This paper considers the process of dynamic reservation of the channel resource of a secure corporate multi-service communication network.

It has been established that the processes of building and functioning of the schemes of a secure corporate multi-service communication network and improving the quality of the implementation of its main work processes involve the evaluation and dynamic reservation of channel resources for incoming aggregated data flows of the network.

The model of dynamic reservation of the channel resource of the aggregated data stream of the secure corporate multi-service communication network was built and proposed. The proposed model makes it possible to set the quantitative values of the reserved channel resource for different service methods depending on the number of component flows in the total aggregated data flow of the VPN tunnel.

It was established that an increase in the density of the aggregated data stream requires an increase in the reserved channel resource. At the same time, its value is influenced by the way of servicing the aggregated data flow in the VPN tunnel of the secure corporate multi-service communication network. Application of the isolated service method gives a gain in the allocated resource for the channel reserve from 10 to 20 percent compared to the group service method for IR and video telephony. This is due to the more flexible management process of the border router's incoming data storage buffer under the isolated service mode.

The model of dynamic reservation of the channel resource of the secure corporate multi-service communication network reported in this paper could be used in the improvement of existing and development of new structures of the secure corporate multi-service communication network. The consequence of such an improvement is a reduction in the delay time for the processing of incoming data packets in the specified network

Keywords: secure corporate multiservice communication network, aggregate flow, channel resource, VPN gateway

UDC 621.396
DOI: 10.15587/1729-4061.2023.285414

IMPROVING THE TECHNOLOGY FOR PROCESSING THE AGGREGATED DATA FLOW OF A SECURE CORPORATE MULTISERVICE COMMUNICATION NETWORK

Liubov Berkman
Corresponding author
Doctor of Technical Sciences, Professor, Vice-Rector for Educational and Scientific Work*
E-mail: berkmanlubov@gmail.com
Andrii Zakharzhevskyi
PhD
Department of National Security and Defence Strategy
The National Defence University of Ukraine named after Ivan Cherniakhovskyi
Povitroflotskyi ave., 28, Kyiv, Ukraine, 03049
Kostiantyn Lavrinets
PhD, Associate Professor
Department of Telecommunication Systems and Networks*
*State University of Telecommunications
Solomyanska str., 7, Kyiv, Ukraine, 03110

Received date 15.05.2023
Accepted date 19.07.2023
Published date 30.08.2023

How to Cite: *Berkman, L., Zakharzhevskyi, A., Lavrinets, K. (2023). Improving the technology for processing the aggregated data flow of a secure corporate multiservice communication network. Eastern-European Journal of Enterprise Technologies, 4 (9 (124)), 14–23. doi: https://doi.org/10.15587/1729-4061.2023.285414*

1. Introduction

Under the modern conditions of intense social and civilizational upheavals, military-political and economic confrontations, the issue of transfer and processing of information with limited access requires a constant solution to the task of reliably protecting its arrays from unauthorized access.

One of the ways to improve the effectiveness of information protection is to use a secure corporate multi-service communication network (SCMCN) based on public access channels for its transmission.

The issue of preserving the integrity and protection of information from unauthorized access in telecommunication networks of various purposes is a constant task of the functioning of existing and development of new telecommunication networks [1].

Vulnerability analysis and the implementation of information protection tasks in SCMCN is determined by the requirements of the current legislation of Ukraine and is extremely important for the improvement of protected telecommunication networks not only at the regional, but also at the global level, connecting various countries and continents with international connections [2].

One of the features of the functioning of such networks is the active use of aggregated data flows in them, which, as a rule, function according to separate, specially devised

mathematical models. The construction and implementation of new and improved implemented mathematical models of aggregated data flow in a secure information communication network is an important direction in the field of ensuring the effectiveness of information security [1, 2]. The specified models could be used to predict the bandwidth of the network, determine the maximum number of users that the network can serve, as well as to develop communication network management algorithms. Usually, such models are built on the basis of certain theories and procedures: Markov model, queuing theory, diffusion model, etc. [1, 3].

One of the important aspects of aggregated data flow modeling is the analysis of the interaction between various network elements, such as nodes, routers, and other devices during data transmission between them. An additional factor that deepens the problem of modeling the aggregated flow of data in SCMCN is the presence in the schemes of its construction of a Virtual Private Network gateway (VPN gateway) and the formation of a VPN tunnel protected by it [1, 3].

The main criterion, based on the achievement of which mathematical models of aggregated data flows are built and applied, is the quantitative assessment of the necessary channel resource (CR). Subsequently, the value of CR is used for guaranteed service of the aggregated data flow by mechanisms for controlling the admission of data flows in the SCMCN channel. To evaluate CR, as a rule, at the first stage, the parameters of the aggregated traffic at the output of the load management system are evaluated. At the next stage, subject to taking into account the normalized values of flow service quality parameters, a decision is made to admit or deny the admission of a new data stream to the network channel [1, 2].

Analysis of the process of construction and operation of SCMCN schemes shows that its main work processes are admission management in information communications, transfer of data blocks, implementation of control algorithms, and smoothing of the traffic profile.

Solving the scientific task of improving the quality of the specified processes involves the development and improvement of the methodological apparatus for assessing the necessary channel resource of the network. The main goal of such an assessment is the predicted dynamic reservation of the channel resource for promising incoming aggregated data flows, which requires a separate procedure. One of the aspects of such development of management methods and evaluation and reservation models is the consideration of the condition regarding the presence of an additional element in the SCMCN scheme that would ensure the security of the network's functioning, namely the VPN gateway.

In the process of carrying out a number of studies and experiments, it was established that one of the main features of the influence of VPN gateways on the parameters of the aggregated data flow of SCMCN is the formation of a certain influence on the protected transmission channel of the aggregated data flow. The obtained results of the assessment of the effect of VPN gateways on the parameters of the aggregated data transmission channel in the SCMCN network showed that the procedures of the VPN gateway have an impact on the following parameters of the transmitted traffic. Namely: peak (p) and average (r) transmission speed of information streams, length of generated packets (L) of video telephony and IP telephony services [3, 4].

Also, an additional effect of such an influence is a decrease in the effectiveness of the use of cryptographic protection of information in SCMCN. This is due to the fact that the presence of VPN gateways does not allow the algorithms to ensure the quality of service (QoS) of the IntServ architecture to fully interact through the DiffServ segment in the packet switching network. This is determined by the process of adding a new packet header with open IP addresses and introducing an additional delay into the packet processing process [5, 6].

