https://doi.org/10.31891/2219-9365-2023-75-20
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

ОЦІНКА КАНАЛЬНОГО РЕСУРСУ 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.

Подано дані оцінки канального ресурсу агрегованого потоку даних для захищеного каналу передачі інформації інфокомунікаційної мережі спеціального призначення. Показано, що зростання навантаження на захищений канал передачі даних викликає ріст необхідного канального ресурсу. При цьому, необхідне значення канального ресурсу залежить від способу обслуговування агрегованого потоку даних в захищеному каналі інфокомунікаційної мережі спеціального призначення та виду трафіку. Використання способу ізольованого обслуговування дає виграш в необхідному канальному ресурсі від 10 до 20 відсотків в порівнянні з груповим методом обслуговування для IP–телефонії та до 25 відсотків для Відео-телефонії.

Встановлено, що при збільшені навантаження агрегованого потоку даних на захищений канал не забезпечується необхідна затримка обробки пакетів даних в встановлених нормативних значеннях. При обслуговувані агрегованих потоків даних в захищеному каналі має значення вид трафіку даних. Для агрегованого потоку даних шифрованої Відео–телефонії заданий рівень необхідної затримка обробки пакетів даних забезпечується за рахунок перевищення зарезервованого ресурсу пікового значення швидкості передачі.

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

ASSESSMENT OF THE CHANNEL RESOURCE OF A SECURED 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.

Data on the evaluation of the channel resource of the aggregated data flow for the protected information transmission channel of the special purpose information communication network are provided. It is shown that an increase in the load on a protected data transmission channel causes an increase in the required 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 and the type of traffic. The use of the isolated service method gives a gain in the necessary channel resource from 10 to 20 percent compared to the group service method for IP telephony and up to 25 percent for Video telephony.

It was established that with an increased load of the aggregated data flow on the protected channel, the necessary delay in the processing of data packets is not provided within the established regulatory values. When aggregated data flows are served in a protected channel, the type of data traffic is important. For the aggregated data flow of encrypted Video-telephony, the specified level of the necessary delay in the processing of data packets is ensured by exceeding the reserved resource of the peak value of the transmission speed.

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, aggregated data flow, channel resource

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

Ефективне використання інфокомунікаційних мереж різного призначення в системі взаємопов’язаних телекомуникаційних ліній зв’язку держави потребує постійного пошуку нових методів та способів, направлених на вирішення завдань удосконалення процесу обробки та передачі в них даних.

Одним з таких завдань є удосконалення процесу обробки агрегованих потоків даних в захищених каналах передачі інформації в інфокомунікаційних мережах спеціального призначення [1,2].

Інфокомунікаційні мережі спеціального призначення (ІКМСП) призначені для забезпечення захисту від несанкціонованого доступу та збереження на етапі передачі важливої конфіденційної інформації в сферах державної та корпоративної діяльності.

Виходячи з існуючих недоліків корпоративних захищених телекомунікаційних мереж та прийнявши до уваги широко розгалужену мережу телекомунікаційних ліній зв'язку загального користування державного та регіонального значення. Розробники перспективних інфокомунікаційних мереж спеціального призначення одним з напрямків їх побудови обрали використання каналів відкритого доступу телекомунікаційних ліній зв'язку загального користування, що функціонують на основі різних технологій захисту інформації.

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].

Відомо, що основою функціонування вузла доступу до транспортної телекомунікаційної мережі під час управління допуском потоків даних є оцінювання необхідного канального ресурсу (КР) для агрегованого потоку даних, що передаються через ораний канал передачі інформації. При цьому КР, що виділяється для обслуговування агрегованого потоку, є одним із основних ресурсів телекомунікаційної мережі [4,5].

Виділення в процесі побудови ІКМСП в системі каналів загальної телекомунікаційної мережі низки спеціальних каналів, забезпечення їх технологіями захисту інформації вимагає вирішення ряду наукових завдань, пов'язаних з оцінкою ефективності передачі пакетів даних, об'єднаних в агреговані потоки. 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 передачі інформації загалом залежить від КР, який виділяється для обслуговування даного трафіку [5,6].

