IJCTA, 9(30), 2016, pp. 95-104
© International Science Press

Formalization of the Description of Spam Attacks with Malicious Attachments of the Networks Structures

Evgeny Aleksandrovich Popov* and Konstantin Aleksandrovich Razinkin, Vladislav Georgievich Yurasov, Yury Konstantinovich Yazov, Nikolay Mikhailovich Tikhomirov**

Abstract : For the first time, there is proposed in the paper a formalization of the processes of realization and consequences of mailout of destructive messages on the basis of evaluating the dynamics of changes of the resources of the network nodes and edges. The resource of the node is represented as a difference of resources (positive and negative). In turn, each of the resources is the product of the value and the amount of information. At the same time, to determine the value of negative information, the expression is used for the damage from the realization of spam attacks with malicious attachments, whereas to determine the amount, the mode of the number of attacks is used, expressed by an irregular lognormal distribution, and the probabilities of actuation of the antivirus and anti-spam protection. In addition, the paper proposes a method for evaluating user activities in the realization of this type of attack. Numerical methods are used for testing the resulting model.

Keywords : Spam, network resource, the value and amount of information, damage.

1. INTRODUCTION

Today, spam can no longer be regarded as an innocent phenomenon. The mailout of the “garbage” network messages brings about quite significant damage, is performed deliberately, and this is obviously fostered by the network character of modern technologies. It may be noted that, to distribute mailouts, an ill-minded person needs Internet access and minimal knowledge in programming. Such little requirements also attract people who want to earn extra money. However, more experienced organizations approach this work much more seriously. Not only highly skilled programmers, but also experts in the field of linguistics, psychology and other sciences are involved in the realization of an attack of the “spam-mailout” type [3,4,12].

A spam message is a content, which reduces the resource of the network and its nodes. It has negative and/or low value and a relatively large amount of information. While the amount of information is an objective category, the value is subjective for a node of the network and conditioned by its functional purpose and its goals and objectives. Hence, making decision requires information of a certain resource. The increase in volume and decrease in the value of the content taken into account when making a decision reduces the adequacy of this decision at the node of the network. This negative phenomenon is fostered by spam. Therefore, the quality of filtering of the information entering the node and deleting spam directly affects the efficiency of functioning of an individual network node and, taking into account the weights of the nodes, of the entire network.

2 METHODICAL DESCRIPTION OF THE DISTRIBUTION OF SPAM ATTACKS

A model of spam distribution over a network is presented in Figure 1.

