UDC 004.056.53

R.A.Umerov (National Aviation University, Ukraine),
F. Galindo, Ph.D. (Universidad de Zaragoza, Spain),
A.A.Tikhomirov, Sc.D. (IIA, Russia),
A.I. Trufanov, Ph.D. (Irkutsk State Technical University, Russia),
A. Rossodivita, M.D. (University of Medicine "Life and Health", Italy)

ADVANCED SCIENTIFIC AND PRACTICAL APPROACHES TO INFORMATION SECURITY

Reviewed developments in the field of information security, implementation of which the most successful acts standard ISO / IEC 27001, which helps to demonstrate the ability of an organization's ability to protect its information resources. Methods for modeling of socio-legal processes - Exponential and scale-free architecture

Currently, the territories of the former Soviet Union (and some other developing countries) can be quite clearly highlight some of the vectors of developments in the field of information security:

- total computerization of society, creating an urgent need for information security systems and information protection . Moreover, the development of computerization greatly predominates over the development of the IS

-the transition from the chaotic and kustarschiny in the creation of integrated systems for information security standardization, systematization and efficient government regulation

-financial obstacles that prevent the majority of public and private organizations and enterprises to adopt and implement the best international expertise on a a number of reasons - lack of finance for implementation of systems information security, lack of appropriate staff (in some way, too, because of lack of funds for the development of a special higher education and the high cost of obtaining a qualified education abroad, the leakage of professionals in connection with the best conditions of work and life)

- regulatory disorder, maladjusted legislation IS, inhibitory, and often to a standstill Exciting development of information security.

In general, the scope of information security is a wide variety of complex heterogeneous problems and limits of this sphere is constantly changing their position and shape

in virtue of their specific characteristics these challenges evolution in the field of information security are in a completely different planes, except for one that unites them time plane. And therefore, it is necessary to consider such issues at atime.

For the effective implementation of such an inhomogeneous complex tasks with one of the most successful solutions supports the ISO / IEC 27001, which establishes requirements for information security management system to demonstrate the organization's ability to protect its information resources. However, in the standard ISO / IEC 27001 little attention paid to the optimization of the above components, or rather, how to overcome the difficulties encountered in implementing complex systems of information security.

Information Security Management System based on the standard ISO / IEC 27001 allows you to:

Achieve reduction and value engineering support to security make information understandable to the assets of the organization's management. Identify the main security threats to existing processes, calculate risks and make decisions based on the organization's goals, to ensure the effective management of the system in critical situations.

Thus, the standard ISO / IEC 27001 provides insight into the readiness of certain procedures, but gives no clear idea on the most procedures for implementation, especially in the coordination and regulation of passage.

In the field of information dissemination objective laws redundancy. Positive data redundancy is designed to optimize the whole process of communication. For example, positive redundancy is used actively in the learning process, when repeated recurrence of typical situations lead to better assimilation of their audiences.

Positive redundancy is often used as a legislator reception improve the perception of regulation. Thus, many provisions of the Constitution of Ukraine are a repetition of the laws and legal entities in the State.

Negative redundancy violates the normal flow of information process. It represents a kind of "noise" or "interference." This, for example, declarative rules and regulations that are not equipped with mechanisms for implementation. Without performing the functions of regulation and self regulation, such laws have a negative overkill. Means of overcoming the negative redundancy is a high level of training regulations. Negative redundancy can make a deadlock introduction of the IB, especially in cases of conflict of laws and regulations, regulatory inconsistencies in the various departments that perform common tasks.

Another objective law, acting for the dissemination of information, the law of misrepresentation on the extent of its movement. This law is associated with different ability and willingness of subjects to its perception. That is why in those cases where important accuracy and completeness of information, raises the question of fixing information in a tangible medium, and subject to certain requirements for the procedure and method of fixation.

For example, to ensure that the information had probative value in court proceedings, it must be documented in compliance with a strict set of procedural requirements.