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

Є очевидним, що значення виділеного канального ресурсу в захищеному каналі може чинити значний вплив на час обробки пакетів даних. А взаємозв'язок параметрів передачі пакетів даних та типу даних, що передаються може значно вплинути як необхідний канальний ресурс для їх обробки так і на час затримки пакетів даних [3,4].

Формування завдання дослідження

Вирішення наукового задання по підвищенню якості обслуговування агрегованих потоків даних в захищених каналах передачі інформації передбачає проведення досліджень щодо оцінки канального ресурсу захищеного каналу передачі інформації ІКМСП та його залежності від параметрів каналу та виду переданих пакетів даних.

Основною метою такої оцінки є встановлення залежності та розрахунок можливого канального ресурсу даного захищеного каналу інформації ІКМСП відносно вхідних агрегованих потоків даних різного типу.

Аналіз останніх досліджень і публікацій

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].

Розгляд параметрів трафіку даних, що подаються в захищені мережі каналів передачі агрегованого потоку даних подано в роботі [7]. В даній роботі запропонована певна класифікація трафіку і визначені відповідно цій класифікації значення його параметрів. Зв'язок вказаних параметрів та значення необхідного канального ресурсу і часу затримки потоку і каналах його передачі в даній роботі відсутні.

Результати оцінки параметрів передачі даних в захищеному каналі передачі агрегованого потоку подано в роботі [8]. Набір поданих в роботі даних містить узагальнену модель мережевого трафіку, що складається з різних типів мережевого трафіку, як-от Інтернет, електронна пошта, відеоконференції, потокове відео та служби терміналів. Для однієї моделі мережевого трафіку дані вимірюються для різних сценаріїв, тобто для передачі даних через різні типи захищеного каналу і без нього. На фоні наявності в даній роботі великих масивів даних що характеризують захищений канал передачі в ній відсутні результати аналізу та оцінка впливу параметрів каналу на канальний ресурс та напрямки його динамічного резервування.

Одним з шляхів підвищення ефективності захищених каналів телекомунікаційних мереж що до передачі даних є класифікація мережевого трафіку, яке є важливим і проблематичним аспектом управління мережевими ресурсами, що зазначено в роботі [9]. В вказаній роботі розглянуто декілька алгоритмів

класифікації, виявлення та управління агрегованим потоком даних при передачі їх захищеним каналом. Але поданий в роботі процес безпосереднього виявлення трафіку не враховує канальні ресурси системи, які необхідні для його безпосередньо прийому та подальшого управління. Відповідно і оцінка вказаного канального ресурсу в роботі не проводилась.

Аналіз публікацій, присвячених розгляду питання оцінки канального ресурсу 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

Вирішення наукового задання по підвищенню якості обслуговування агрегованих потоків даних в захищених каналах передачі інформації передбачає оцінки канального ресурсу захищеного каналу передачі інформації ІКМСП.

Метою публікації є встановлення залежності канального ресурсу захищеного каналу передачі інформації від параметрів агрегованого потоку даних та виду трафіку пакетів даних.

Для досягнення мети були поставлені наступні завдання:

– провести оцінку канального ресурсу та визначення його впливу на критерій якості обслуговування захищеного каналу передачі даних ІКМСП;

– провести аналіз отриманих даних та встановити залежності параметрів каналу передачі інформації та виду трафіку пакетів даних щодо прогнозованого динамічного резервування канального ресурсу

Виклад основного матеріалу

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

Розрахунки значення канального ресурсу агрегованого потоку даних для захищених каналів інфокомунікаційної мережі спеціального призначення проведем по наступному порядку.

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].

Для проведення розрахунків використаєм наступні параметри потоку: максимальний розмірі пакету даних i-го потоку L_i (байт); відому пікову швидкість генерації пакетів p_i (байт/с); середню швидкості генерації пакетів r_i (байт/с); виділений розмір буфера b_i (байт).