* 14 Moskovsky prospect, Voronezh, 394026, Russian Federation

** 14 Moskovsky prospect, Voronezh, 394026, Russian Federation

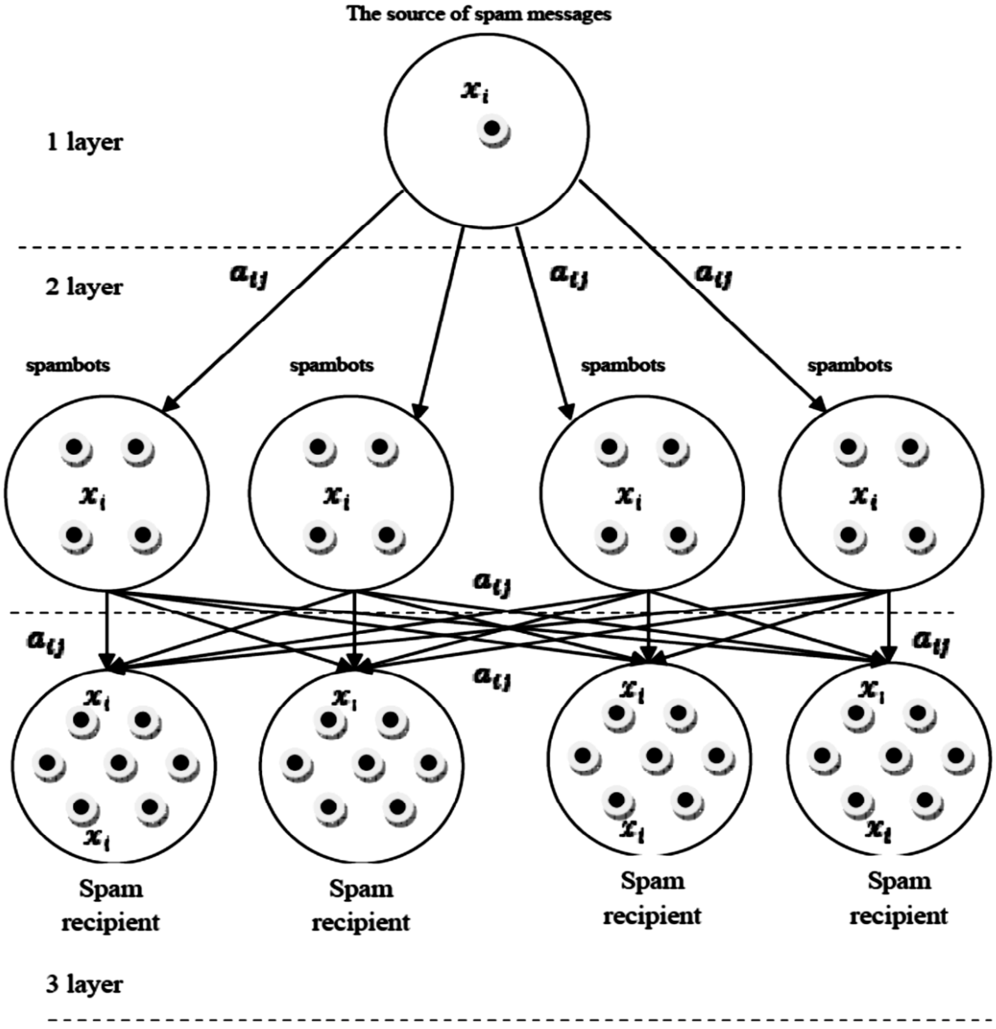

Fig. 1. Dissemination of spam over a network.

As a result, in an enlarged form, the network will consist of three layers.

Let us consider each of the layers in more detail :

The first layer. At the vertices of this layer, there are the nodes performing the following tasks:

- preparation of spam-messages for sending;
- sending spam-messages to spambots for mailing out the information;
- infecting computers with the purpose of turning them into spambots.

The second layer. The vertices of this level are the transport nodes, with the help of which negative information is distributed over the network to a spam victim. This layer consists of a set of vertices, because the spreading process is intricate and complex.

The third layer. The vertices of this level are the victims of malefactors. These nodes are of most interest as an object for the analysis of destructive impact of spam attacks, because they, on one hand, take the damage and, on the other hand, can be organizationally and technically protected against this type of attacks.

Formally, a description of the process of destructive impact of spam is possible on the basis of the concepts of resource of the vertex Res(x_i) and the arc Res (a_{ij}) of the network:

$$\mathrm{Res}(x_i) = \mathrm{C}(x_i)\mathrm{V}(x_i) - \mathrm{C}_S(x_i)\mathrm{V}_s(x_i); \tag{1}$$

$$\mathrm{Res}(a_{ij}) = \mathrm{C}(a_{ij})\frac{\partial \mathrm{V}(a_{ij})}{\partial t} - \mathrm{C}_S(x_i)\frac{\partial \mathrm{V}_s(a_{ij})}{\partial t}; \tag{2}$$

where $C(x_i)$ and $V(x_i)$ are, correspondingly, the value of the unit volume and the volume of useful information at the vertex x_i of the network;

$C_S(x_i)$ and $V_S(x_i)$ are, respectively, the (negative) value of the unit amount and the amount of spam-information at the vertex x_i of the network;

$C(a_{ij})$ and $V(a_{ij})$ are, respectively, the value of the unit volume and the volume of useful information, pumped through the arc a_{ij} of the network;

$C_S(a_{ij})$ and $V_S(a_{ij})$ are, respectively, the (negative) value of the unit volume and the volume of spam information, pumped through the arc of the network.

