Scholars Journal of Engineering and Technology (SJET) **ISSN 2321-435X (Online)**
Sch. J. Eng. Tech., 2015; 3(8):707-714 **ISSN 2347-9523 (Print)**
©Scholars Academic and Scientific Publisher
(An International Publisher for Academic and Scientific Resources)
www.saspublisher.com

Research Article

Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters

Snihurov Arkadii[1], Chakrian Vadym[2]
[1]Acting Dean of TCI faculty, Ph.D., Associate Professor; Kharkiv National University of Radio Electronics, Ukraine, Kharkiv, 61166, 14 Lenin ave
[2]Ph.D. student; Kharkiv National University of Radio Electronics, Ukraine, Kharkiv, 61166, 14 Lenin ave

***Corresponding author**
Chakrian Vadym
Email: vadym.chakrian@gmail.com

Abstract: In this paper it's proposed to use the parameter of information security risk in the formula of EIGRP protocol metric calculation to route the traffic by the most secure paths in the network. The method proposes to calculate the risk on the basis of two risk parameters: the risk, which is calculated to the basis of the NIST CVSS standard and the risk calculated on the basis of formula for the degree of node vulnerability from the theory of information systems survivability. It lets to consider and the information security of routed packets and the structural integrity of the network. Also it's proposed the modified algorithm of load balancing between paths that let to offload the most efficient routing node while the network is under the denial of service (DoS) attack.The results of the research shows that the proposed approach can be used to increase the chance of prevention of the information security violation of routed packets and to keep safe the most efficient routing nodes in the network that allow to route the trusted traffic in efficient manner while the network is under DoS attack or lack critical system resources.

Keywords: EIGRP, dynamic routing, route metric, information security risk, NIST CVSS, survivability, network node vulnerability.

INTRODUCTION

One of the up-to-date problems of improvement for routing process in telecommunication systems (TCS) is the development of mechanism for route selection in routers able to take into account the requirements of informational security in order to balance transit traffic [1, 2].

The formula for calculation of EIGRP protocol metric differs from the formula for metric calculation no fits ancestor, IGRP protocol, only in multiplying by constant equal to256. This was done due to several reasons: first of all, to simplify the procedure of transfer from IGRP to EIGRP; second of all, to increase the range of values for metrics of routes, in which parameters to calculate a metric value are slightly different. The formula for the calculation of metric for EIGRP protocol is given below [3].

$$\mathrm{M}_p = \left[\left(K_1 \cdot B_{min}^p + \frac{K_2 \cdot B_{min}^p}{256 - L_{max}^p} + K_3 \cdot \frac{D_{sum}^p}{10}\right) \cdot \frac{K_5}{K_4 + R_{min}^p}\right] \cdot 256, \qquad (1)$$

where B_{min}^p – the smallest value of the weighted score of throughput in the route p; L_{max}^p – the biggest load of one of the communication links in the route p; D_{sum}^p – the total delay in the route [ms]; R_{min}^p – the smallest reliability of one of the communication links in the route p; $p \in P_{i,j}$,$P_{i,j}$ – all possible routes in the given network under information transmission between nodes i, j, if $i \neq j$. Coefficients $K_{1,}K_{2,}K_{3,}K_{4,}K_5$ allow to consider (or not to consider) abovementioned parameters in the metric. In the standard algorithm described by the Cisco company the given coefficients have the following values: $K_1 = K_3 = 1$ and $K_2 = K_4 = K_5 = 0$.

When $K_2 = K_4 = K_5 = 1$, there are cases, where the dynamic change in such parameters as reliability and load of communication links will lead to constant recalculation of the metric (as these values change during traffic transmission) and this will have a negative impact on the central processor of the router. Due to this fact Cisco does not recommend to use them in metric calculation.

The calculation of weighted throughput (1) is performed as follows:

$$B_{min}^{p} = \left\lfloor \frac{10^7}{\min(B_{i,j}^{l,p})} \right\rfloor \left[\frac{Kbit}{s}\right], \qquad (2)$$

where $\min\left(B_{i,j}^{l,p}\right)$ – the smallest throughput of one of the links l in the route p when information is transferred between the nodes i, j.

To calculate the total delay of route the following formula is used:

$$D_{sum}^{p} = \sum_{i \neq j} D_{i,j}^{p} \; (\mu s) \,, \qquad (3)$$

where $\sum_{i \neq j} D_{i,j}^{p}$ – the total of delays of each communication channel in the route p when information is transmitted between the source node i and the receiver node j.