Потік даних на виході визначається по 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.

Потік на виході системи управління трафіком захищеного каналу мережі опишемо 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 $t_{ЗАПi}$ – час обробки пакетів, який визначається виразом:

$$t_{ЗАПi} = \frac{L_i}{R_i} + \frac{L_i}{R_{КС}}. \quad (4)$$

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

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]:

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

Вираз для розрахунку залежності значення часу затримки від керованих параметрів обслуговуючої трафік системи у вигляді [5,11].

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

В виразі (6) значення часу затримки - $t_{ПМ}$ 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].

Час затримки пакетів на вході прикордонного маршрутизатора при проведені розрахунку не приймемо 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.

Оцінимо необхідний канальний ресурс, що запланований до обслуговування трафіку, який прогнозується на вході прикордонного маршрутизатора при заданій необхідної наскрізній затримці пакету *i*-го потоку даних при проходженні каналу ($t_{(вимог)}$) за виразом [5,11]:

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» [14-16].

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

Сума потоків даних (n), визначених як *TSpec*, опишемо сумарною функцією надходження (СФН) $A_{СФН}(t)$:

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

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 потоків захищених 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.

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 розрахуємо по виразу [17, 18]:

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

Розрахунок канального ресурсу методом групового обслуговування потоків даних на основі сумарної функції надходження (СФН) при умові відсутності впливу маршрутизатора захищеного каналу розрахуємо по виразу [17]:

В поданих виразах (9) і (10) прийнято [17,18]:

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.

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

Оцінка канального ресурсу захищеного каналу інфокомунікаційної мережі спеціального призначення

Для оцінки канального ресурсу захищеного каналу 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 та Відео-телефонії. Їх значення подано в табл.1 [18,19]. Пропускна здатність каналів $R_{КС}$ в розрахунках мала значення 100 Мбіт/сек.

Таблиця 1

Кількісні значення параметрів агрегованого потоку даних

Потоки даних від терміналу	Значення параметрів трафіку					
	Відео-телефонія			IP-телефонія		
	p, Мбіт/с	*r*, Мбіт/с	*L*, Байт	*p*, Мбіт/с	*r*, Мбіт/с	*L*, Байт
	2,1	0,87	1346	0,112	0,096	214

Отримані значення необхідного КР в залежності від навантаження, що надходить при описі поведінки агрегованого потоку з використанням існуючої моделі ізольованого обслуговування потоків даних – (9) і моделі групового обслуговування потоків даних на основі СФН – (10), представлені на рис.1 та рис.2.