The expressions (1) and (2) clearly demonstrate a destructive function of spam. It reduces the resource of the vertices (1) and the throughput capacity of the arcs (2) of the network. The main influencing factor is the damage that may be inflicted on a network node as a result of exposure to malicious software, “phishing” or some fraudulent operations [6,7].

In addition, the network is deliberately filled by the “garbage” filler, which may cause a threat to its effective functioning. [7] However, given the increasing network performance, the use of spam messages as a tool for the implementation of a DDoS-attack is unlikely. [10] In this regard, let us pay the main attention to considering the resource of the node vertices.

The expression for the resource of a vertex can also be represented as the difference of resources, namely:

$$\mathrm{Res}(x_i) \; = \; \mathrm{Res}_{+}(x_i) - \mathrm{Res}_{-}(x_i); \tag{3}$$

where $\mathrm{Res}(x_i)$ is the positive resource at the vertex x_i of the network;

$\mathrm{Res}\_(x_i)$ is the negative resource at the vertex of the network.

When considering real systems, it can be assumed that is a constant. The reason for this is that keeping track of the dynamics and value of useful information coming to the vertex of the network is an intractable problem, which depends on many factors, including those that cannot be subjected to mathematical evaluation.

Let us consider in more detail the negative resource of the network. To estimate the negative part of the resource more accurately, it is necessary to present the expression as the sum of products of the value of information and the flow of information for each type of spam, namely, “phishing”, spam attacks with malicious attachments, fraudulent spam and the advertising spam messages.

As a result, the expression for the negative resource of the network vertex will be as follows:

$$\mathrm{Res}_{-}(x_i) \; = \; \mathrm{C}_{S_f}(x_i)\mathrm{V}_{S_f}(x_i) + \mathrm{C}_{S_v}(x_i)\mathrm{V}_{S_v}(x_i) + \\ + \mathrm{C}_{S_m}(x_i)\mathrm{V}_{S_m}(x_i) + \mathrm{C}_{S_r}(x_i)\mathrm{V}_{S_r}(x_i);$$

where

C_{S_f} is the value of a spam message of the “phishing” type,
V_{S_f} is the volume of a spam message of the “phishing” type,
C_{S_v} is the value of a spam message with malicious attachments,
C_{S_v} is the volume of a spam message with malicious attachments,
C_{S_m} is the value of a spam message of fraudulent type,
V_{S_m} is the volume of a spam message of fraudulent type,
C_{S_r} is the value of a spam message of the advertisement type,
C_{S_r} is the volume of a spam message of the advertisement type.

In this work, we will consider spam attacks with malicious attachments, so the expression for the negative resource in this case will have the form:

$$\mathrm{Res}_{-}(x_i) \; = \; \mathrm{C}_{S_v}(x_i)\mathrm{V}_{S_v}(x_i) + \mathrm{Res}_{-\mathrm{o}}(x_i); \tag{5}$$

$\mathrm{Res}_{-\mathrm{o}}(x_i)$ is the negative resource of other types of spam; in this paper we take this quantity as constant.

Thus, the resource quantity depends on two parameters: the value and the volume of information. Let us consider each of these components separately.

The value of information. In this case, the value is negative and depends primarily on the type of spam. The spam having exclusively advertising purposes will have the minimal negative value, whereas the spam that is intended to causing damage [13] to victim or gaining the own benefit has the greatest negative value.

