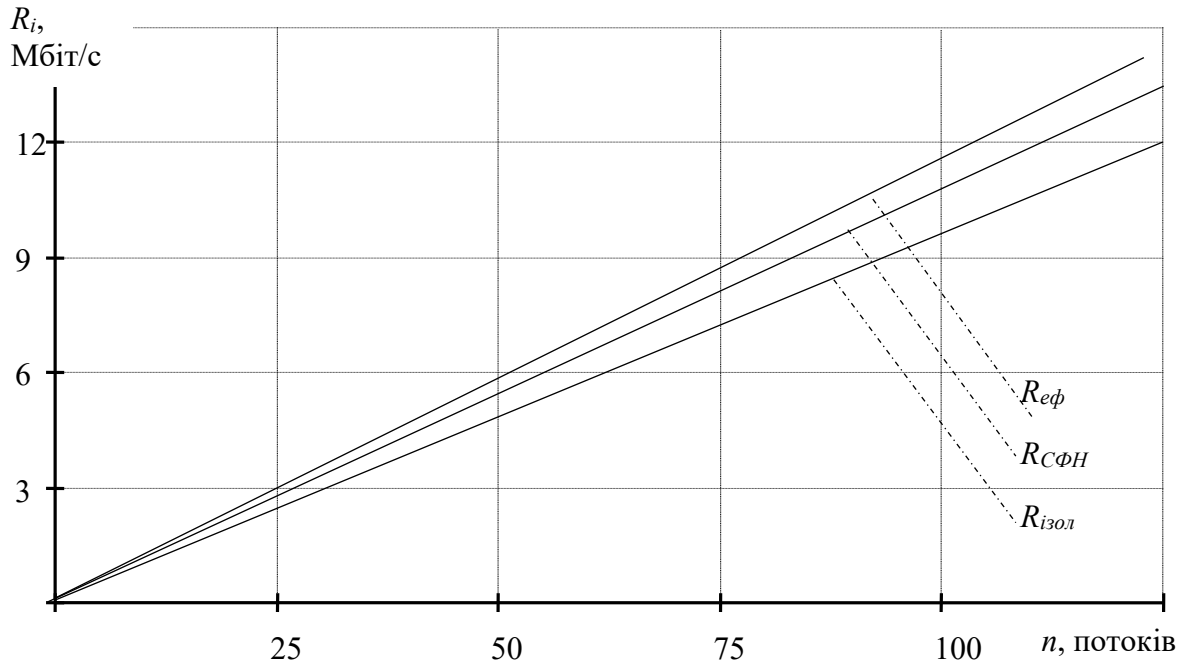

Рис. 1. Значення розрахованого канального ресурсу для обслуговування групового потоку передачі даних по каналу IP-телефонії

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

В статі вирішується нове актуальне наукове задання щодо оцінки канального ресурсу агрегованого потоку даних для захищеного каналу передачі інформації інфокомунікаційної мережі спеціального призначення.

1. Розроблено та подано модель розрахунку канального ресурсу агрегованого потоку даних інфокомунікаційної мережі спеціального призначення.

Подана модель дозволяє отримати кількісні значення канального ресурсу для різних способів обслуговування в залежності від навантаження агрегованим потоком захищеного каналу інфокомунікаційної мережі спеціального призначення. Відмінністю моделі є можливість до здійснення розрахунків з врахуванням критерію якості обслуговування каналу передачі даних в залежності від обраного способу обслуговування потоку даних захищеного каналу передачі інформації.

2. Показано, що зростання навантаження на захищений канал передачі даних ріст необхідного канального ресурсу. При цьому, необхідне значення канального ресурсу залежить від способу обслуговування агрегованого потоку даних в захищеному каналі інфокомунікаційної мережі спеціального призначення. Використання способу ізольованого обслуговування дає виграш в необхідному канальному ресурсі від 10 до 20 відсотків в порівнянні з груповим методом обслуговування для IP–телефонії.

Література

1. Попівський В.В., Лемешко О.В., Ковальчук В.К. Плотніков М.Д., Картушин Ю. П. (2012) Телекомунікаційні системи та мережі. Структура й основні функції. Том 1. URL: http://www.znanius.com/3534.html.

2. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації: НД ТЗІ 1.1-005-07. [Чинний від 2007.12.12]. К. : ДСТСЗІ СБУ, 2007. № 232. URL:https://tzi.com.ua/nd-tz-1.1-005-07.html

3. Галкін В.В., Пархоменко І.І. (2016) Використання VPN-технологій для захисту інформації в каналах корпоративних мереж. Проблема кібербезпеки інформаційно-телекомунікаційних систем: матеріали наук.- техніч. конф.,КНУ, Київ, Україна, 10 – 11 березня 2016. – К.: КНУ, 2016. – С. 66–76.

4. Бурячок В. Л., Аносов А. О., Семко В. В. (2012) Технології забезпечення безпеки мережевої інфраструктури. Підручник. Київ: «КУБГ», 218. URL:https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf

5. Поповський В.В., Олійник В.Ф. (2011) Математичні основи управління і адаптації в телекомунікаційних системах: підручник. Харьків: ТОВ “Компанія СМІТ”, 362.

URL:https://ice.nure.ua/ua/books-and-tutorials/pidruchnyk-matematychni-osnovy-upravlinnia-ta-adaptatsii-v-telekomunikatsijnykh-systemakh.

6. IPSec – протокол захисту мережевого трафіку на IP-рівні. [Електронний ресурс]. URL: https://www.ixbt.com/comm/ipsecure.shtml

7. Talib, H.A., Alothman, R.B. (2023) Mohammed, M.S. Malicious attacks modelling: a prevention approach for ad hoc network security Indonesian Journal of Electrical Engineering and Computer Science, 30 (3), 1856-1865. DOI: 10.11591/ijeecs.v30.i3.pp1856-1865. (Scopus, **Q2**).

8. Ammar Almomani (2022) Classification of Virtual Private networks encrypted traffic using ensemble learning algorithms,Egyptian Informatics Journal, 23(4), 57-68. https://doi.org/10.1016/j.eij.2022.06.006. (Scopus, **Q1**). https://www.sciencedirect.com/science/article/pii/S1110866522000482

9. Balachandran, A., Amritha, P.P. (2022) VPN Network Traffic Classification Using Entropy Estimation and Time-Related Features. Smart Innovation, Systems and Technologies, 251, 509-520. DOI: 10.1007/978-981-16-3945-6_50.

10. Geyer, F., Scheffler, A., & Bondorf, S. (2022). Network Calculus with Flow Prolongation–A Feedforward FIFO Analysis enabled by ML. *IEEE Transactions on Computers*, *72*(1), 97-110.

11. Кучук Н.Г., Гавриленко С.Ю., Лукова-Чуйко Н.В., Собчук В.В. (2019) Перерозподіл інформаційних потоків у гіперконвенгертній системі / С.Ю. Гавриленко. Сучасні інформаційні системи. Т.3, № 2. 116-121. DOI:https://doi.org/10.20998/2522-9052.2019.2.20

12. Kovalenko, A., Kuchuk, H.,Tkachov, V. (2021). Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання. Системи управління, навігації та зв'язку. Збірник наукових праць, 1(63), 90-95. https://doi.org/https://doi.org/10.26906/SUNZ.2021.1.090

13. Свиридов А. С., Коваленко А. А., Кучук Г. А. (2018) Метод перерозподілу пропускної здатності критичної ділянки мережі на основі удосконалення ON/OFF-моделі трафіку. Сучасні інформаційні системи. Т.2, № 2. 139–144. DOI: https://doi.org/10.20998/2522-9052.2018.2.24

14. ITU-T. Technical Report. XSTR-SEC-MANUAL Security in telecommunications and information technology (7th edition). 09/2022. International Telecommunication Union. 2022. P.244. URL:https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTSS-2020-4-PDF-E.pdf

15. ITU-T. Y.1541 (12/2011). Network performance objectives for IP-based services. URL:https://www.itu.int/rec/T-REC-Y.1541-201112-I/en