The goal of the research is improvement of the routing algorithm for the EIGRP protocol by introduction of a risk parameter of information security (IS) into the formula of route metrics calculation, and the analysis of performance features of the given routing algorithm. The risk of information security means a potential possibility to damage the information in consequence of the implementation of information security threats on the vulnerability of the network infrastructure.

Introduction of information security risk parameter into formula for calculation of EIGRP protocol metric

In order to consider the risk of information security in the metric of EIGRP protocol the following formula is used:

$$\mathrm{M}_p = \left[\left(K_1 \cdot B_{min}^{p} + \frac{K_2 \cdot B_{min}^{p}}{256 - L_{sum}^{p}} + K_3 \cdot \frac{D_{sum}^{p}}{10}\right) \cdot \frac{K_5}{K_4 + R_{sum}^{p}}\right] \cdot 16^{(2-(1-R_s^P))}, \qquad (4)$$

where R_s^P – the risk of informational security of the route p, $R_s^P \in [0;1]$ that is evaluated on the basis of information security risks of nodes. In this case the degree of constant value is within the limits $[1;2]$, and the constant value itself can vary within the limits $[16;256]$. In fact, the expression $1 - R_s^P$ is a rating of the given route security, i.e. the value, which is opposite to the risk. The increase of the contrast value is exponential under the growth of R_s^P. Such dependability reflects the essence of the risk of information security, as the higher risk parameter value makes the metric less attractive than the lower one.

Approach to evaluation of information security risk for network nodes

The given article proposes to calculate the risk of information security on the basis of the NIST CVSS methodology, as well as on the basis of mathematical approaches of the theory of information systems survivability [4, 5].

It is known that the NIST CVSS standard evaluates the risk on the basis of several global metric groups:

- basic metrics – constant and not changing with time;
- temporal metrics – not constant and changing in time;
- environmental metrics – metrics that allow to destabilize basic and timing metrics and to take into account features of the environment of a vulnerability to be estimated.

Temporal and environmental metrics are calculated separately for each individual case, and they can change the final risk parameter based on the specific situation in the telecommunications network. The formula for calculating the risk of information security of a network device based on the basic metrics (excluding temporal and environmental metrics) is the following:

$$R_{CVSS} = \frac{\sum_{i=1}^{n} B_{score_i}}{n} \cdot \frac{1}{10}\,, \qquad (5)$$

where B_{score} – the score of the basic metric; $\sum_{i=1}^{n} B_{score_i}$ – the total of all basic metrics of all vulnerabilities of the network device; n-the total amount of estimated vulnerabilities of the network device. As $B_{score} \in [0;10]$, then division into 10 is needed to set the necessary limits for information security risk parameter, i.e. $R_{CVSS} \in [0;1]$.

The basic metric score B_{score} is determined from the expression:

$$B_{score} = \lceil((0{,}6 \cdot I) + (0{,}4 \cdot E) - 1{,}5) \cdot f(I)\rceil^{1\text{-}dec}, \qquad (6)$$

where I – the potential damage from informational attacks; E – the possibility of vulnerability to be used by an attacker; $f(I)$ – a function from the damage, calculation of which is given below; $\lceil \quad \rceil^{1\text{-}dec}$ – upward rounding with the accuracy of one tenth.

$$I = 10{,}41 \cdot (1 - (1 - I_c) \cdot (1 - I_i) \cdot (1 - I_a)) \ , \qquad (7)$$

where I_c – the impact on confidentiality of a successfully exploited vulnerability; I_i – the impact on integrity of a successfully exploited vulnerability; I_a – the impact on availability of a successfully exploited vulnerability.

$$E = 20 \cdot A \cdot A_v \cdot A_c \ , \qquad (8)$$

where A – the requirements to authentication; A_v – an access vector; A_c – an access complexity.

$$f(I) = \begin{cases} 0, \text{если } I = 0; \\ 1{,}176, \text{если } I \neq 0. \end{cases} \qquad (9)$$

The basic metric score is calculated on the basis of the standard values proposed by the NIST CVSS methodology and given in the Table1.

The advantage of the approach of information security risk assessment methodology based on NIST CVSS is simplicity. The drawback is that many of the variable metrics are rather difficult, and sometimes even impossible to calculate without an operator. This fact makes the approach to risk assessment inflexible and does not allow to automatically take into account many parameters of modern networks.

To remove this draw back it is proposed to use the mathematical apparatus of the theory of information systems survivability, which allows to take into account many dynamic parameters of modern telecommunication networks, to calculate the risk of information security.