Standard 27000 limited scope of the enterprise (organization), for all its sequenced unfortunately did not reflect some new stages in the development of the subject area, such as the use of modern socio-legal models, especially those based on the theory of complex networks.

For explore a variety of socio-legal phenomena and processes of a long and successful method of socio-legal model [1].

The simulation method of socio-legal process - a method of cognition, in which process uses a helper object - a model. The most common types are graphical, verbal or mathematical model.

Consider, for example, the model number of conflicts in the regional network of the Autonomous Republic of Crimea (and nearby regions), recorded at the site cert.crimea.ua:

The verbal model:

1. Suppose that on the territory under consideration at time t_0 registered x_0 conflicts.
2. Let the number of conflicts detected increases over time the value of kx.
3. The adoption of measures of CERT-CRIMEA reduce the number of conflicts with the square of the total number of conflicts mx_2.

Then the mathematical model, which can be used to determine the number of conflicts at any time will have the form:

$$x(t) = kx_0 e^{kt}/(k-mx_0(1-e^{kt})) \quad (1)$$

4. Graphic model is presented in Fig. 1.

Stability of network architecture is one of the major problems of building effective complex systems, including and information. The models of Erdos-Renyi [2] Barabash-Albert [3] are now the most popular ones that describe real networks. The former has probability distribution of the links k that corresponds to the Poisson law:

$$P(k) \sim e^{-\lambda} (\lambda^k)/ k! \quad (2)$$

where λ - the distribution parameter.

These network models also are called random or exponential (E-net).Most of the 20 th century the exponential network is the base for the analysis of systems. With this kind of models connected with the development of graph theory. In [3], the authors drew the attention of researchers, that

many real networks (communications, Web, social, and metabolic) are different from that described by the exponential model in nature and have proposed a network model, in which:

i. Distribution of connectivity (number of bonds) corresponds to a power law

$$P(k) \sim k^{-\gamma}, \qquad (3)$$

where γ, the exponent while for the real world $1 \leq \gamma \leq 3$.

ii. Characteristic is the growth of a network with the introduction of new nodes and new connections, and there is a so-called "preferred connection"

iii. to use the terminology simple and understandable for experts from different disciplines.

This network model is called the scale-free (SF) one :such models with nontrivial topological properties best suited to the term "complex".

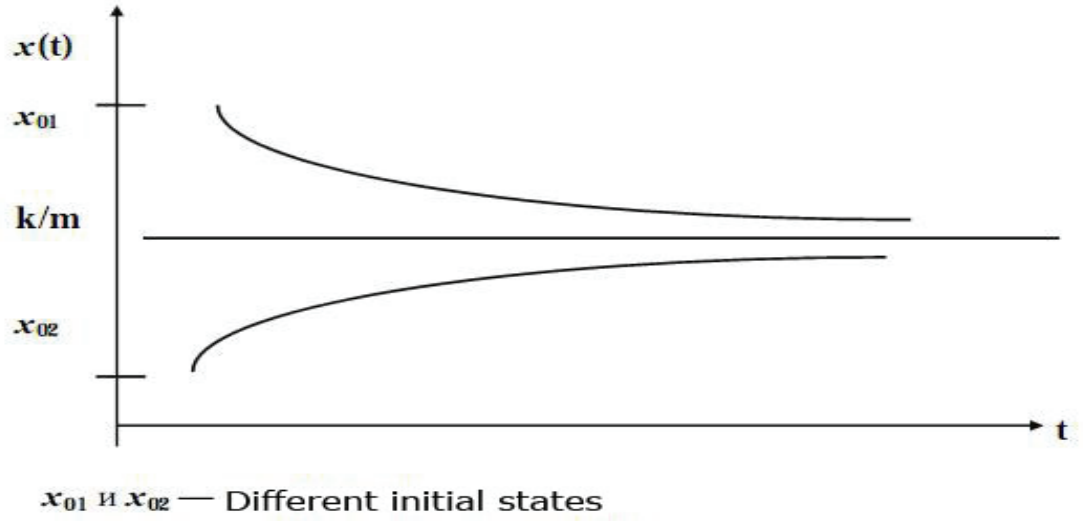

Fig. 1. Graphic model of the dynamics of conflicts detected in time.