It is obvious that the value of the channel resource is directly related to the above parameters of the data transmission channel and to the additional delay in the processing of packets in the protected channel [1, 4]. Accordingly, the procedure for assessing the necessary channel resource and its dynamic reservation should take into account the values of the above-mentioned channel parameters and be related to the processing delay time of packets of the aggregated data flow in the specified channel.

Based on the above, the solution to the scientific task of increasing the efficiency of channel resource reservation in relation to SCMCN is timely and relevant. And this requires the search for new theoretical and practical approaches to the development of new ways of solving it.

2. Literature review and problem statement

A number of scientific works [2, 3, 7–14] consider the issue of processing aggregated data streams and estimating the necessary channel resource.

General issues of building and functioning of secure corporate multi-service communication networks based on public access channels are covered in [2, 3]. These papers consider the general principles of building effective secure telecommunication networks and the implementation of information protection in them using special network elements. But the direct influence of the specified network element on the operation of this type of network and the issue of assessing the necessary channel resource for the aggregated data flow for all types of networks are not covered in these works.

In [7], a virtual version of a separate secure network based on the use of a VPN gateway is proposed as a means of ensuring the necessary level of security for specific connections that cover large networks. The main indicator for evaluating the efficiency of data transmission in the cited work is the time delay and throughput of data packets through a secure channel. When calculating the indicated indicators, the parameters of the necessary channel resource were not considered. Accordingly, there is no assessment of the degree of influence of the channel resource of the network and the presence of a VPN gateway in it on the proposed values of data transmission efficiency indicators in the cited work.

Work [8] considers the evaluation of the effectiveness of the delay time calculation model presented in the article as a criterion for traffic analysis in VPN tunnels. It suggests dividing protected traffic into different categories according to the type of traffic, for example, viewing information, streaming video, etc. The model proposed in the cited paper does not necessarily estimate the channel resource of the aggregated data stream, which is used to estimate the delay time accordingly. Accordingly, the value of the specified channel resource in the presented model is not interconnected with the flow delay time.

In [9], the traffic estimation of the aggregated data flow through the VPN tunnel of the protected telecommunication network is proposed based on the estimation of the data transmission time. The work presents separate evaluation results for channels with and without a VPN gateway but there are no results based on which it is possible to trace the influence of the parameters of the required channel resource on the determined time parameters of traffic data transmission.

Consideration of data traffic parameters transmitted in protected networks of aggregated data flow is given in [10]. In order to improve the effectiveness of network security, a certain classification of traffic is proposed in the work and the values of its parameters are determined in accordance with this classification. The relationship between the specified parameters and the value of the necessary channel resource and the delay time of the stream and the channel is absent in the cited work.

The results of the evaluation of the effect of the VPN gateway on the parameters of data transmission by an aggregated stream are reported in [11]. The data set presented in the paper contains a generalized model of network traffic consisting of different types of network, such as Internet, e-mail, video conferencing, streaming video, and terminal services. For one model of network traffic, data is measured for different scenarios, i. e., for data transmission through different types of VPN gateway and without it.

Against the background of the presence in the cited work of large arrays of data characterizing the effect of the VPN gateway, it lacks the results of the analysis and assessment of the impact of the values of the specified values on the channel resource and directions of its dynamic reservation.

In [12], a balanced scheme of queue management on router interfaces of telecommunication networks is proposed. The novelty of the proposed scheme consists in the application of a two-level calculation method. At the first level, the task of distributing and optimally aggregating packet flows according to queues formed on the router interface is solved. At the second level, the task of allocating and balancing the bandwidth of the interface is solved, taking into account the classification of flows and queues. Bandwidth in the cited work is balanced on the basis of the necessary channel resource, but there are no corresponding principles of its value calculation and subsequent dynamic reservation in the work.

The issue of the security of a secure data transmission network and the construction of its architecture under the condition of optimizing the transmission of large data sets by aggregated streams is considered in [13]. The authors solve the issue of network protection with additional secure encryption of data transmitted through a network protected by a VPN gateway. This paper provides a comparative assessment of the effectiveness of data transmission over channels with VPN protection according to two models of network protection and a new model personally proposed by the authors. In order to increase the efficiency of the transmission of aggregated traffic, the cited paper proposes an improvement of the data transmission channel architecture, which does not involve the allocation of a channel resource and its dynamic reservation.

One of the ways to improve the performance of a protected network in terms of data transmission is the classification of network traffic, which is an important and problematic aspect of network resource management, as stated in [14]. In the work, several algorithms for classification, detection, and management of the aggregated data flow under the conditions of influence on the data transmission channel of the VPN gateway are considered. But the process of direct traffic detection does not take into account the channel resources of the system, which are necessary for its direct reception and further management. Accordingly, dynamic reservation of the specified channel resource is not considered in the work.

The review of studies that consider the issue of processing aggregated data flows in the SCMCN allowed us to identify certain inconsistencies that significantly affect the effectiveness of the SCMCN operation and require conducting research into their elimination. One of such important studies is the solution of the task of dynamic reservation of the channel resource as one of the aspects of increasing the efficiency of SCMCN operation.

3. The aim and objectives of the study

The purpose of this study is to improve the technology of processing aggregated data flow in SCMCN by implementing a model of dynamic channel resource reservation. This will make it possible to increase the efficiency of the operation of the specified network when managing the aggregated data flow of SCMCN.

To achieve the goal, the following tasks were set:

– to build mathematical dependences and, based on them, a holistic model of dynamic reservation of the channel resource of the aggregated data flow for a secure corporate multi-service communication network;

– to evaluate the channel resource and determine its impact on the data channel service quality criterion.

4. The study materials and methods

The object of our research is the process of processing aggregated data flow in a secure corporate multi-service communication network.

The question of the impact of dynamic parameters of the reserved channel resource on the processing delay of the aggregated data flow in the protected corporate multiservice communication network is investigated.

The following was adopted as an assumption and simplification during the research. The WFQ “weighted fair queuing” algorithm is applied at the entrance of the scheduler of the secure communication channel. For each service provided, a channel resource is assigned with an orientation to the possible peak load in the process of data transmission and processing.

The classic structure of a secure corporate multi-service communication network was chosen for research. The scheme of its construction is shown in Fig. 1.

The specified SCMCN has a VPN gateway in its structure. The total aggregated data flows passing through the VPN tunnel consist of separate flows.