One of the main survivability parameters, which can be used in the risk assessment of information security, is the degree of network vulnerability determined by the following formula:

$$\theta_i = \frac{\varepsilon - \varepsilon_i}{\varepsilon}, \qquad (10)$$

where θ_i – the degree of network vulnerability when removing the node i and all its communication links from the network, $\theta_i \in (0; 1]$; ε – global efficiency of the network; ε_i – global efficiency of the network in case of removing the i-th node and all its communications links.

It is dimmed that the effectiveness of packets transmission between the nodes is inversely proportional to the distance between them. However, the formula of the middle way in the network can be infinite because some networks can be unconnected. To consider such cases we use the global network efficiency parameter, which reflects an average in verse path of routes and is calculated according to the following formula:

$$\varepsilon = \frac{1}{n \cdot (n-1)} \cdot \sum_{i \neq j; i,j \in [1,n]}^{n} \frac{1}{\min_{p \epsilon P_{i,j}} \mu_p} \ , \qquad (11)$$

where $\min_{p \epsilon P_{i,j}} \mu_p$ – the minimal metric of one of the routes p between nodes i, j; when $i \neq j$, the calculation is done between each pair of nodes in the network under study; n – the number of nodes in the given network.

$$\mu_p = \sum_{m \in p} \mu_m, \qquad (12)$$

where $\sum_{m \in p} \mu_m$ – the total of metrics of each communication link m included into the route p; μ_m – calculated according to the formula (1) with the same parameters and values of coefficients needed for the calculation of the standard metric of EIGRP protocol on the given node.

The degree of node vulnerability calculated by the formula (10) shows how much the data transmission efficiency deteriorates in the network in case of removal of the given node$i$and all its links. Accounting vulnerability of a network node during the calculation of risk parameter of the route estimated by the formula (4), allows reducing the load on the node by re-routing traffic through a reserved route, if such a route exists.

Table 1: Parameters of basic metrics of information security

Meaning	Description	Numerical characteristic
Node access vector		
Local access is needed (L)	An intruder needs a direct physical access to the object with the vulnerability.	0,395
Possible access from the adjacent network (A)	An intruder needs an access within one local network (one broadcasting domain) with the vulnerable object.	0,646
Possible access from any network (N)	An intruder can remotely use the vulnerability from any part of the network, including the Internet.	1,0
Requirements to authentication		
Multiple(M)	An intruder has to perform more than one procedure of authentication for exploitation of the node vulnerability.	0,45
Single (S)	To exploit the vulnerability of the node it is enough for an intruder to authenticate himself just one time.	0,56
None (N)	An intruder does not need to go through the procedure of authentication to exploit the vulnerability of the node.	0,704
Complexity of access to node		
High (H)	There are several hard constraints in the access to a node. For instance, exploitation of node vulnerability is possible only in a very short period of time or it needs application of social engineering, under which an intruder can be easily recognized.	0,35
Medium (M)	There are some constraints on the access to a node. For example, the connection to the vulnerable device is possible only from the certain nodes or the vulnerable device should function with unstandardized settings.	0,61
Low (L)	There are no special conditions for the access of node vulnerability. For instance, when the system is available to many users simultaneously or when the vulnerable configuration works on the set of network nodes.	0,71
Confidentiality impact		
None (N)	There is no possibility of information confidentiality disclosure.	0,0
Partial (P)	There is a significant but limited information disclosure.	0,275
Complete (C)	There is full information disclosure.	0,66
Integrity impact		
None (N)	There is no possibility of information integrity violation.	0,0
Partial (P)	There is a possibility of partial modification of data or system files.	0,275
Complete (C)	There is a possibility of modification of any node data.	0,66
Availability impact		
None (N)	There is no possibility of resource availability violation.	0,0
Partial (P)	There is a possibility of performance degradation or denial of service of some node functions.	0,275
Complete (C)	There is a possibility of full node denial of service.	0,66

The calculation of the final risk parameter is proposed to be made by the following formula:

$$R_s^P = 1 - \left(1 - K_{CVSS} \cdot \frac{\sum_{i \in p} R_{CVSS_i}}{n_p}\right) \cdot \left(1 - K_\theta \cdot \left(1 - \frac{\sum_{i \in p} \theta_i}{n_p}\right)\right), \tag{13}$$

where R_s^P – the risk of information security of the overall route p; K_{CVSS} and K_θ – are coefficients of risk parameters importance evaluated by the methodology of the NIST CVSS standard and the theory of information systems survivability, $K_{CVSS} \in [0;1], K_\theta \in [0;1]$ accordingly; $\sum_{i \in p} R_{CVSS_i}$ – the total of risk parameter values of each node of the route p calculated on the basis of the NIST CVSS standard methodology; $\sum_{i \in p} \theta_i$ – the total of vulnerability degrees of each node in the route p calculated on the basis of the node vulnerability formula from the theory of informational systems survivability; n_p – the total number of nodes within the route p.