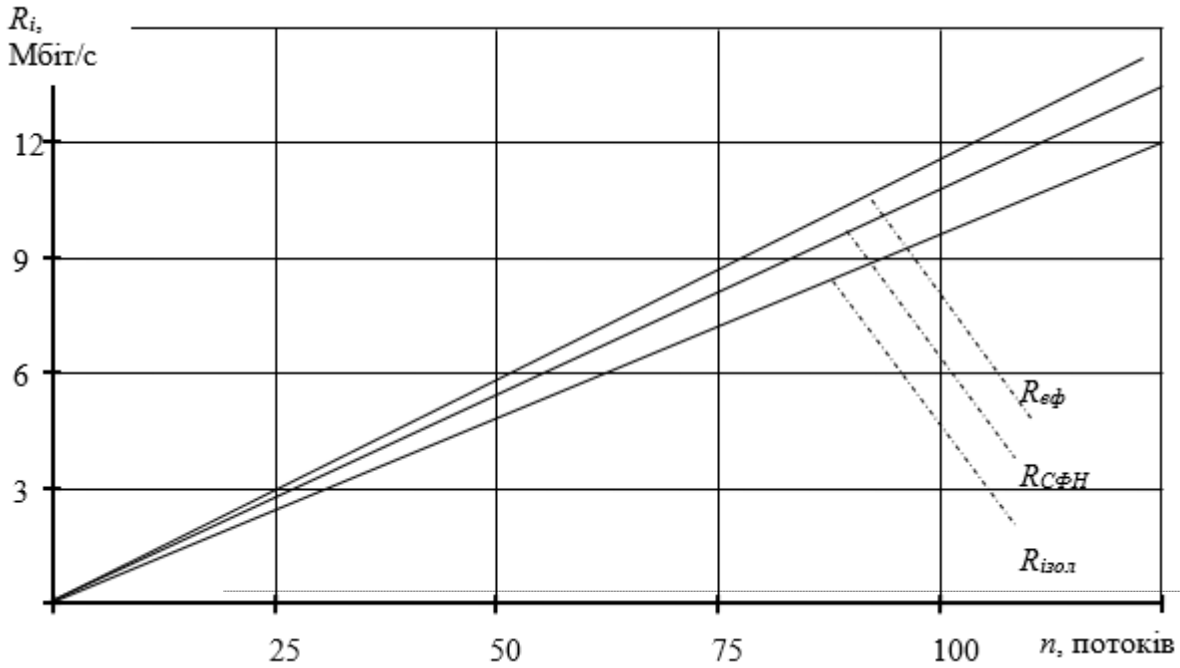

Рис. 1. Значення канального ресурсу для обслуговування групованого потоку передачі даних по каналу IP-телефонії

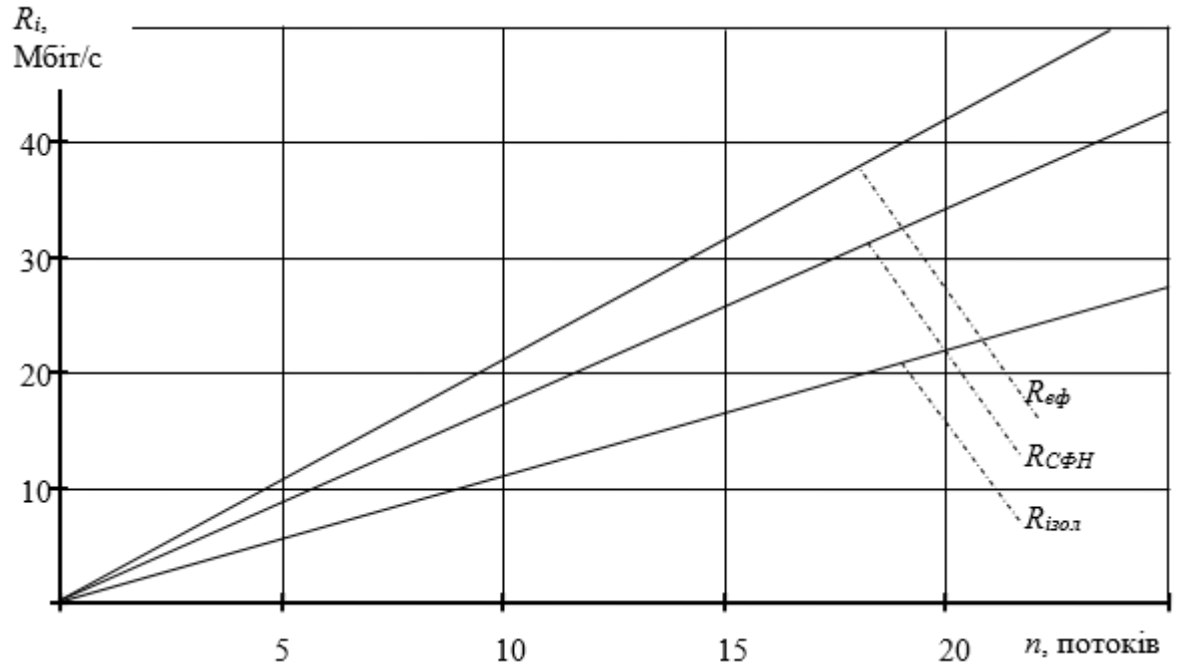

Рис. 2. Значення канального ресурсу для обслуговування групованого потоку передачі даних по каналу Відео–телефонії

На рис.1 та рис.2. 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 $P_{loss}=10^{-3}$ [18,19].