As a criterion for the quality of service of the aggregated data flow, the end-to-end delay time for the transmission of the data packet of the incoming flow arriving at the border router of the data transmission channel was chosen.

The MATLAB programming and numerical calculation platform was used for data analysis and visualization.

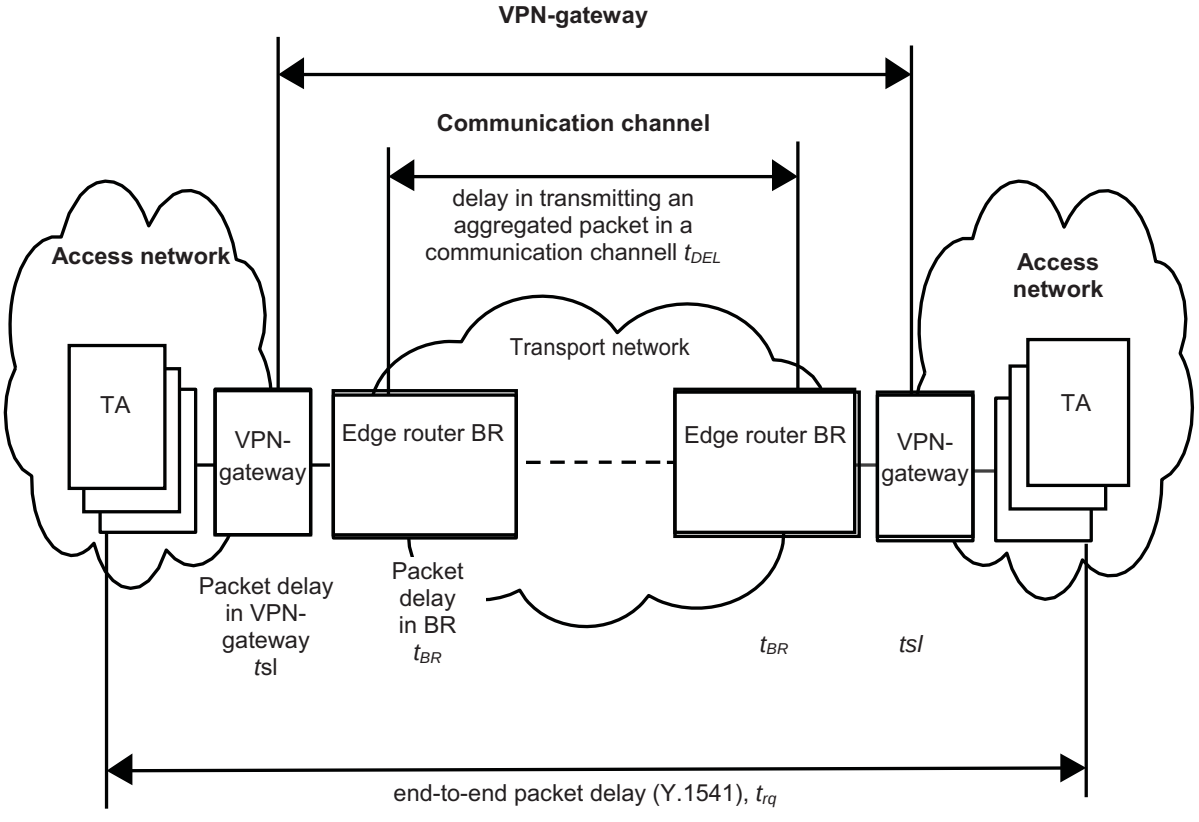

Fig. 1. Structural diagram of a secure corporate multi-service communication network with a VPN gateway

5. Model of dynamic reservation of the channel resource of the aggregated data flow

5. 1. Building a model of dynamic reservation of the channel resource of the aggregated data stream

The theory of network calculation (NC – Network Calculus) [3, 15] was used to build a model of dynamic reservation of the channel resource of the aggregated data flow. Its application makes it possible, based on the known numerical parameters of the traffic shaper, inherent in the flow management system of the VPN gateway of the SCMCN access network, to calculate the limit estimates of the parameters of the criterion of the quality of service of the data flow in the network (KO).

According to this theory, the input flow of data entering the traffic shaper of the VPN gateway flow control system (Fig. 1) is limited by the deterministic function of the input flow. The output data flow directly depends on the adopted service model, and is limited by the service function [4, 6]. The deterministic nature of the used assumptions of mathematical models is quite adequate if we take into account that in real networks traffic is always limited by the bandwidth of the communication channel. This is caused by the use of load-forming mechanisms implemented in the IntServ and DiffServ architectures [4, 6]. The description of data flows using this mathematical apparatus makes it possible to reduce complex nonlinear systems to linear ones.

The cumulative function $A(t)$ is used to describe the data flows coming from the sources to the traffic shaper of the VPN gateway flow control system, which determines the number of bytes of data received in the system during the time interval $(0, t]$. At the same time, it is assumed that $A(0)=0$. The function $A(t)$ is always increasing. Hereafter, such a function is referred to as a deterministic arrival function.

Flow A is a bounded function $f(t)$ if and only if for all $f(t)$ the following condition is met:

$$A(t_2)-A(t_1)\le f(t_2-t_1). \quad (1)$$

From a computational point of view, it is much more convenient to use continuous functions to describe telecommunication systems. However, real systems use minimal indivisible blocks of data – packets, and therefore, models describing the continuous operation of transmission systems are ideal and take into account the "sampling" error. In multi-service IP networks using Ethernet technology at the EMVOS channel level, the incoming load can be approximated by a continuous function. This is explained by the fact that the dispersion of the packet sizes and the inter-packet interval is quite large [4, 5].

The following are adopted as the main data flow parameters of SCMCN. The maximum data packet size of the i-th stream L_i (bytes), the known peak packet generation rate p_i (bytes/s), the average packet generation rate r_i (bytes/s) and the allocated buffer size b_i (bytes). Then, in the flow management system of the VPN gateway of the SCMCN access network with an implemented traffic shaping function, the output data flow is described by the following expression [3, 4, 16]:

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

where $A_i(t)$ is the amount of load of the i-th flow that arrived in the system during the time period $(0, t]$ for the worst case, when the size of the packets is equal to the maximum possible value of L_i.

At the same time, the peak value of the packet arrival speed of the i-th flow must always be strictly higher than the average speed in the interval of the average duration of the session for the analyzed flow. That is, $p_i > r_i$, and this condition is mandatory for all expressions considered below, which does not contradict the physical meaning of real processes in the network.