The coefficients of importance K_{CVSS} and K_θ allow to vary the effect of appropriate indicators, on the basis of which the calculation of the final risk is made. It should be noted that for the accuracy of the presented method, these factors should be the same on all nodes of the network under study.

Management of information security risk parameter using coefficient of importance

As the degree θ_i takes in account degradation of data transmission due to the outage of one of the network nodes, it has prevailing meaning in those cases when it is needed to take measures for node protection against attacks such as Denial of Service and in other situations under which performance on the node decreases.

In its turn the indicator R_{CVSS} considers the levels of vulnerabilities which can be used to violate different categories: confidentiality, availability and integrity of information. In the general case the given indicator shows how much a certain node is exposed to the attack.

If we assume that the coefficients of importance are binary variables and the conditions $K_{CVSS} \in \{0;1\}$, $K_\theta \in \{0;1\}$ are fulfilled, then there are four combinations under which the parameters are activated or deactivated and on the basis of which the final information security risk parameter is calculated. In this paper we propose to use the combinations of data in the following cases:

- $K_{CVSS} = 0, K_\theta = 0$ – in case when the indicator of information security risk is not used. This variant of coefficients is normally activated. An administrator can change it to one of the following variants;
- $K_{CVSS} = 1, K_\theta = 0$ – in case when the maximal priority is given to provide confidentiality, integrity and availability of transit traffic;
- $K_{CVSS} = 0, K_\theta = 1$ – in case when the maximal priority is given to provide protection of network structural integrity;
- $K_{CVSS} = 1, K_\theta = 1$ – considers parameters of confidentiality, integrity and availability of traffic as well as protection of network structural integrity.

The case with the choice of $K_{CVSS} = K_\theta = 1$ coefficients is not recommended to be used. In the case where R_{CVSS} has a significant impact on the overall risk assessment, this can minimize the attempts to protect the most productive unit (or the most important unit from a structural point of view) from attacks such as Denial of Service. In the opposite case, when the degree θ_i has dominant influence on assessment of the overall risk, this can lead to traffic passing through the vulnerable node, exposing transit traffic to the significant risk of breach of confidentiality and integrity.

In order to manage risk more effectively and dynamically we can assume the controlling factor, which will automatically choose which of the indicators should be taken into account in the calculations.

It should be noted that the degree θ_i allows discovering the nodes which are the most productive for the given network. This became possible due to the fact that in the formula for calculation of the network global effectiveness (11) in the standard theory of information systems survivability the score μ_p represents the distance between the nodes $i, j$and it is measured in the numbers of hops between them. The given article proposes to use the metric calculated on the basis of formula (1) as μ_p. The given approach allows taking into account not only the distance to the remote node but also such important network characteristics as a delay and links throughput as well as others that can be considered as metrics of EIGRP protocol.

There is a problem which lies in the fact that in the case when we take into account only the degree of θ_i to calculate the final risk of the route, the traffic will be transmitted by the path with the most effective network nodes. However, this decision just worsens the condition in case of realization of the attack such as Denial of Service on the network elements. This is easy to demonstrate – the formula of the final risk parameter for the route p under $K_{CVSS} = 0$ and $K_{\theta} = 1$ takes the following form:

$$R_s^P = 2 - \theta_i.$$

It follows from the formula given above that with the increase of the degree θ_i the route metrics $M_p$decreases, what makes it more attractive.

To solve this problem the following approach is proposed. Under a single-path routing when there is only one route to the remote network – the information security risk parameter is irrelevant as the path has no alternative. In the case when there are several paths into the network, the process of solving of the multi-path routing problem – the mechanism of forced load balancing consists of two rules:

- more prioritized and confidential traffic is passed though the most effective path;
- less prioritized and non-confidential traffic is passed through the path, nodes in which will do the minimum damage to effectiveness of the network in case of attacks such as Denial of Service.

