BIOSCIENCES BIOTECHNOLOGY RESEARCH ASIA, November 2014. Vol. **11**(Spl. Edn.), p. 251-255

Peak Risk Assessing The Process of Information Epidemics Expansion

Nikolay Mikhaylovich Radko, Alexander Grigorievich Ostapenko, Sergey Vyacheslavovich Mashin, Olga Aleksandrovna Ostapenko and Artem Sergeyevich Avdeev

Voronezh State Technical University, Russian Federation, 394026, Voronezh, Moskovsky prospect, 14, Russian.

doi: http://dx.doi.org/10.13005/bbra/1471

(Received: 27 September 2014; accepted: 10 October 2014)

In this article, we propose a probabilistic development model of information epidemic and approaches to peak assessment of epi-resistance based on an analytical risk analysis of systems viral infection under a variety of information infections sources.

Key words: Information and Telecommunication System (ITCS), Risk, damage, model, chance, epi-resistance.

Currently researches are actively conducted on possibilities of using risk models of various attacks on ITCS components and damages emerging from their implementation for providing information security of the system. The unpredictability of these attacks does not allow creating a deterministic description of these processes and emerging from its implementation damages[1].

The main part

Let us consider the information and telecommunications system (ITCS), in which epidemic spread of harmful information occurs according to the SEIR model. To describe the model of information epidemic implementation, we consider the approach according to which spreading of harmful information in ITCS is studied using the binomial probability distribution. For correct use of such an approach it is necessary to consider that ITCS is closed, i.e. there is no immigration or emigration of elements[2]. Besides, within the timeframe of the information epidemic, failure of a system component is also not taken into account.

According to the SEIR model, system elements can refer to one of the following[3] sets:

1. S[i] – the set of elements, which are susceptible to receiving malicious information. Once they are infected, they pass to the category of incubation processes.
2. E[i] – the set of elements that have already been infected, but do not spread software threats yet. When they can already infect other objects, they move to the infected category.
3. I[i] – the set of elements, which can spread harmful information to receptive processes. Time that they spend in the infected state is an infectious period, after which they go to the recovered category.
4. R[i] – the set of elements that are completely free from harmful information and immune to the harmful effects with which they were

* To whom all correspondence should be addressed.

affected before.

Let us introduce parameters:

p_{li} – probability of latent infection of the element;

p_{fi} – probability of final infection;

p_{rec} – probability of recovering of the element;

N – total number of elements;

n – average number of connections between the affecting the ITCS elements and responses of protection means for this threat can generally be divided into two stages:

1. Infection of objects;
2. Treatment of objects (in this case, we assume that cured nodes are not infected again).

Let us consider the mathematical expectation as the primary measure of chance and risk [4] and carry out their evaluation (Table 1).

Table 1. Analytical evaluation of the set of elements parameters of the network structure in the course of infection on the SEIR model

Stage of infection	S[i]	E[i]	I[i]	R[i]
1	$(1-p_{li})n$	$p_{li}n$	_____	_____
2	$(1-p_{li})n \times (1-p_{li})n$	$p_{li}np_{li}n - p_{fi}p_{li}n$	$p_{fi}p_{li}n$	_____
3	$[(1-p_{li})n]^3$	$[(p]_{li}n)^3 - [(p]_{fi}p_{li}n)^2$	$[(p]_{fi}p_{li}n)^2 - [(p]_{li}p_{fi}p_{rec}n)$	$p_{li}p_{fi}p_{rec}n$
4	$[(1-p_{li})n]^4$	$[(p]_{li}n)^4 - [(p]_{fi}p_{li}n)^3$	$[(p]_{fi}p_{li}n)^3 - [(p]_{li}p_{fi}p_{rec}n)^2$	$[(p]_{li}p_{fi}p_{rec}n)^2$
…	……	… …	……	……
m	$[(1-p_{li})n]^m$	$[(p]_{li}n)^m - [(p]_{fi}p_{li}n)^{m-1}$	$[(p]_{fi}p_{li}n)^{m-1} - [(p]_{li}p_{fi}p_{rec}n)^{m-2}$	$[(p]_{li}p_{fi}p_{rec}n)^{m-2}$

It is easy to notice that we are dealing with geometric progression and after m stages of such infection the number of infected and recovered elements will amount to [5]:

$$S[m] = \frac{((1-p_{li})n)^m - 1}{(1-p_{li})n - 1};$$

$$E[m] = \frac{(p_{li}n)^m - 1}{p_{li}n - 1} - \frac{(p_{fi}p_{li}n)^{m-1} - 1}{p_{fi}p_{li}n - 1};$$

$$I[m] = \frac{(p_{fi}p_{li}n)^{m-1} - 1}{p_{fi}p_{li}n - 1} - \frac{(p_{li}p_{fi}p_{rec}n)^{m-2} - 1}{p_{li}p_{fi}p_{rec}n - 1};$$

$$R[m] = \frac{(p_{li}p_{fi}p_{rec}n)^{m-2} - 1}{p_{li}p_{fi}p_{rec}n - 1}.$$

In fact, Figure 1 represents some fractal in describing ITCS set on the SEIR model. By analogy, fractals can be created for other types of viral models. With their help, it is possible to adequately describe an arbitrarily long ongoing epidemic. Algebraically this model (see Fig. 1) corresponds to a system of difference equations:

$$S[i+1] = (1-p_{li})S[i] + (1-p_{fi})I[i];$$

$E[i]=S[i]$;

$I[i]=E[i]$;

$R[i]=I[i]$.