Assuming that the flow at the output of the VPN-gateway flow control system when reserving a share of the CR of the k-th communication channel with the bandwidth R_{BW} for the i-th data stream R_i (bytes/s) is determined by the condition $\sum_i^n R_i \le R_{BW}$. The specified flow can be described by the service function $W_i(t)$, which determines the minimum amount of data transmitted in the communication channel during time t [16]:

$$W_i(t) = R_i(t - t_{BLi}), \tag{3}$$

where t_{BLi} is defined by the expression:

$$t_{BLi} = \frac{L_i}{R_i} + \frac{L_i}{R_{BW}}. \tag{4}$$

The service function of the WFQ scheduler is a rate-delay function with the characteristics of rate R_i and delay t_{BLi} in seconds.

Let's take into account the fact that the delay of the packet transmission from the VPN gateway in the access network to the border router (BR) of the transport network is not taken into consideration. The flow description in the flow management system of the VPN gateway can be carried out to the BR traffic shaper of the transport network. Then the volume characteristics of the data flows at the output of the BR traffic shaper of the SCMCN transport network can be represented in the form shown in Fig. 2 [16, 17]:

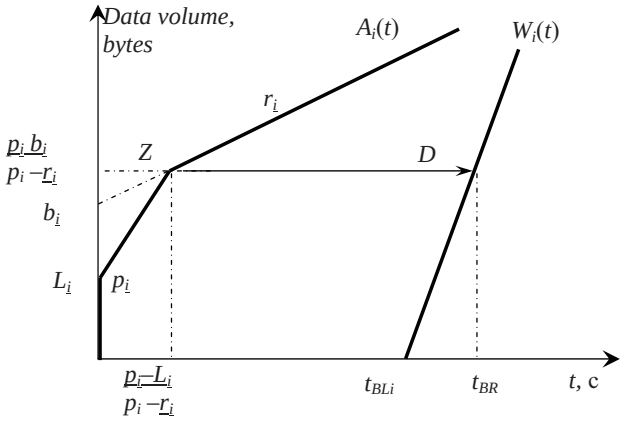

Fig. 2. Graphic representation of volume characteristics of data flows at the output of a network device of a secure corporate multi-service communication network

Fig. 2 shows the load arrival and service functions, illustrating the procedure for calculating the parameters that characterize the provision of a guaranteed quality of service (QoS) criterion for the worst case of critical overload. The input of the input data flow scheduler, implemented according to the "weighted fair queuing" (WFQ) algorithm, receives the load passed through the "marker basket" traffic shaper, which makes it possible to formally describe the load characteristics of variable speed flows [4, 5].

The specified WFQ algorithm makes it possible to apply any actions (resetting or relabeling) only to packets that do not match the declared profile. Conformal packets pass through the "basket with markers" without additional delay associated with the limited intensity of the output load [4, 5].

In the control systems for the admission of data streams to the network, an important advantage of the mathematical apparatus for describing traffic parameters at the output of network devices is the minimum time for calculating the necessary CR [17, 18]. This is especially important when the intensity of requests for service to SCMCN and the requirements for the admission time of the data flow do not allow the use of analytical expressions that are difficult to calculate without a significant increase in the performance of processors.

Ensuring the required level of the quality of service (QoS) criterion for each transport data stream entering BR is ensured by estimating the upper delay time of packet processing in the BR. Assuming the condition that the service mechanism is implemented on the basis of the scheduler of the WFQ class, a delay is set for the i-th flow, which should not exceed the value given by expression (5) [18, 19]:

$$t_{BR} \le \frac{t_{(rq)} - t_{BW} - 2t_{sl}}{2}. \tag{5}$$

Based on the approach presented in [5, 17, 18], it becomes possible to calculate the values of the controlled parameters of the service system based on the known functions of arrival and service. They are determined by the position of the straight line ZD (Fig. 2) as the upper limit of the total delay of the packet in BR and the condition that $p_i > r_i$:

$$t_{BR} = \begin{cases} \dfrac{(b_i - L_i)(b_i - R_i)}{R_i(p_i - r_i)} + \dfrac{2L_i}{R_i}; \\ \dfrac{2L_i}{R_i} + \dfrac{L_i}{R_{BW}}, \end{cases} \quad R_i > p_i > r_i. \tag{6}$$

In expression (6), the value of t_{BR} has the physical meaning of the upper limit value of the delay time, which guarantees the required level of KO of the data streams arriving at BR. This value can be ensured by reserving bandwidth R_i (in bytes/sec) in BR for further servicing of the incoming data stream.

The value of t_{BR}, in turn, depends on the value of the bandwidth R_i allocated for data flow maintenance.

The basis of operation of the access node to the SCMCN transport network during data flow admission management is the assessment of the necessary CR for the aggregated data flow of the VPN tunnel. At the same time, the CR allocated to this flow is the most important of the network resources. It is taken into account that the buffer space of the switching equipment port is also a resource for the calculation of which exact analytical expressions are required. But the cost of the memory elements that implement the functioning of the buffer is much lower than the cost of renting the CR of the transport network [17, 18]. That is, increasing the size of the buffer space does not bring great economic losses. In this regard, it is assumed that the BR buffer has an infinite length.

When operating a communication network, the inverse problem often arises. Its essence is that given the required end-to-end packet delay of the *i*-th data flow ($t_{(rq)}$), it is necessary to estimate the required CR to service the proposed load allocated to BR:

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

The value of the required end-to-end packet delay of the *i*-th data stream is determined by expression (6). The value of the end-to-end end-to-end packet delay of the *i*-th data stream $t_{(rq)}$ is determined by the Y.1541 recommendation [20].

The analysis of the structure of SCMCN and the determined features of its functioning showed that the VPN gateway implements the aggregation of data flows into the general flow of the VPN tunnel during data transmission and the division of the general flow into sub-flows during reception [6, 11, 16].

For the analytical description of the aggregated data flow coming from the output port of the network element, the concept of traffic characterization of aggregated flows presented in RFC 2216 is used [4, 5]. According to this concept, the sum of data flows (*n*), specified as TSpec, is described by the total arrival function (TAF) $A_{TAF}(t)$:

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

where L_i is the maximum packet length of the *i*-th flow out of *n* flows included in the aggregate data flow of the VPN tunnel; p_{TAF} is the peak rate of packet generation of the aggregated flow of the VPN tunnel; r_{TAF} is the average packet generation speed of the aggregated flow of the VPN tunnel; b_i (byte) – the allocated buffer size of the traffic shaper of aggregated flows of VPN tunnels, equal to the size of the buffer allocated for serving the *i*-th flow out of *n* flows that are part of the aggregated data flow of the VPN tunnel.