Traffic priority can be determined using the ToS («Type of Service») field in the header of the packet of the IPv4 protocol or TC («Traffic Class») field in the packet header of the IPv6 protocol. Moreover, on the basis of access lists it is possible to determine both priority of traffic, and also if this traffic can be trusted. Despite the proposed methods of determining priority and confidentiality of traffic this issue is subject to more detailed investigation.

To implement the given solution it is possible to store several metrics of EIGRP protocol routes for the same networks which, however, consider different coefficients K_{CVSS} and K_{θ}. This approach can demand enormous consumption of the RAM («random access memory»), what can be unacceptable in large networks. Currently the problem of lack of the RAM remains unsolved.

The example of impact of information security risk of nodes on routes selection by EIGRP protocol

The given chapter presents the example of calculation for metrics of EIGRP protocol taking into consideration the risk parameter. Also we conduct the analysis of the impact of the given indicator on selection of routes by EIGRP protocol under the single-path routing and on the redistribution of packets under the unequal cost load balancing.

The network topology under study and the metrics of each of communication links, calculated by the formula (1), are shown in the Fig. 1.

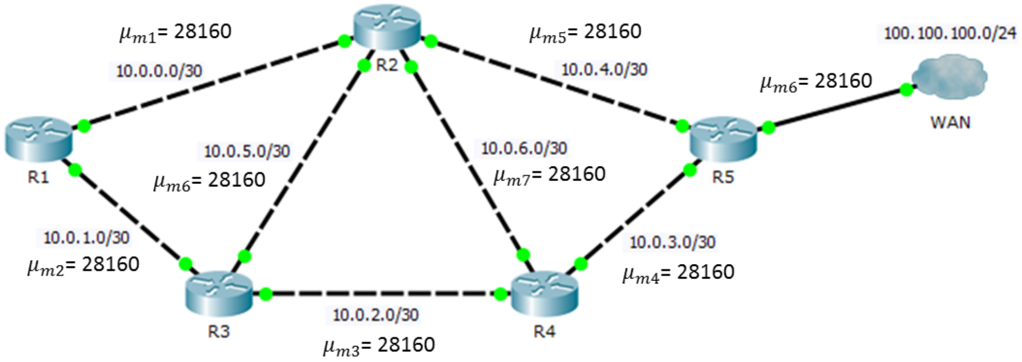

Fig.1: The topology of the network studied in the given article with the metrics of each communication links

Traffic is transmitted from the router R1 into the network 100.100.100.0/24. The communication link between R5 and the WAN cloud is the standard Fast Ethernet with the appropriate parameters of the interface on both sides. Bandwidth of all the links in the studied topology are equal to 100 [Mb/s].
Four routes will be studied in the given example:

- the shortest two routes from R1 to WAN: $p1 \in [R1; R2; R5; WAN]$, $p2 \in [R1; R3; R4;\ R5; WAN]$,
- two routes: $p3 \in [R2; R5; WAN]$ and $p4 \in [R3; R4; R5; WAN]$,

The metrics of which will be necessary to take a decision on the ability of $p1$ or $p2$ to become backup path. The selection of a backup route is made on the basis of the «feasibility condition» [6]. The given condition means that if route

$p1$ is selected by the router R1 as the main one, then the route $p2$ can be the backup oneif the metric of the route $p4$ is smaller, than the metric of the route $p1$. The same rule works for the route $p2$, if it was selected as the main one, then the route $p1$ could be the backup one only in the case when the metric of the route $p3$ would be smaller than the metric of the route $p2$.

In order to find the θ_i we study the graph built of vertexes represented by nodes R1, R2, R3, R4, R5, WAN, and their edges represented by communication links between routers. The solution for the problem of the shortest path selection is formalized as a problem of Boolean programming which is possible to be solved using «bintprog» function in the «Optimization Toolbox» of the MATLAB.

If we consider that the block diagram and network parameters are set in accordance with the topology in the Fig. 1, then simulation of the situation will show the following results of calculation of the θ_i:

$$\theta_{R1} = 0{,}9579;\ \theta_{R2} = 0{,}9655;\ \theta_{R3} = 0{,}9606;\ \theta_{R4} = 0{,}9615;\ \theta_{R5} = 0{,}9704;\ \theta_{WAN} = 0{,}9543.$$

Let us choose the following indicators of $R_{CVSS_i}$for each of the routes:

$$R_{CVSS_{R1}} = 0{,}3;\ R_{CVSS_{R2}} = 0{,}7;\ R_{CVSS_{R3}} = 0{,}4;\ R_{CVSS_{R4}} = 0{,}4;\ R_{CVSS_{R5}} = 0{,}2.$$

On the basis of R_{CVSS_i} and θ_i parameters we will calculate the total risk of information security for each of the possible routes taking into account different cases of enabling the coefficients of importance K_{CVSS} and K_θ, and show the results in the Table 2. It should be noted that as the WAN node is considered to be external for the given network, then the $CVSS_{WAN}$ parameter value cannot be calculated for it, and its θ_{WAN} parameterwill not be considered in the following risk calculations.