Розрахунки максимального значення часу затримки для потоку передачі даних по каналам IP-телефонії та Відео–телефонії, а також залежності, що апроксимують їх середні значення, представлені на рис.3, 4 відповідно.

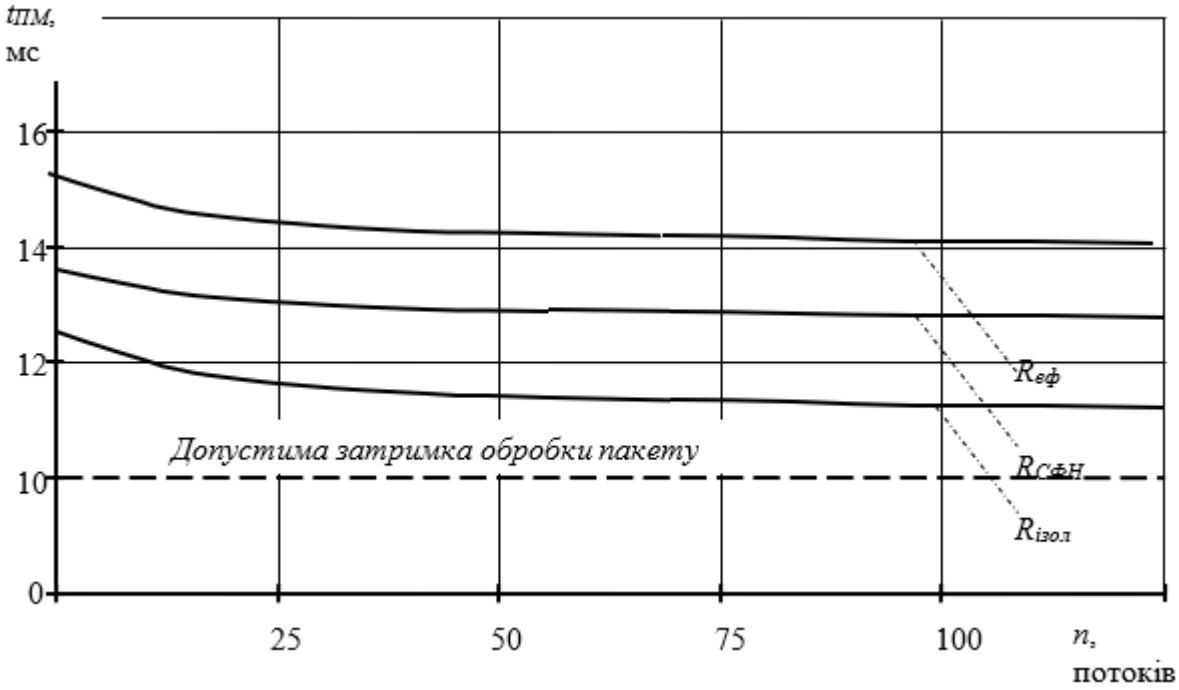

Рис.3. Максимально-досяжна затримка часу обробки пакету даних у прикордонному маршрутизаторі для обслуговування групового потоку по каналу IP-телефонії