Expression (8) allows us to describe the most complex case of traffic generation by *n* sources, on the basis of which it becomes possible to calculate the required CR for *n* flows, taking into account the provision of t_{BR} in accordance with all the requirements received by KO. At the same time, the aggregated data flow is served in the routers of the SCMCN transport network as an isolated connection with the FIFO g_j service discipline in a separately reserved buffer [13, 21].

In order to estimate the required CR for aggregated data flows based on the theory of network computing, the following methods of data flow maintenance are proposed.

The technique of isolated maintenance of data flows is described as follows:

$$R_{IS}(n) = \sum_{i=1}^{n} \frac{p_i \frac{(b_i - L_i)}{(p_i - r_i)} + 2L_i}{t_{BR} + \frac{(b_i - L_i)}{(p_i - r_i)} - \frac{L_i}{R_{BW}}}. \quad (9)$$

The technique of group maintenance of data flows based on the total arrival function (TAF):

$$R_{TAF}(n) = \frac{\sum_{i=1}^{n} \frac{\sum_{i=1}^{n}(b_i - L_i)}{\sum_{i=1}^{n}(p_i - r_i)} + 2L_i}{t_{BR} + \frac{\sum_{i=1}^{n}(b_i - L_i)}{\sum_{i=1}^{n}(p_i - r_i)} - \frac{L_i}{R_{BW}}}. \quad (10)$$

In the above expressions (9) and (10), we accepted:

n – the number of flows in the aggregated data flow;

i is the serial number of the stream included in the aggregated data stream;

L_i is the maximum size of the data packet of the *i*-th flow, selected from all flows of the *n* aggregated data flow;

t_{BR} is the minimum required delay before packet processing in BR among *n* data streams;

R_{BW} is the bandwidth of the communication channel;

p_i is the peak packet generation rate of the *i*-th flow;

r_i is the average packet generation speed of the *i*-th stream;

b_i is the allocated buffer size of the traffic shaper for the *i*-th flow.

5. 2. Evaluation of the channel resource and its influence on the criterion of the quality of service of the data transmission channel

Numerical values of data flow parameters generated by the terminal equipment involved in the standard structure of SCMCN (Table 1) [11, 17] were used to calculate the required CR. The bandwidth of channels R_{BW} is assumed to be 100 Mbit/s.

Table 1

Numerical values of traffic parameters

Data streams from the terminal	Traffic parameter values					
	Video-telephony			IP-telephony		
	p, Mbps	*r*, Mbps	*L*, Byte	*p*, Mbps	*r*, Mbps	*L*, Byte
	2.1	0.87	1346	0.112	0.096	214

Calculations were made using the proposed model of isolated service of data flows – expression (9) and the model of group service of data flows based on TAF – expression (10) [22, 23].

The obtained values of the necessary CR depending on the incoming load when describing the behavior of the aggregated flow using the existing model of isolated service of data flows – (9) and the model of group service of data flows based on TAF – (10) are shown in Fig. 3, 4.

In Fig. 3, 4, R_{EF} – the value of the reserved CR for *n* flows of real-time services, obtained on the basis of the calculation of the effective speed of transmission of the information flow [5, 21] according to the expression:

$$R_{EF}(n) = n\left(1 - \frac{1}{50}\log P_{loss}\right) \times$$
$$\times r_i\left(1 + 3\left(-\frac{2p_I}{R_K}\log P_{loss}\right)\left(1 - \frac{r_i}{p_i}\right)\right),$$

where $P_{loss}=10^{-3}$ is the packet loss coefficient for zero (0) – quality of service class.

Calculations of the maximum value of the delay time for the flow of data transmission over IP-telephony and video-telephony channels, as well as dependences approximating their average values, are shown in Fig. 5, 6, respectively.

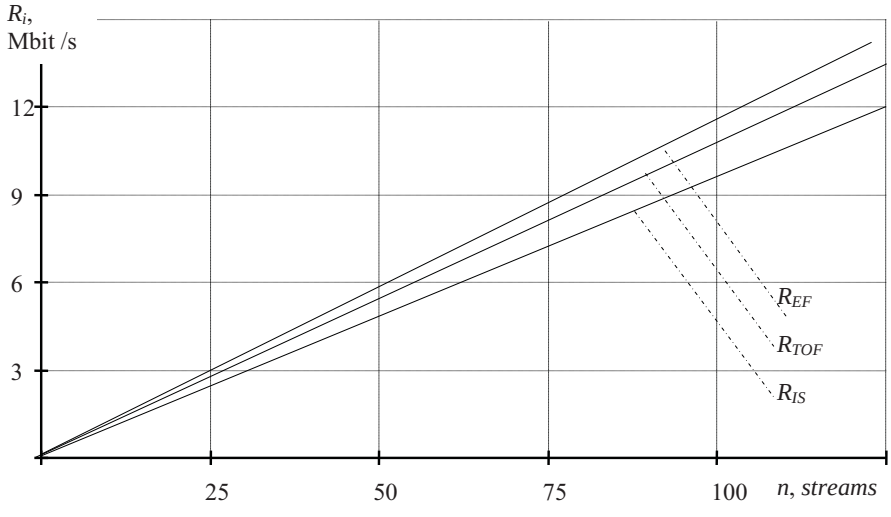

Fig. 3. The value of the necessary channel resource for the maintenance of a grouped flow of data transmission over the IP-telephony channel

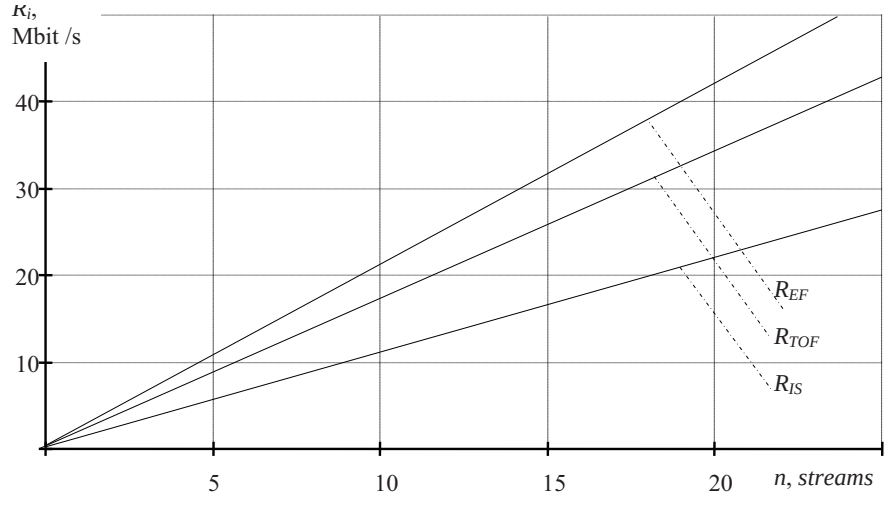

Fig. 4. The value of the necessary channel resource for the maintenance of a grouped flow of data transmission over the video telephony channel