16. RFC 2216. URL: (https://datatracker.ietf.org/doc/html/rfc2216)

17. Гнатушенко В. В. (2014) Моделювання агрегованого трафіку передачі даних на основі моделі ON/OFF. Системні технології. Вип. 5. 65-72. URL:http://nbuv.gov.ua/UJRN/st_2014_5_10

18. Беркман Л., Захаржевський А., Лаврінець К. (2023). Удосконалення технології обробки агрегованого потоку даних захищеної корпоративної мультисервісної мережі зв'язку. Східно-Європейський журнал підприємницьких технологій , 4 (9 (124), 14–23. https://doi.org/10.15587/1729-4061.2023.285414

19. Лебеденко Т.М., Головешко М.В., Холодкова А.В. (2019) Дослідження методу активного управління чергами на інтерфейсах маршрутизаторів телекомунікаційних мереж. Системи управління, навігації та зв'язку. 4(56), 57-62. DOI:10.26906/SUNZ.2019.4.057.

20. Лебеденко Т.М., Головешко М.В., Северілов А.В. (2019) Результати експериментального дослідження методу активного управління чергами на інтерфейсах телекомунікаційних мереж. Електронне наукове фахове видання – журнал «Проблеми телекомунікацій». 2(25), 37-55. https://doi.org/10.30837/pt.2019.2.03.

21. Бойко Ю. SAML : дефініція та принцип роботи через VPN тунель у захищених інформаційних мережах /Ю. Бойко, Б. Білявець //Вимірювальна та обчислювальна техніка в технологічних процесах. – 2022. – № 4. – С. 41-48. https://doi.org/10.31891/2219-9365-2022-72-4-4.

22. Пятін І. С. Порівняння продуктивності завадостійких кодів на основі програмного HDL моделювання для захищених інформаційних технологій /І. С. Пятін, Ю. М. Бойко //Інфокомунікаційні та комп'ютерні технології. – 2022. – № 1(03). – С. 39-62.

23. Бойко Ю. Transmission of control information in 5G broadband telecommunication systems /Ю. Бойко, І. П'ятін, Л. Карпова, І. Пархомей //Адаптивні системи автоматичного управління. – 2021. – Т. 1. – №. 38. – С. 82-95.

References

1. Popivskyi V.V., Lemeshko O.V., Kovalchuk V.K. Plotnikov M.D., Kartushyn Yu.P. (2012) Telecommunication systems and networks. Structure and main functions. Volume 1. URL: http://www.znanius.com/3534.html.

2. Protection of information at the objects of information activity. Creation of a complex of technical protection of information: ND TZI 1.1-005-07. [Effective from 12.12.2007]. K.: DSTSZI SBU, 2007. No. 232. URL: https://tzi.com.ua/nd-tz-1.1-005-07.html

3. Galkin V.V., Parkhomenko I.I. (2016) Using VPN technologies to protect information in corporate network channels. The problem of cyber security of information and telecommunication systems: scientific and technical materials. conference, KNU, Kyiv, Ukraine, March 10-11, 2016. - K.: KNU, 2016. - P. 66-76.

4. Buryachok V. L., Anosov A. O., Semko V. V. (2012) Technologies for ensuring network infrastructure security. Textbook. Kyiv: "KUBG", 218. URL: https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf

5. Popovsky V.V., Oliynyk V.F. (2011) Mathematical foundations of control and adaptation in telecommunication systems: a textbook. Kharkiv: SMIT Company LLC, 362. URL: https://ice.nure.ua/ua/books-and-tutorials/pidruchnyk-matematychni-osnovy-upravlinnia-ta-adaptatsii-v-telekomunikatsijnykh-systemakh.

6. IPSec is a network traffic protection protocol at the IP level. [Electronic resource]. URL: https://www.ixbt.com/comm/ipsecure.shtml

7. Talib, H.A., Alothman, R.B. (2023) Mohammed, M.S. Malicious attacks modeling: a prevention approach for ad hoc network security Indonesian Journal of Electrical Engineering and Computer Science, 30 (3), 1856-1865. DOI: 10.11591/ijeecs.v30.i3.pp1856-1865. (Scopus, Q2).