Regarding the mathematical evaluation, we assume that the value of information can be interpreted as the damage inflicted as a result of successful implementation of a spam attack with malicious attachments on the network node. [11] The damage is considered in the works on spam attacks with malicious attachments under an irregular distribution of the damage [3,5] and is described by the expression:

$$u_i(n) = u_{i\,\min} + u_{ir}(n),\ u_{ir}(n) = (n - n_{i\,\min})$$
$$\times (t_{io}c_i + \exp(-\lambda_{iu} \cdot (t_{iu} - t_{ir})) - \exp(-\lambda_{iz} t_{ir})).$$

where

u_i is the damage from the spam attacks,

$u_{i\min}$ is the minimal damage from the spam attacks,

$n_{i\min}$ is the minimal number of the spam attacks,

$t_{i\min}$ is the minimal time, spent by the user to process the spam message,

c_i is the value of the unit of time (*c.u.*),

λ_{iz} is the infection intensity by the malicious software,

λ_{iu} is the intensity of treatment from the malicious software,

t_{ir} is the time period of the system's reaction to the introduction of the malicious software,

t_{iu} is the time moment of the treatment of the system from the malicious software,

t_{io} is the time, spent for the user's processing of the spam message.

Thus, the value of a spam message with malicious attachment will be determined by the following expression:

$$\mathrm{C}_{S_v}(x_i) = t_{io}c_i + \exp(-\lambda_{iu} \cdot (t_{iu} - t_{ir})) - \exp(-\lambda_{iz} t_{ir})$$

The amount of negative information can be considered as the number of spam attacks successfully implemented during a certain period of time. The number of attacks is a random variable. In [3] it was proved that the number of spam attacks with malicious attachments has a lognormal distribution. However, an analysis of statistics has showed that in the considered period of time one can distinguish a certain constant component of the number of attacks, determining its minimum value.

As a result, we find that the random variable of the number of attacks is summed up from two components: a constant quantity $n_{\min}$ and the random component n_{irand} itself:

$$n = n_{\min} + n_{irand}$$

As a result, we obtain for the distribution law:

$$\varphi_\xi(n_i \mid n_{i\min}) = \frac{1}{(n_i - n_{i\min})\sigma_i\sqrt{2\pi}} e^{-\frac{(\ln(n_i - n_{i\min}) - m_i)^2}{2\sigma_i^2}},$$

where

n_i is the random variable of the number of spam attacks,

$n_{i\min}$ is the minimal number of spam attacks,

m_i, σ_i are the parameters of distribution.

To determine the volume of spam messages, we use an expression for the most probable value:

$$\sigma_i^2 - m_i + \ln(n_i^* - n_{i\min}) = 0 \qquad (6)$$

To determine n_i^*, we need to use numerical methods. In the case $n_{i\,\min} = 0$, the mode of the number of attacks is equal to:

$$n_i^* = e^{m_i - \sigma_i^2}. \tag{7}$$

Using expressions (6) and (7), one can obtain the value of the number of spam messages containing malicious attachments, coming to the network node. However, this quantity is a characteristic of all attacks targeting the system. To find the number of successfully realized attacks, it is necessary to take into account the elements of the protection system of the considered node.

In [4], there are considered the applied protection systems against spam attacks with malicious attachments, as well as the criteria for evaluating their effectiveness, which are expressed in the probability of realization of attack, namely:

p_{iantis} is the probability of blocking by the filter of the spam message;

$p(l_i)$ is the probability of wrong actions by the user of the level l [9]:

$$p(l_i, \lambda_{Ueduc}) = \begin{cases} 1 - \lambda_{ion} \cdot l_i, & 0 \le l_i \le l_{in}; \\ \exp(-\lambda_{ioo}(l_i - l_{in})) - \lambda_{ion} \cdot l_i, & l_{in} \le l_i \le l_{io}; \\ \exp(-\lambda_{ioo}(l_{io} - l_{in})) - \lambda_{iop} \cdot l_i, & l_{in} \le l_i \le 1. \end{cases} \tag{8}$$

where

l_i is the user's level,

l_{in} is the level boundary of the illiterate user,

l_{io} is the level boundary of the trained user,

λ_{ion} is the intensity of training the illiterate user,

λ_{ioo} is the intensity of training the trained user,

λ_{iop} is the intensity of training the advanced user.

p_{iantiv} is the likelihood of actuation of the anti-virus system.