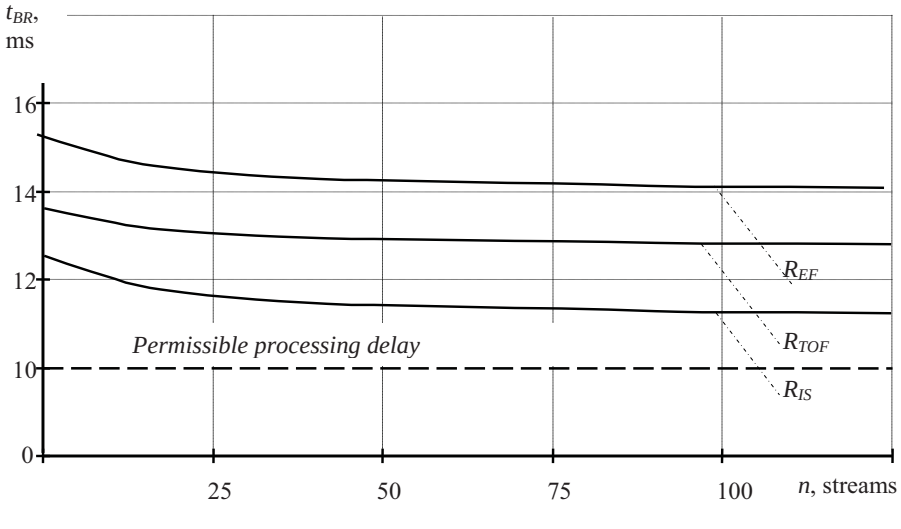

Fig. 5. Maximum achievable delay in the border router for servicing a grouped stream over an IP telephony channel

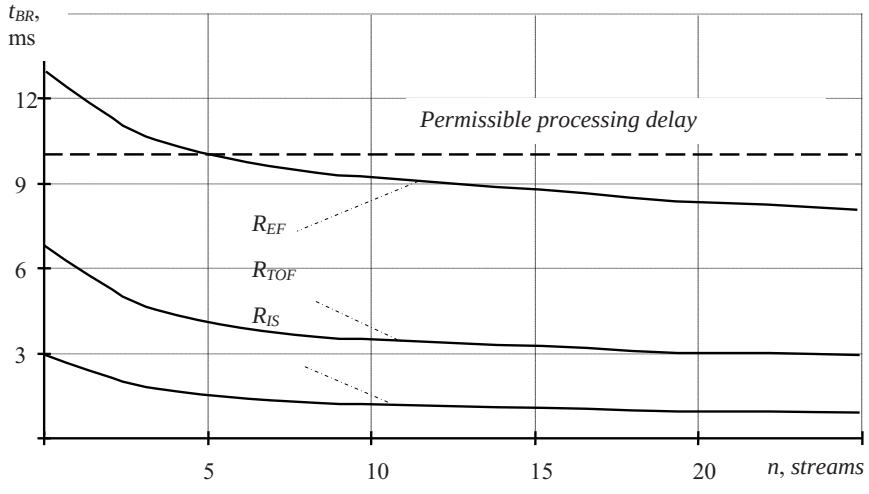

Fig. 6. Maximum achievable delay in the border router for servicing a grouped stream over a video telephony channel

When evaluating the results of the calculation, it is accepted that the numerical value of the time required for the processing of the BR packet, based on the physical and logical topology of this SCMCN in accordance with the Y.1541 recommendation, should not exceed 10 ms [20].

Taking into account the proposed approach to static reservation, the daily load factor of channels leased by a typical transport-level SCMCN can be represented in the form of one of the options for the daily distribution of CR, which is shown in the diagram in Fig. 7 [22, 23].

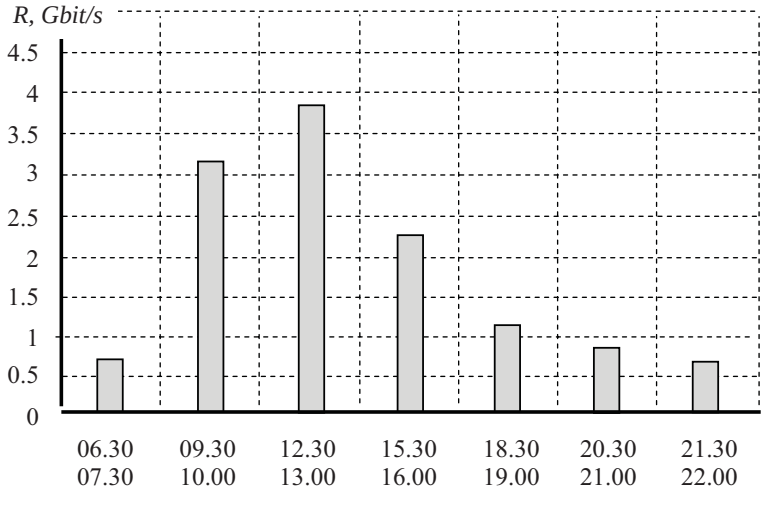

Fig. 7. Load level of communication channels of a typical secure corporate multi-service communication network of the transport layer

The data on the basis of which the diagram in Fig. 7 is shown were obtained for the peak load, taking into account the predicted reservation of the channel resource for a period of up to 24 hours of service of the aggregated data flow.

6. Discussion of results of the assessment of the influence of the channel resource on the criterion of the quality of service of the data transmission channel

Analysis of the dependences in Fig. 3, 4 reveals that the method of isolated maintenance of the data flow provides a lower value of CR in comparison with the group technique. On average, the gain is from 10 to 20 percent for IR and video telephony. This is due to the more flexible management process of the border router's incoming data storage buffer in the isolated service mode. With a flexible buffer management process, isolated service does not lead to significant loss of incoming packets due to BR buffer overload.