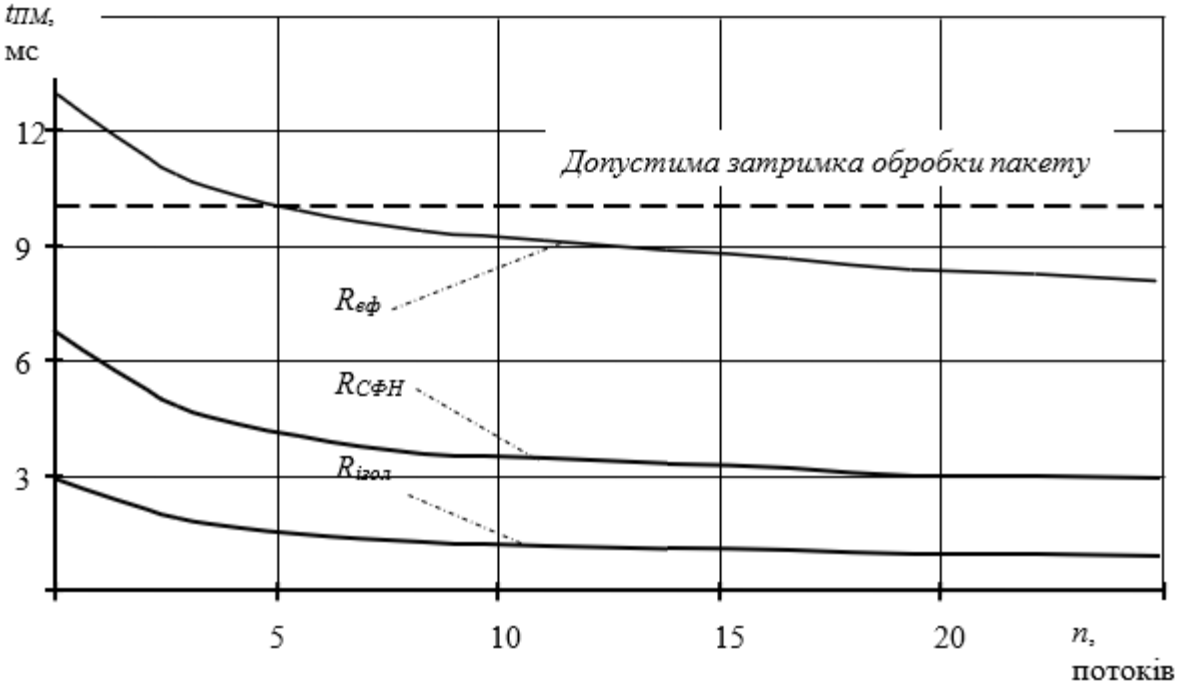

Рис. 4. Максимально-досяжна затримка часу обробки пакету даних у прикордонному маршрутизаторі для обслуговування групованого потоку по каналу Відео–телефонії

При оцінці результатів розрахунку прийнято, що чисельне значення часу необхідної затримки обробки пакета ПМ, виходячи з фізичної та логічної топології даної ЗКМСС відповідно до рекомендації Y.1541 не повинно перевищувати 10 мс [15,18].

Аналіз залежностей рис.1, 2 показує, що нижче значення КР захищеного каналу ІКМСП в порівняні з груповим методом забезпечує метод ізольованої обслуговування потоку даних. В середньому виграш

становить від 10 до 20 відсотків для IP – телефонії та Відео–телефонії. Це пояснюється більш гнучким процесом керування буфером зберігання вхідних даних прикордонного маршрутизатора при ізольованому способі обслуговування. При гнучкому процесі керування буфером ізольоване обслуговування не приводить до значних втрат вхідних пакетів через перевантаження буфера прикордонного маршрутизатора ІКМСП.

При обслуговуванні агрегованих потоків шифрованої Відео–телефонії заданий рівень необхідної затримка обробки пакетів даних забезпечується за рахунок перевищення зарезервованого ресурсу пікового значення швидкості передачі.

Результати розрахунків значення КР, як функції від кількості складових агрегованого потоку даних різних типів, свідчить про невідповідність швидкості надходження пакетів даних та швидкості їх обслуговування. У першому випадку виділений КР менший від пікової швидкості передачі, у другому навпаки перевищує її.

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 [18, 19].

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 [21-23] 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.

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. Подано дані оцінки канального ресурсу агрегованого потоку даних для захищеного каналу передачі інформації інфокомунікаційної мережі спеціального призначення враховують взаємозалежності параметрів потоку даних та виду трафіку, який передаються захищеним каналом передачі даних

2. Показано, що зростання навантаження на захищений канал передачі даних викликає ріст необхідного канального ресурсу. При цьому, необхідне значення канального ресурсу залежить від способу обслуговування агрегованого потоку даних в захищеному каналі інфокомунікаційної мережі спеціального призначення та виду трафіку.