Thus, the static resource of the network vertex node is determined by the following expression:

$$\begin{aligned} \mathrm{Res}_{-}(x_i) &= \mathrm{C}_{S_v}(x_i)\mathrm{V}_{S_v}(x_i) + \mathrm{Res}_{-o}(x_i) \\ &= (t_{io}c_i + \exp(-\lambda_{iu} \cdot (t_{iu} - t_{ir})) - \exp(-\lambda_{iz}t_{ir}))) \times\ n_i^* \cdot (1 - p_{antis}) \cdot (1 - p_{antiv}) \cdot p(l_i) + \mathrm{Res}_{-\mathrm{o}}(x_i). \end{aligned} \tag{9}$$

For a formal description of the resource of the entire layer, it is necessary to sum up the resources of all nodes of the network:

$$\mathrm{Res}_{lay} = \sum_{i=0}^{n} \mathrm{Res}_{+}(x_i) - \mathrm{Res}_{-}(x_i) = \sum_{i=0}^{n} \mathrm{Res}_{+}(x_i)$$

As a result, we obtain an estimate for the layer resource and the resource of the individual network nodes. This representation allows making an adequate assessment of the state of the node, as well as performing resource management using the settings of the protection system.

The main objective is to increase the overall resource of the node. From (3) it follows that, to increase it, it is necessary to reduce the negative resource. Let us analyze the expression in terms of the values of the varying quantities:

t_{io} is the time, spent by the user for the processing of one spam message. This value can be changed with the help of organizational measures; in particular, informing the users on the most characteristic features of a spam message, in order to diminish the time of analysis of its content;

c_i is the value of a unit of time. This quantity is determined for each node individually and cannot be subjected to regulation;

n_i^* is the most probable number of attacks directed at a node of the network. This value is determined by statistical methods, so to record a change of this parameter, it is necessary to carry out a long-term experiment;

p_{iantiv} is the probability of triggering the anti-virus protection system. The value is determined by statistically independent experts; it depends on the particular protection used by the network node. Changing the protection system entails a change of this quantity. As a protection from malicious software, this is one of the basic technical measures;

p_{iantis} is the probability of triggering an anti-spam filter. This quantity is estimated similar to the anti-virus protection systems;

t_{ir} , λ_{iu} , t_{iu} are the quantities, characterizing the process of treatment of the node from the destructive influence of malicious software. It depends on the used protection system, therefore it can be influenced;

l_{iz} is the intensity of infection. This value is a characteristic of the attacking side, thus it can be taken as a constant quantity.

Thus, the resulting expression allows evaluating the current network resource, as well as its dynamics by tracking the changes in the quantities that characterize the protection system.

The results of numerical simulation of spam attacks with malicious attachments

The resource management consists in the application of organizational and technical measures of protection. Let us consider the impact and methods of each of these measures.

To evaluate the applied methods of protection, we use the above model together with numerical simulation, that is, we determine the numeric value of the negative resource of the network vertices.

Consider a network consisting of 100 nodes of the third layer. Let us make the following assumptions:

1. the volume of spam messages coming to each node is the same for all nodes in the network;

Table 1. Parameters and values of the nodes of the considered system.

Parameter	***Value***
m_i	-2.02
σ_i	0.601
c($c.u.$/hour)	2000
l_{ir}(hour)	0.0004
l_{iz}(1/ hour)	2
t_{io}(hour)	0.0028
λ_{iu}(1/ hour)	4
t_m(hour)	0.0008
l	0.2
ln	0.3
l_o	0.6
l_p	0.9
λ_{ion}	0.5
λ_{ioo}	2
λ_{iop}	0.3
p_{iantis}	0.98
p_{iantiv}	0.91

2. the nodes are equipped with the same means of protection against spam and malware;
3. the level of all network users is the same.

Let us calculate the value of the negative potential of the entire system, using the expression (9) and the values of the system parameters (Table 1).