Analysis of the resulting dependences shown in Fig. 5, 6 shows that, in accordance with the calculated values of the necessary CR for aggregated traffic service flows, certain features are formed in relation to encrypted IP telephony. Their influence is manifested in the fact that with an increase in the number of component flows, the necessary delay in the processing of data packets is not provided. That is, for the total aggregated BR data flow, the required delay of data packet processing may not be provided within the established regulatory values [24–26].

When serving aggregated streams of encrypted video telephony, a given 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 results of calculations of the CR value as a function of the number of components of the aggregated data flow of various types indicate a discrepancy between the speed of receiving data packets and the speed of their service. In the first case, the selected CR is less than the peak transmission speed, in the second, on the contrary, it exceeds it.

Certain difficulties in the implementation of existing mathematical models in SCMCN lead to the need to statically fix the CR for each service provided, with an orientation to the possible peak load.

The diagram in Fig. 7 shows that allocation of CR for peak load makes it possible to guarantee the required level of CO during the day, however, approximately 60 % of the loading time of the transport channel does not exceed 40 % of the loading level.

This gives grounds for further calculations of the involved economic resource, for example, for the lease of the data transmission channel and its losses from the inactive CR.

Thus, our work establishes and substantiates the interrelationships and mutual influences of the parameters of the aggregated data flow on the value of the channel resource and the necessary delay in the processing time of data packets in the transmission channel. The studies were carried out in relation to the secure corporate multi-service communication network, taking into account the influence of the VPN-gateway functioning procedures on the parameters of the traffic transmitted through the specified network.

In order to establish the specified interrelationships and assess the impact of traffic parameters on the value of the channel resource, a corresponding assessment model was

built and presented in the paper. The specified model takes into account the order of isolated and group service of data streams based on the total arrival function. It provides an assessment of the influence of the channel resource on the value of the required time delay for the processing of data packets in the protected transmission channel of SCMCN.

The proposed model makes it possible to evaluate the channel resource and its influence on the quality criterion of data transmission channel service depending on the selected method of servicing the aggregated data flow. This, in aggregate, allows dynamic reservation of the channel resource of the aggregated data flow in accordance with the specified delay time values. This improves the quality of functioning of the secure corporate multi-service communication network.

The results reported in the current work on the development of a complete model of dynamic reservation of the channel resource make it possible to estimate its quantitative values in accordance with the number of aggregated flows and substantiate recommendations for ensuring the specified value of the data transmission delay time.

The specified evaluation model can be used in practical improvement of existing and development of new secure corporate multi-service communication networks.

A limitation of this study is that the presented evaluation model is designed for the application of the WFQ "weighted fair queuing" algorithm at the input of the scheduler. This makes it possible to formally describe the load characteristics of streams with a variable speed but creates conditions for the loss of a certain number of data packets that do not match the declared profile and do not pass through the "marker basket".

Limitations also include the accepted condition of static fixing of CR for each service provided, with an orientation to the possible peak load. This is due to certain difficulties in the implementation of existing mathematical models in SCMCN, the solution of which requires additional research in the direction of creating a separate model for their implementation.

Among the shortcomings of the model proposed in the work is the condition adopted during modeling about the infinite length of the BR buffer. In reality, the buffer has limited values that, with a significant load on the data transmission channel, SCMCN can affect the dynamic reservation of the channel resource and delay the processing time of data packets. This limitation of the value of the BR buffer is especially manifested in various variants of building code structures of data packets [27].

The lack of algorithms for calculating the optimal length of the BR buffer in accordance with the required channel resource creates the next scientific task and requires conducting relevant research.

As further promising research and development in the direction of increasing the efficiency of the functioning of the protected corporate multi-service network, the subsequent work is proposed in the direction of further improving the quality of the dynamic reservation of the channel resource by the method of flexible reservation of the BR clipboard length. This will ensure the achievement of a higher quality of channel usage during peak loads. One of the ways to solve such a task can be the construction of a separate model of dynamic anchoring of the channel resource for each SCMCN service according to the current load with an orientation to the possible peak load, which results from the specifics of the use of this service.

7. Conclusions

1. A model of dynamic reservation of the channel resource of the aggregated data flow of the secure corporate multi-service communication network has been built. The proposed model makes it possible to set the quantitative values of the reserved channel resource for different service techniques depending on the number of component flows in the total aggregated data flow of the VPN tunnel. A feature of the model is the ability to evaluate the influence of the reserved channel resource on the quality criterion of data transmission channel service depending on the selected technique of servicing the aggregated data flow.

2. It is established that an increase in the density of the aggregated data stream requires an increase in the reserved channel resource. At the same time, its value is influenced by the way of servicing the aggregated data flow in the VPN tunnel of the secure corporate multi-service communication network. Application of the isolated service technique gives a gain in the allocated resource for the channel reserve from 10 to 20 percent compared to the group service method for IR and video telephony.

It is shown that with an increase in the number of component streams in the aggregated data stream, 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 VPN tunnel of a secure corporate multi-service communication network, the type of data flow is important. In general, for the aggregated data flow of encrypted video telephony, a given level of the required delay in the processing of data packets is provided by exceeding the reserved resource of the peak value of the transmission rate.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study and the results reported in this paper.

Funding

The study was conducted without financial support.

Data availability

All data are available in the main text of the manuscript.

Acknowledgment

We express our respect and deep gratitude to Mr. Oleksandr Drobyk, PhD, Professor, Director of the Scientific Center of the State University of Telecommunications for fruitful cooperation and significant contribution to the preparation of material for this study.