Використання способу ізольованого обслуговування дає виграш в необхідному канальному ресурсі від 10 до 20 відсотків в порівнянні з груповим методом обслуговування для IP–телефонії та до 25 відсотків для Відео-телефонії.

3. Встановлено, що при збільшені навантаження агрегованого потоку даних на захищений канал не забезпечується необхідна затримка обробки пакетів даних в встановлених нормативних значеннях.

При обслуговувані агрегованих потоків даних в захищеному каналі має значення вид трафіку даних. Для агрегованого потоку даних шифрованої Відео–телефонії заданий рівень необхідної затримка обробки пакетів даних забезпечується за рахунок перевищення зарезервованого ресурсу пікового значення швидкості передачі.

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. Xiuli Ma, Wenbin Zhu, Jieling Wei, Yanliang Jin, Dongsheng Gu, Rui Wang (2023) EETC: An extended encrypted traffic classification algorithm based on variant resnet network, Computers & Security, Volume 128, 103175, https://doi.org/10.1016/j.cose.2023.103175. (Scopus, Q1).

8. Mohamed Naas, Jan Fesl (2023) A novel dataset for encrypted virtual private network traffic analysis, Data in Brief, Volume 47, 108945. https://doi.org/10.1016/j.dib.2023.108945. (Scopus).

https://www.sciencedirect.com/science/article/pii/S235234092300063X

9. A. A. Afuwape, Y. Xu, J. H. Anajemba, G. Srivastava (2021) Performance evaluation of secured network traffic classification using a machine learning approach. Computer Standards & Interfaces, 78, 103545. https://doi.org/10.1016/j.csi.2021.103545.

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. 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.

18. Захаржевський, А. (2023). Модель розрахунку канального ресурсу агрегованого потоку даних захищеного каналу передачі інформації інфокомунікаційної мережі спеціального призначення. Measuring and computing devices in technological processes, (2), 202–210. https://doi.org/10.31891/2219-9365-2023-74-28

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. https://doi.org/10.36994/2788-5518-2022-01-03-03.

23. Бойко Ю. М., Макаришкін Д. А., Пасічник О. І. Дослідження ефективності алгоритмів канального кодування в захищених телекомунікаційних системах передавання інформації //Зв'язок. – 2016. – №. 5. – С. 56-67.

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. Xiuli Ma, Wenbin Zhu, Jieling Wei, Yanliang Jin, Dongsheng Gu, Rui Wang (2023) EETC: An extended encrypted traffic classification algorithm based on variant resnet network, Computers & Security, Volume 128, 103175, https://doi .org/10.1016/j.cose.2023.103175. (Scopus, Q1).

8. Mohamed Naas, Jan Fesl (2023) A novel dataset for encrypted virtual private network traffic analysis, Data in Brief, Volume 47, 108945. https://doi.org/10.1016/j.dib.2023.108945. (Scopus).

https://www.sciencedirect.com/science/article/pii/S235234092300063X

9. A. A. Afuwape, Y. Xu, J. H. Anajemba, G. Srivastava (2021) Performance evaluation of secured network traffic classification using a machine learning approach. Computer Standards & Interfaces, 78, 103545. https://doi.org/10.1016/j.csi.2021.103545.

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. 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

18. Zakharzhevsky, A. (2023). Model for the development of a channel resource of an aggregated data flow of a protected channel for the transmission of information and information communication measures for special purposes. Measuring and computing devices in technological processes, (2), 202–210. https://doi.org/10.31891/2219-9365-2023-74-28.

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. https://doi.org/10.36994/2788-5518-2022-01-03-03.

23. Boiko J., Makaryshkin D., Pasichnyk O. Research into effectiveness of channel coding algorithms in protected telecommunication information transmission systems //Connectivity– 2016. – №. 5. – S. 56-67.