Then we conclude that for an individual element :

$$\begin{aligned}\mathrm{Res}\_(x_i) &= \mathrm{C}_{\mathrm{S}_v}(x_i)\mathrm{V}_{\mathrm{S}_v}(x_i)+\mathrm{Res}_{-\mathrm{o}}(x_i)\\ &= (5,6+\exp(-4\cdot(0,0004))-\exp(-2\cdot 0,0004)))\cdot\\ &\qquad \exp(-2,02-0,601^2)\cdot 0,09\cdot 0,02\cdot(1-0,5\cdot 0,2)\\ &\qquad + \mathrm{Res}_{-\mathrm{o}}(x_i)=8,412\cdot 10^{-4}+\mathrm{Res}_{-\mathrm{o}}(x_i).\end{aligned}$$

As a result, the value for the entire system will be equal to:

$$\mathrm{Res}_{\mathrm{lay}} = \sum_{i=0}^{100}\mathrm{Res}\_(x_i)=0,08412+100\cdot\mathrm{Res}_{-o}(x_i).$$

Suppose that this value is inadmissible. In order to change it, it is necessary to apply certain protective measures: organizational and technical ones.

The technical protection measures include modernization and adjustment of protection systems against malicious software and spam. [8] To use the protection systems effectively, we need to determine an optimal set of instruments with respect to different criteria. As a means of the instrument selection, we can use the fall-down vector method with the construction of the Pareto set of optimal solutions. As an objective function, we use the following expression:

$$\mathrm{F}(x_1,...,x_n)=k_{risk}\cdot risk(x_1,...,x_n)+k_{\cos t}\cdot\cos t(x_1,...,x_n),$$

where $\mathrm{F}(x_1,...,x_n)$ is the objective function;

x_1, ..., x_n is a vector, indicating the presence or absence in the set of a protection means {0,1};

k_{risk} is the risk priority in calculating the objective function;

$risk(x_1,...,x_n)$ is the risk value, expressed as monetary losses due to realizations of the threats of the spam type and malicious attachments,

k_{cost} is the cost coefficient in using a set of protection means,

$\cos t(x_1,...,x_n)$ is the value of costs due to the applied protection means.

The risk value is determined in accordance with the following expression:

$$risk(x_1,...,x_n) = \sum_{j=1}^{2}\sum_{i=1}^{n}x_i\cdot(1-p_{ij}^{opp})\cdot p_j^{imp}\cdot u_j,$$

where p_{ij}^{opp} is the probability of neutralization of *j*th attack by *i-th* protection means,

p_j^{imp} is the probability of realization of *j-th* attack,

u_j is the damage from *j-th* attack.

As the attacks, we consider the spam attacks themselves and an attack through the implanted malicious software. For the calculation convenience, the probabilities of realization of these threats will be taken to be one.

Correspondingly, the value of costs can be found from the following expression:

$$\cos t(x_1,...,x_n) = \sum_{i=1}^{n}x_i\cdot c_i,$$

where c_i is the cost of the protection means.

Besides, in solving this optimization problem of decision making, we adopt the following restrictions:

$$\begin{cases} risk(x_1,...x_n) < risk_{\max} \\ \cos t(x_1,...x_n) < \cos t_{\max} \end{cases},$$

where : $risk_{\max}$ is the maximum admissible risk in the system,

$\cos t_{\max}$ is the maximum expenses on the means of information protection.

As the initial data for solving this optimization problem of decision making, we use the information on the percentage of blocking the corresponding attacks for each of the means of protection, as well as information provided by the manufacturers of these information protection means on the cost of 50 annual licenses [1,2]. All data are presented in a table (Table 2).

Table 2. Parameters and values of the protection systems.