8. Ammar Almomani (2022) Classification of Virtual Private networks encrypted traffic using ensemble learning algorithms, Egyptian Informatics Journal, 23(4), 57-68. https://doi.org/10.1016/j.eij.2022.06.006. (Scopus, Q1). https://www.sciencedirect.com/science/article/pii/S1110866522000482

9. Balachandran, A., Amritha, P.P. (2022) VPN Network Traffic Classification Using Entropy Estimation and Time-Related Features. Smart Innovation, Systems and Technologies, 251, 509-520. DOI: 10.1007/978-981-16-3945-6_50.

10. Geyer, F., Scheffler, A., & Bondorf, S. (2022). Network Calculus with Flow Prolongation–A Feedforward FIFO Analysis enabled by ML. IEEE Transactions on Computers, 72(1), 97-110.

11. Kuchuk N.G., Havrylenko S.Yu., Lukova-Chuiko N.V., Sobchuk V.V. (2019) Redistribution of information flows in a hyperconvergent system / S.Yu. Gavrilenko. Modern information systems. Vol. 3, No. 2. 116-121. DOI:https://doi.org/10.20998/2522-9052.2019.2.20

12. Kovalenko, A., Kuchuk, H., Tkachov, V. (2021). A method for ensuring the survivability of a computer network based on VPN tunneling. Control, navigation and communication systems. Collection of scientific papers, 1(63), 90-95. https://doi.org/https://doi.org/10.26906/SUNZ.2021.1.090

13. Sviridov A. C., Kovalenko A. A., Kuchuk G. A. (2018) A method of redistributing the bandwidth of a critical section of the network based on the improvement of the ON/OFF traffic model. Modern information systems. Vol. 2, No. 2. 139–144. DOI: https://doi.org/10.20998/2522-9052.2018.2.24

14. ITU-T. Technical Report. XSTR-SEC-MANUAL Security in telecommunications and information technology (7th edition). 09/2022. International Telecommunication Union. 2022. P.244. URL:https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTSS-2020-4-PDF-E.pdf

15. ITU-T. Y.1541 (12/2011). Network performance objectives for IP-based services. URL:https://www.itu.int/rec/T-REC-Y.1541-201112-I/en

16. RFC 2216. URL: (https://datatracker.ietf.org/doc/html/rfc2216)

17. V. V. Hnatushenko (2014) Modeling of aggregated data transmission traffic based on the ON/OFF model. System technologies. Vol. 5. 65-72. URL: http://nbuv.gov.ua/UJRN/st_2014_5_10

18. Berkman L., Zakharzhevsky A., Lavrynets K. (2023). Improvement of the processing technology of the aggregated flow of data of the protected corporate multi-service communication network. East European Journal of Entrepreneurial Technology, 4 (9 (124), 14–23. https://doi.org/10.15587/1729-4061.2023.285414

19. Lebedenko T.M., Goloveshko M.V., Kholodkova A.V. (2019) Research on the method of active queue management on router interfaces of telecommunication networks. Control, navigation and communication systems. 4(56), 57-62. DOI:10.26906/SUNZ.2019.4.057.

20. Lebedenko T.M., Goloveshko M.V., Severilov A.V. (2019) Results of an experimental study of the method of active queue management on the interfaces of telecommunication networks. Electronic scientific publication - the journal "Telecommunications Problems". 2(25), 37-55. https://doi.org/10.30837/pt.2019.2.03.

21. Boiko J, Biliavets B. (2022). SAML: definition and principles of operation through a vpn tunnel in secure information networks. Measuring and computing devices in technological processes, (4), 41–48. https://doi.org/10.31891/2219-9365-2022-72-4-4.

22. Pyatin I. Comparison the performance of error-control code based on software HDL modeling for information security technologies / I. Pyatin, J. Boiko //Infocommunication and computer technologies. – 2022. – Vol. 1, No. 3. – S. 39-62.

23. Boiko J. Transmission of control information in 5G broadband telecommunication systems /J. Boiko, I. Pyatin, L Karpova, I Parkhomey //Adaptive systems of automatic control. – 2021. – Vol. 1. – No. 38. – S. 82-95.