The total number of elements involved in the infection at the first stage is n. At the second stage, each of n elements interacts with n adjacent elements; the process can be represented with the recurrence relation. Then the total number of elements affected by viruses will be:

$$\overline{N_m} = n + n^2 + \cdots + n^m = \sum_{i=1}^{m} n^i = \frac{n^m - 1}{n - 1}.$$

Thus, the average damage from the viral insecurity of ITCS elements in normalized form will amount to [4]:

$$\mathbf{u} = \frac{I[m] - R[m]}{S_n} = \frac{\frac{(p_{fi}p_{li}n)^{m-1} - 1}{p_{fi}p_{li}n - 1} - 2 \times \frac{(p_{li}p_{fi}p_{rec}n)^{m-2} - 1}{p_{li}p_{fi}p_{rec}n - 1}}{\frac{n^m - 1}{n - 1}}.$$

The above function represents the risk of virus epidemic during m stages of infection. Hence the chance (virus protection utility) will be:

$$\bar{U} = \frac{S[m] + R[m]}{S_n} = \frac{\frac{((1-p_{li})n)^m - 1}{(1-p_{li})n - 1} + \frac{(p_{li}p_{fi}p_{rec}n)^{m-2} - 1}{p_{li}p_{fi}p_{rec}n - 1}}{\frac{n^m - 1}{n - 1}}.$$

Then the normalized epi-resistance will be equal to [6] the ratio:

Let us consider the development model of the information epidemic, in which the spread of infection begins with a single element. At the same time we will start from the worst case, in which at each stage of the process only uninfected and unrecovered elements will be subject to the effects with the probability of final infection and the probability of latent infection respectively p_{fi}=0.5, p_{li}=0.4, and infected elements will be recovered with the probability p_{rec}=0.15, the average number of connections for each element is n = 8.

The system epi-resistance for m = 10 will be equal to . Thus, benefits from means of protection are 136 times greater than the damage from infection of ITCS elements according to the SEIR model. Let us consider the parameters that determine the epi-resistance value. If we improve the antivirus subsystem, then elements will be recovered with a higher probability [7]. In addition, it is possible to restructure the system so that the average number of connections between the elements of the system has changed.

Therefore, the ITCS epi-resistance value for updated parameters p_{rec}=0.3 will be $L_f(10)$=138. As it can be clearly seen, the system epi-resistance has increased, but its level is still unacceptable. For new parameters p_{rec}=0.8 we have $L_f(10)$=143 In other words, changing probability of infected elements recovery have little effect on the system epi-resistance.

We obtain the value of the system epi-resistance function by changing the average number of connections for each element up to n=7. At the same time it is necessary to clarify that with such reorganization the efficiency of the entire system will remain the same. As a result, we have $L_f(10)$=358 Thus, as a result of changing the n parameter we have received the system epi-resistance that is double that the system epi-resistance with n = 8. Therefore, when regulating epi-resistance with the initial conditions it is the most effective to change the average number of connections, and by doing that the efficiency of the whole system does not change[8].

Epi-resistance management process can be divided into the following steps:

1. Determining characteristics of the information and telecommunication system.
2. Selecting an epi-resistance evaluation technique.
3. Analysing threats and their consequences, defining security vulnerabilities.
4. Epi-resistance evaluation.
5. Selecting safeguards.
6. Implementing and verifying selected measures.

Steps (5) and (6) relate to the selection of safeguards (neutralization of damage), and the rest – to epi-resistance evaluation.

Epi-resistance management, as well as any other activities in the field of information security, must be integrated into the life cycle of IS. Then the effect is maximum, and the costs are minimal.

The first two stages of the process of risk management can be regarded as preparatory. Overall, the point is as follows:

1. Selecting analyzed objects and the level of detail of their consideration as a primary step in risk assessment[9]. Here it is usually possible to consider all the ITCS infrastructure. However, if ITCS is large,