Title	***Cost***	***P_{antiv}***	***P_{antis}***
Kaspersky	45000	0.92	0.99
MacAfee	73830	0.98	0.99
Norton	74500	0.96	0.98
Avast	249750	0.91	0.99
Avira	49675	0.96	0.99
Comodo	305700	0.9	0.98
Eset NOD32	23600	0.95	0.99

Applying the algorithm described above, we see that the solution, provided by the ESET company, can be most effectively used as a defense system. The peculiarity of this system is that it provides comprehensive protection from both spam and malware attachments in the case of wrong actions of users. Based on statistical data, this instrument will provide virus protection at the level of 95.2% and spam protection at the level of 99.27%.

Then we get that for an individual node :

$$\begin{aligned} \mathrm{Res}_{-}(x_i) &= \mathrm{C}_{S_v}(x_i)\mathrm{V}_{S_v}(x_i) + \mathrm{Res}_{-o}(x_i) \\ &= (5,6 + \exp(-4\cdot(0,0004)) - \exp(-2\cdot 0,0004)))\cdot\exp(-2,02 - 0,601^2)\cdot 0,05\cdot 0,01\cdot(1-0,5\cdot 0,2) + \\ &\qquad + \mathrm{Res}_{-o}(x_i) = 2,337\cdot 10^{-4} + \mathrm{Res}_{-o}(x_i). \end{aligned}$$

As a result, the value for the entire system will be equal to:

$$\mathrm{Res}_{\mathrm{lay}} = \sum_{i=0}^{100} \mathrm{Res}_{-}(x_i) = 0,02337 + 100\cdot\mathrm{Res}_{-o}(x_i).$$

In this case, the organizational measures of protection include the solutions aimed at the users of the system, to increase literacy in the field of spam. In fact, a feature of spam attacks is that the most important role in their success is played by the human factor. The reason for this is that the attackers develop new methods of breaking the protection systems. In turn, the manufacturers of protection systems often do not release updates of their systems promptly. As a result, realization of the attack will depend ultimately on the users. For their training, it suffices to carry out regular instruction to provide them with relevant information about trends in the development and improvement of the methods used by malefactors.

To quantitatively evaluate the user knowledge and skills, we can use the expression (9). To simulate the system, it is only necessary to determine the user levels and the boundaries of levels by statistical methods. Suppose that as a result of applied organizational measures aimed at training of users, the level of users has increased to 0.4. We calculate the probability of wrong actions of users:

$$\begin{aligned} p(l) &= \exp(-2\cdot(0.4-0.3)) - 0.5\cdot 0.3 = 0.669, \\ \mathrm{Res}_{-}(x_i) &= \mathrm{C}_{S_v}(x_i)\mathrm{V}_{S_v}(x_i) + \mathrm{Res}_{-o}(x_i) \end{aligned}$$

$$= (5.6 + \exp(-4 \cdot (0.0004)) - \exp(-2 \cdot 0.0004))) \cdot \exp(-2.02 - 0.601^2) \cdot 0.05 \cdot 0.01 \cdot 0.669$$

$$+ \mathrm{Res}_{-o}(x_i) = 1.737 \cdot 10^{-4} + \mathrm{Res}_{-o}(x_i).$$

$$\mathrm{Res}_{lay} = \sum_{i=0}^{100} \mathrm{Res}_{-}(x_i) = 0.01737 + 100 \cdot \mathrm{Res}_{-o}(x_i).$$

Thus, as a result of the taken protection measures, the negative resource of the network nodes and of the entire system has decreased. In the case, when this value is still unacceptable, it is necessary to carry out additional instruction or choose a more secure set of technical protection.

4. DISCUSSION OF THE SIMULATION OF SPAM ATTACKS WITH MALICIOUS ATTACHMENTS

The methods proposed in the paper adequately describe the process of spam attacks with malicious attachments from the point of view of the object. The model takes into account the main influencing factors, which have a destructive effect on the network node. Also we take into consideration the applied protection system. Particular attention is paid to the user, which in this case is one of the most important elements of the process. His/her actions, in particular, determine the success of attack implementation. To estimate the actions of users, a method is proposed allowing considering the system in terms of user groups, which simplifies the modeling process.