Table 2: The results of IS risk calculation for each of the routes with consideration of enabling different coefficients of importance

	$K_{CVSS} = 0$ and $K_\theta = 0$	$K_{CVSS} = 1$ and $K_\theta = 0$	$K_{CVSS} = 0$ and $K_\theta = 1$	$K_{CVSS} = 1$ and $K_\theta = 1$
R_s^{p1}	0	0,4	0,0354	0,42124
R_s^{p2}	0	0,325	0,0374	0,350245
R_s^{p3}	0	0,45	0,03205	0,467628
R_s^{p4}	0	0,333333	0,035833	0,357222

According to the Table 2 let us calculate the metrics of each of the routes by the formula (4). The results of the calculation are given in the Table 3.

Table3: The results of the calculation of EIGRP protocol metrics using the information security risk parameter

	$K_{CVSS} = 0$ and $K_\theta = 0$	$K_{CVSS} = 1$ and $K_\theta = 0$	$K_{CVSS} = 0$ and $K_\theta = 1$	$K_{CVSS} = 1$ and $K_\theta = 1$
M_{p1}	2080	6305	2295	6688
M_{p2}	2240	5516	2485	5915
M_{p3}	1920	6686	2098	7021
M_{p4}	2080	5241	2297	5600

As we can see from the Table 3 when $K_{CVSS} = 0$ and $K_\theta = 0$, the route $p1$ will be chosen as the main one, however, it will not have any backup route because the condition $\mathrm{M}_{p4} < \mathrm{M}_{p1}$ is not fulfilled. The same situation can be seen when $K_{CVSS} = 0$ and $K_\theta = 1$, however, in this case the mechanism of forced balancing of traffic is enabled, meanwhile confidential and prioritized traffic will be passing through the path $p1$ and all the remained traffic will pass through the path $p2$.

At the same time, when $K_{CVSS} = 1$ and $K_\theta = 0$ the situation is reversed – the main route is $p2$, which does not have any backup route, because the condition $\mathrm{M}_{p3} < \mathrm{M}_{p2}$ is not fulfilled. The similar situation can be also observed when $K_{CVSS} = 1$ and $K_\theta = 1$. In such situations the indicator R_{CVSS_i} has significantly worsened the metrics of the effective route and the choice preference was given to provision of security for transit traffic. In these cases forced balancing of traffic is not enabled.

CONCLUSION

The article proposes the approach to the calculation of metric for EIGRP protocol, which takes into account the information security risks of transit traffic. The method proposes to calculate the risk on the basis of two risk parameters: the risk, which is calculated to the basis of the NIST CVSS standard and the risk calculated on the basis of formula for the degree of node vulnerability from the theory of information systems survivability. The first parameter allows to consider risks of data confidentiality and integrity; the second parameter, allows to evaluate risks of unavailability for transit traffic and risks of structural integrity of the network.

Outstanding issues in this article are: prioritization and evaluation of traffic credibility, as well as mechanisms to assess the state of the network that allow to dynamically consider parameters, on the basis of which the calculation of the route information security risk is made. These issues will form the basis for further scientific work of the authors.

REFERENCES

1. Snigurov AV, Chakryan VK; Approach of routing metrics formation based on information security risk. 12th International Conference on the Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), Lviv, 2013; 339-340.
2. Snigurov AV, Chakryan VK; Approach of calculation of network devices security rating. Information processing systems, 2014; Publ. 1(117): 150-155.
3. Enhanced Interior Gateway Routing Protocol. Available from http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html
4. Mell P, Kent KA, Romanosky S; The common vulnerability scoring system (CVSS) and its applicability to federal agency systems. US Department of Commerce, National Institute of Standards and Technology, 2007.
5. Dodonov AH, Lande DV; Zhivuchest informatsionnikh system [Survivability of information systems]. K.: Nauk.dumka, 2011; 256 pp.
6. Enhanced Interior Gateway Routing Protocol draft-savage-eigrp-04. RFC Internet-Draft. Available from https://tools.ietf.org/html/draft-savage-eigrp-04