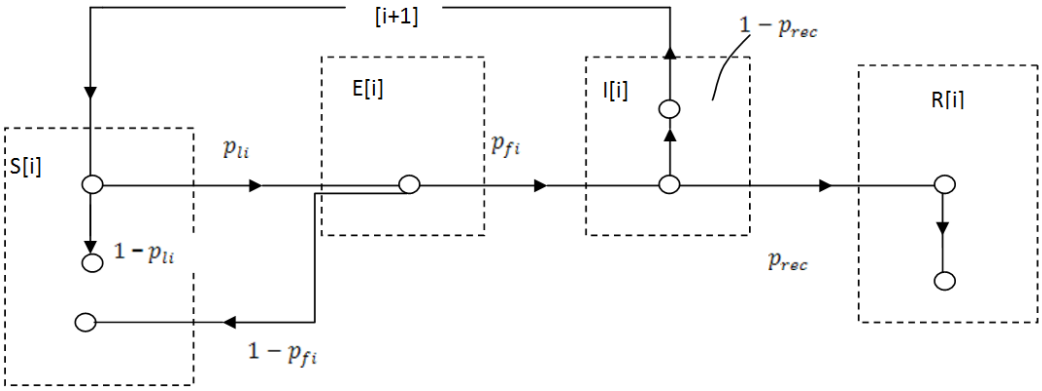

Fig. 1. The graph interpretation of the SEIR models of network structure infection on the m-th stage

comprehensive assessment may require unacceptable costs. In this case, it is advisable to focus on the most important services, agreeing in advance with an approximate final evaluation. If there are many critical services, we choose those risks for which are knowingly high or unknown.

2. The next step in the process of risk assessment is to determine the object of evaluation, that is, the boundaries of the analyzed information and telecommunications system, as well as resources and information, forming ITCS.
3. In this case, a system needs to have or to collect the following information:

a) ITCS architecture;
b) used hardware;
c) used software;
d) system interfaces (internal and external connectivity);
e) network topology;
f) data and information in the system;
g) criticality of the system and data;
h) sensitivity (i.e., the desired level of security) of the system and data.

4. Epi-resistance evaluation must be quantitative, providing a comparison with pre-selected boundaries of acceptability and costs of safety regulation.
5. The presence of a particular threat is the result of vulnerabilities in ITCS antivirus protection, which, in turn, is due to the lack of some security services or shortcomings in implementing their protective mechanisms. Identification is necessary here. It is advisable to identify not only the threat, but also the sources of their origin; it will help in selecting additional means of protection.
6. After identifying the threat, it is necessary to estimate the probability of its implementation. In addition to the probability of occurrence, the size of potential damage is important. To evaluate epi-resistance of information and telecommunication system, security of each valuable resource is determined by analyzing threats affecting a particular resource and vulnerabilities through which these threats can be implemented[10].
7. Regular reassessment (monitoring) of epi-resistance will allow maintaining ITCS safety data of an organization up to date, quickly identifying new risks and neutralizing them in a cost-effective manner.

CONCLUSION

We proposed a new approach to epi-resistance assessment and management for ITCS, components of which are exposed to viral effects according to the SEIR model.

Output

To summarize this research, we can say that ITCS epi-resistance strongly depends on parameters of the system itself and on an infection attacking it. Since it is usually not possible to affect parameters of the virus, by changing ITCS parameters we can adjust the epi-resistance indicator based on monitoring risk of information epidemic. At the same time, especially for mission-critical objects, peak epi-resistance assessment is of practical interest, this technique is described in this paper.

REFERENCES

1 Ostapenko, A.G., S.S Kulikov, N.N. Tolstykh, Y.G. Pasternak and L.G. Popova, Denial of Service in Components of Information Telecommunication Systems through the Example of “Network Storm” Attacks. *World Applied Sciences Journal*, 2013; **25**(3): 404-409.

2 Ostapenko, G.A., L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov and K.V. Simonov, Analytical Models of Information-Psychological Impact of Social Information Networks on Users. *World Applied Sciences Journal*, 2013; **25**(3): 410-415.

3 Ostapenko, G.A., D.G. Plotnikov, O.Y. Makarov, N.M. Tikhomirov and V.G. Yurasov, Analytical Estimation of the Component Viability of Distributed Automated Information Data Systems. *World Applied Sciences Journal*, 2013; **25**(3): 416-420.

4 Kephart, J., D.M. Chess and S. White, Computers and epidemiology. IEEE Spectrum, 2009; **5**(30): 14-34.

5 Piqueira, J., B. Navarro and L. Monteiro, Epidemiological Models Applied to Viruses in Computer Networks: 2010; 4.

6 Braichevsky, S.M. and D.V. Lande, Modern

information flows: actual problems. NTI-2005-Ser. 1. (Organization and methods of information work), 2005; **11**: 21-33.

7 Varlataya, S.K. and M.V. Shakhanov, Hardware, software, and methods of information security. Vladivostok, 2007; 317.

8 Olifer, V.G. and N.A. Olifer, Computer Networks. Principles, technologies, protocols. St. Petersburg, 2001; 158.

9 Ostapenko, G.A., L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov and K.V. Simonov, Information risks in social networks. Voronezh: Nauchnaya Kniga, 2013; 160.

10 Kalashnikov, A.O., E.V. Yermilov, O.N. Choporov, K.A. Razinkin and N.I. Barannikov, Attacks on information and technology infrastructure of mission-critical objects: risk assessment and management. Voronezh: Nauchanya Kniga, 2013; 160.