Additionally, into the model there can be introduced an additional source of damage caused by spam attacks, expressed in material expenses resulting from the malefactor’s traffic. However, due to a tendency to increase the throughput of computer networks, this parameter is not so significant.

The numerical simulation described above demonstrates the applicability in practice of the developed mathematical model. In addition, knowing the value of the resources of the network elements, one can identify the vulnerable components and apply additional protection measures to them.

The methods of protection, presented in the paper, cover both the technical side of the process and the organizational one. The resulting model reflects their impact on the resource value that allows evaluating the effectiveness of the possible application in terms of costs and the change of the protection level.

9. CONCLUSION

The model proposed above is of interest for considering the network node as an object of spam attacks with malicious attachments. The expressions for the network resource can be used for numerical simulation of real systems and evaluation of the results of application of various methods of protection, both organizational and technical ones. The organizational protection methods will be primarily aimed at reducing the likelihood of wrong actions of users through carrying out instructions and other kinds of informing. The technical methods of protection are reflected in the probabilities of triggering the anti-spam and anti-virus systems.

The further development of the work is seen in generalization of this model of resource difference to all kinds of spam attacks targeting the network node.

10. REFERENCES

1. APWG Global phishing report [Electronic resource]. – Access mode: http://apwg.org/report-phishing/reporter/.
2. Consumer AV/EPP comparative analysis: phishing protection [Electronic resource]. – Access mode: https://www.nsslabs.com/reports/consumer-avepp-comparative-analysis-phishing-protection-edition-1.
3. Popov, E.A. Spam attacks on the distributed automated systems: an analytical expression of damage [text] / Popov E.A., Choporov O.N., Popova L.G., Ostapenko O.A. // Information and safety. – 2014. – 17 (4). – P. 634-637.
4. Popov E.A. Analytical evaluation of the risk of spam attacks with maliñious attachments on the elements of information-telecommunication networks [text]. / Popov E.A., Guzev Yu.N. // Management of information risks – 2015.

5. Spam. Security response [Electronic resource]. – Access mode: http://www.symantec.com/security_response/landing/spam/.

6. Ensuring the security of critically important objects and trends in the development of information technology / A.O. Kalashnikov, Y.V. Yermilov, O.N. Choporov, K.A. Razinkin, N.I. Barannikov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 399-403.

7. Analytical estimation of the component viability of distribution automated information data system / G.A. Ostapenko, D.G. Plotnicov, O.Y Makarov, N.M. Tikhomirov, V.G. Yurasov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 416-420.

8. Lvovich I.Ya. Analysis of potential of error-correcting capabilities of codes / I.Ya. Lvovich, A.P. Preobrazhensky, O.N. Choporov // Life Science Journal. – 2013. – 10 (4). – P. 830-834.

9. Analytical models of information-psychological impact of social information networks on users / G.A. Ostapenko, L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov, K.V. Simonov // World Applied Sciences Journal. – 2013. – 25 (3). –P. 410-415.

10. Denial of service in components of information telecommunication systems through the example of “network storm” attacks / A.G. Ostapenko, S.S. Kulikov, N.N. Tolstykh, Y.G. Pasternak, L.G. Popova // World Applied Sciences Journal. – 2013. – 25 (3). – P. 404-409.

11. Analytical estimation of the component viability of distribution automated information data system / G.A. Ostapenko, D.G. Plotnicov, O.Y Makarov, N.M. Tikhomirov, V.G. Yurasov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 416-420.

12. Yazov Yu. K. Improving an algorithm for detecting of urgent threats to security of personal data when they are processed in information systems of personal data / Yu. K. Yazov, E.S. Ostroukhova, I.G. Nazarov // Telecommunications and Radio Engineering. – 2012. – 71 (5) – P. 455-463.

13. The usefulness and viability of systems: assessment methodology taking into account possible damages / A.G. Ostapenko, E.F. Ivankin, V.S. Zarubin, A.V. Zaryaev // World Applied Sciences Journal. – 2013. – 25 (4). – P. 675-679.