References

1. Popivskyi, V. V., Lemeshko, O. V., Kovalchuk, V. K. Plotnikov, M. D., Kartushyn, Yu. P. et al. (2012). Telekomunikatsiini systemy ta merezhi. Struktura y osnovni funktsiyi. Vol. 1.
2. Zakhyst informatsiyi na obiektakh informatsiynoi diyalnosti. Stvorennia kompleksu tekhnichnoho zakhystu informatsiyi. Osnovni polozhennia. ND TZI 1.1-005-07. Available at: https://tzi.com.ua/nd-tz-1.1-005-07.html
3. Halkin, V. V., Parkhomenko, I. I. (2016). Vykorystannia VPN-tekhnolohiy dlia zakhystu informatsiyi v kanalakh korporatyvnykh merezh. Problema kiberbezpeky informatsiyno-telekomunikatsiynykh system: materialy nauk.- tekhn. konf. Kyiv: KNU, 66–76.
4. Buriachok, V. L., Anosov, A. O., Semko, V. V., Sokolov, V. Yu., Skladannyi, P. M. (2019). Tekhnolohiyi zabezpechennia bezpeky merezhevoi infrastruktury. Kyiv: «KUBH», 218. Available at: https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf
5. Popovskyi, V. V., Oliinyk, V. F. (2011). Matematychni osnovy upravlinnia i adaptatsiyi v telekomunikatsiynykh systemakh. Kharkiv: TOV "Kompaniya SMIT", 362.
6. IPSec – protokol zakhystu merezhevoho trafiku na IP-rivni.
7. Talib, H. A., Alothman, R. B., Mohammed, M. S. (2023). Malicious attacks modelling: a prevention approach for ad hoc network security. Indonesian Journal of Electrical Engineering and Computer Science, 30 (3), 1856. doi: https://doi.org/10.11591/ijeecs.v30.i3.pp1856-1865
8. Almomani, A. (2022). Classification of Virtual Private networks encrypted traffic using ensemble learning algorithms. Egyptian Informatics Journal, 23 (4), 57–68. doi: https://doi.org/10.1016/j.eij.2022.06.006
9. Balachandran, A., Amritha, P. P. (2022). VPN Network Traffic Classification Using Entropy Estimation and Time-Related Features. Smart Innovation, Systems and Technologies, 509–520. doi: https://doi.org/10.1007/978-981-16-3945-6_50
10. Ma, X., Zhu, W., Wei, J., Jin, Y., Gu, D., Wang, R. (2023). EETC: An extended encrypted traffic classification algorithm based on variant resnet network. Computers & Security, 128, 103175. doi: https://doi.org/10.1016/j.cose.2023.103175
11. Naas, M., Fesl, J. (2023). A novel dataset for encrypted virtual private network traffic analysis. Data in Brief, 47, 108945. doi: https://doi.org/10.1016/j.dib.2023.108945
12. Lemeshko, O., Lebedenko, T., Nevzorova, O., Snihurov, A., Mersni, A., Al-Dulaimi, A. (2019). Development of the Balanced Queue Management Scheme with Optimal Aggregation of Flows and Bandwidth Allocation. 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM). doi: https://doi.org/10.1109/cadsm.2019.8779246
13. Patil, H. K., Chen, T. M. (2017). Wireless Sensor Network Security. Computer and Information Security Handbook, 317–337. doi: https://doi.org/10.1016/b978-0-12-803843-7.00018-1
14. Afuwape, A. A., Xu, Y., Anajemba, J. H., Srivastava, G. (2021). Performance evaluation of secured network traffic classification using a machine learning approach. Computer Standards & Interfaces, 78, 103545. doi: https://doi.org/10.1016/j.csi.2021.103545
15. Geyer, F., Scheffler, A., Bondorf, S. (2023). Network Calculus With Flow Prolongation – A Feedforward FIFO Analysis Enabled by ML. IEEE Transactions on Computers, 72 (1), 97–110. doi: https://doi.org/10.1109/tc.2022.3204225
16. Kovalenko, A., Kuchuk, H., Tkachov, V. (2021). Method of ensuring the survivability of the computer network based on vpn-tunneling. Control, Navigation and Communication Systems. Academic Journal, 1 (63), 90–95. doi: https://doi.org/10.26906/sunz.2021.1.090
17. Kuchuk, N., Gavrylenko, S., Sobchuk, V., Lukova-Chuiko, N. (2019). Redistribution of information flows in a hyperconvergent system. Advanced Information Systems, 3 (2), 116–121. doi: https://doi.org/10.20998/2522-9052.2019.2.20
18. Svyrydov, A., Kovalenko, A., Kuchuk, H. (2018). The pass-through capacity redevelopment method of net critical section based on improvement ON/OFF models of traffic. Advanced Information Systems, 2 (2), 139–144. doi: https://doi.org/10.20998/2522-9052.2018.2.24
19. ITU-T Technical Report. XSTR-SEC-MANUAL Security in telecommunications and information technology (7th edition) (2022). International Telecommunication Union. Available at: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTSS-2020-4-PDF-E.pdf
20. Y.1541: Network performance objectives for IP-based services (2011). Available at: https://www.itu.int/rec/T-REC-Y.1541-201112-I/en
21. Hnatushenko, V. V. (2014) Modeliuvannia ahrehovanoho trafiku peredachi danykh na osnovi modeli ON/OFF. Systemni tekhnolohiyi, 5, 65–72. Available at: http://nbuv.gov.ua/UJRN/st_2014_5_10
22. Lebedenko, T., Goloveshko, M., Holodkova, A. (2019). Investigation of the method of active queue management on the interfaces of telecommunication networks routers. Control, Navigation and Communication Systems. Academic Journal, 4 (56), 57–62. doi: https://doi.org/10.26906/sunz.2019.4.057
23. Lebedenko, T., Goloveshko, M., Severilov, A. (2019). The results of the experimental study of the Active Queue Management method at the interfaces of telecommunication networks. Problems of Telecommunications, 2 (25), 37–55. doi: https://doi.org/10.30837/pt.2019.2.03
24. Gnatyuk, S., Kinzeryavyy, V., Kyrychenko, K., Yubuzova, K., Aleksander, M., Odarchenko, R. (2019). Secure Hash Function Constructing for Future Communication Systems and Networks. Advances in Intelligent Systems and Computing, 561–569. doi: https://doi.org/10.1007/978-3-030-12082-5_51
25. Brumnik, R., Kovtun, V., Okhrimenko, A., Kavun, S. (2014). Techniques for Performance Improvement of Integer Multiplication in Cryptographic Applications. Mathematical Problems in Engineering, 2014, 1–7. doi: https://doi.org/10.1155/2014/863617
26. Odarchenko, R., Gnatyuk, V., Gnatyuk, S., Abakumova, A. (2018). Security Key Indicators Assessment for Modern Cellular Networks. 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC). doi: https://doi.org/10.1109/saic.2018.8516889
27. Berkman, L., Turovsky, O., Kyrpach, L., Varfolomeeva, O., Dmytrenko, V., Pokotylo, O. (2021). Analyzing the code structures of multidimensional signals for a continuous information transmission channel. Eastern-European Journal of Enterprise Technologies, 5 (9 (113)), 70–81. doi: https://doi.org/10.15587/1729-4061.2021.242357