Fig. 2 demonstrated the topology of exponential and scale-free networks [3].

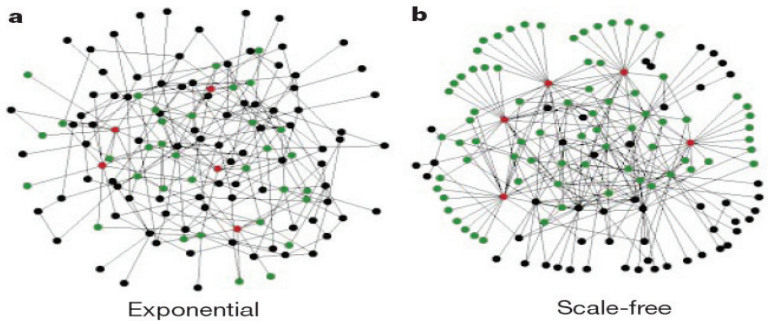

Fig. 2. Exponential (a) and scale-free (b) network [3]

The stability of these two different: exponential and scale-free architectures was substantially different to the two main classes of attacks on network nodes: random and intended ones.

Random attacks (denial, disruption, R-attacks) have a random selection to destroy a node. The classic strategy of targeted or intended attacks (I-attacks) is the subsequent destruction of the nodes with maximum connectivity. Usually, the consequences of attacks studied networks are analyzed using a broad set of metrics: record the change in the diameter, the average connectivity, separating the middle, the clustering coefficient of various central, the maximum size of the cluster and its relative values. It was found [3] (Fig. 3) that the exponential network is equally vulnerable to the R- and I-attacks

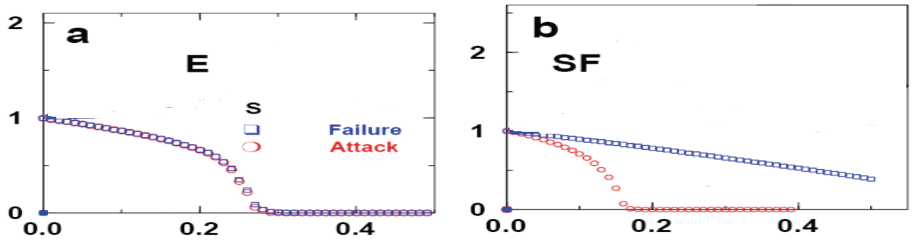

Fig. 2. The dependence of the relative size of maximal cluster in the exponential (a) and scale- free (b) networks exposed to random (□) and intentional (○) attacks.

Complex (scale-free) networks were resistant to R-attacks ,and are extremely vulnerable to attacks focused.

Indeed, targeted attacks on SF- network more efficient, but they are considerably expensive.

In practice, there are far more complex situation than a separate R-attack or I-attack: it is often possible combinations of failures and targeted attacks [4].

References

1. Chubukova S.G, Elkin V.D. Foundations of Legal Informatics. - Moscow, 2007. – 84p.

2. P. Erdos, A. Renyi, Publ. Math. Inst. Hung. Acad. Sci. 5, 1960, p.17-25.

3. A.-L. Barabási, R. Albert, H. Jeong. Mean-field theory for scale-free random networks. Physica A 272, 1999, p. 173-187.

4. F. Galindo, A. Caruso, A. Rossodivita, A.A. Tikhomirov, A.I. Trufanov, E.V. Shubnikov. Restructuring of the topology of complex networks as a strategy to protect against blended threats. Energy conservation and energy efficiency: challenges and solutions. MM: Inforizdat, July, 2010, pp. 102-106.