Simulation of data safety components for corporative systems

Svetlana A. Yaremko[a], Elena M. kuzmina[a], Tamara O. Savchuk[b], Valeriy E. Krivonosov[c], Andrzej Smolarz[d], Abenov Arman[e], Saule Smailova[f], Aliya Kalizhanova[g]
[a]Vinnitsa Institute of Trade and Economics Kiev National Trade and Economic University, [b]Vinnytsia National Technical University, [c]Pryazovskyi State Technical University; [d]Lublin University of Technology, Nadbystrzycka 38A, 20-618 Lublin; [e]Joint-Stock Company "Alatau Zharyk Companiyasy" Regional Energy Transmitting Company; [f]D.Serikbayev East Kazakhstan State Technical University, Ust-Kamenogorsk, Kazakhstan; [g]al-Farabi Kazakh National University, 71 al-Farabi Ave., Almaty, Kazakhstan

ABSTRACT

The article deals with research of designing data safety components for corporations by means of mathematical simulations and modern information technologies. Simulation of threats ranks has been done which is based on definite values of data components. The rules of safety policy for corporative information systems have been presented. The ways of realization of safety policy rules have been proposed on the basis of taken conditions and appropriate class of valuable data protection.

Keywords: data protection, safety policy, corporative information systems, scale of values, data protection risks, definition of access rules, classes of data protection resources

1. INTRODUCTION

The latest information technologies are one of motive factors of development of all spheres of human vital activity, i.e. economics, technology, science and education. Thus using Internet telecommunication means makes it possible to perform centralized control of great corporations whose structural subsections are located in different regions of the country and abroad. It allows to solve problems of ensuring appropriate speed of telecommunication, message exchange, business transactions as well as electronic contracts. Nevertheless, along with some advantages provided by telecommunication means for message exchange and financial data there is a problem confidential data protection from unauthorized access and defects. So according to statistics, given in [1], coordination centre CERT in Carnegie Mellon University (USA) receives daily about 225 reports about security violation in corporation information systems. Besides, some outside intrusion can influence data reliability and result in threatening financial stability of corporation. Therefore, data security control in corporative systems based on the developed standards, rules and practical techniques of safety policy (SP), what can regulate control, protection and distribution of valuable information is a relevant task of research.

The main notions of data protection theory, rules and propositions of safety policy are grounded by such scientists as Barychev S.H.[2], Barmen S.[3], Hlavatiy V.[4], Hrusho A.A.[5], Stollynhs V.[8], Shcherbakov A.[10] and others. Their works represent the basis for creation and realization new trends and methods in the area of data protection. The purpose of the article is simulation of fundamental components of information security in corporative information systems, which allows to ensure confidential information as well as its availability and protection from outside intrusion.

2. METHOD

Some methods of mathematical simulation have been used in the work. They are one of the effective instruments, which allows to design functional components of complicated systems. Currently, the role of computer security is constantly increasing. The companies invite administrations, designers and engineers to provide reliability of their systems and services during a day. However, to become a victim of users with criminal intent as well as special programs or coordinated attacks is direct threat for successful activity of any company. At the same time the process of designing SP standards and rules may be complicated enough and it requires taking into account basic principles of data protections as well as some peculiarities of definite systems. Thus, particular SP in different corporative information systems can be

*:svitlana_Yaremko@ukr.net

Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2017, edited by Ryszard S. Romaniuk, Maciej Linczuk, Proc. of SPIE Vol. 10445, 104451R
 · doi: 10.1117/12.2280834

changed depending on the set of information components, chosen scale of values, defined threats or data security as well as real hardware and software used for data protection.

In general, the policy SP for information systems includes the following sequence of actions [2, 3]:

- creation of structure of values;
- analysis of threats for information security;
- determination of rules for any process using a given king of access to data components which have a given scale of values.

Let's develop basic SP regulations for the corporative information system which comprises the following information components:

- messages transmitted from structural subsections along the information channel of Internet network towards Web-server of the corporation head office;
- data base of corporation staff;
- data base which stores information about structural subsections;
- data base which comprises total indicators of corporation record and financial activity;
- module of data processing which are sent from structural subsections;
- module of making control decisions as for corporation activity;
- control indications that are transmitted to structural subsections of corporation on the information channel in the opposite direction.

To determine values of each information component let's apply the ordinal scale which is used for evaluating secret information in state structures [2, 3], i.e. "non-secret" (NS), "for official use" (FOU), "secret" (S), "top secret" (TS). The given levels of secrecy make plural R = {NS, FOU, S, TS} which is linearly ordered:

$$NS < FOU < S < TS.$$

Besides the upper level has more importance. That's why the requirements for its protection from unauthorized access are also much higher. Taking into consideration the above mentioned we can give the corresponding levels of secrecy to information components of the corporative system. For example, messages transmitted from structural subsections towards Web-server of the corporation head office are given S-level, data base of corporation staff is given FOU, data base which stores information about structural subsections activity is given FOU, data base comprising total indicators of corporation activity is given FOU, module of data processing sent from structural subsections is given S, module of making control decisions is given TS, control indications transmitted in the opposite direction towards structural subsections is given S. As a result of identification the system components make plural $M = \{ K_{ir}, \ldots, K_{ir} \}$, where $i=1,2,\ldots,n$ – information components of the system, r – is a secrecy level of information component, $r \in R$. According to [3], this plural can be considered as a linear lattice of values. Then for components of plural M, which have different kinds of secrecy K_{iFOU}, K_{iS}, K_{iTS} there are true ratios, i.e.

$$K_{iFOU}<K_{iS},\ K_{iS}<K_{iTS} \Rightarrow K_{iFOU}<K_{iTS}.$$

The given properties generate the following statements:

1) For $K_{iFOU}, K_{iS} \in M$ element $K_{iTS}=K_{iFOU} \oplus K_{iS} \in M$ is the upper limit, if

$$K_{iFOU}<K_{iS},\ K_{iS}<K_{iTS};$$

$$K_{iFOU}<K_{iFOU} \oplus K_{iS},\ K_{iS}<K_{iFOU} \oplus K_{iS} \Rightarrow K_{iTS}<K_{iFOU} \oplus K_{iS} \text{ forall } K_{iFOU} \oplus K_{iS} \in M.$$

Thus, the upper limit of a lattice is an element whose level has the greatest value which provides for the highest level of protection.

For $K_{iFOU}, K_{iS} \in K_{iTS}$ element $K_{iNS}=K_{iFOU} \oplus K_{iS} \in M$ is the lower limit, if:

$$K_{iNS}<K_{iFOU},\ K_{iNS}<K_{iS};$$

$$K_{iFOU} \otimes K_{iS}<K_{iFOU},$$

$$K_{iFOU} \otimes K_{iS}<K_{iS} \Rightarrow K_{iNS}<K_{iFOU} \otimes K_{iS} \text{ for all } K_{iFOU} \otimes K_{iS} \in M.$$

The lower limit of a lattice is an element which has the least value and it is characterized by the least degree of protection.

2) Plural M is a lattice, if for any K_{iFOU}, $K_{iS} \in M$ there exist $K_{iFOU} \oplus K_{iS} \in M$ and $K_{iFOU} \otimes K_{iS} \in M$.

According to the above mentioned we might come to a conclusion that for all elements M of a lattice of values there exists the upper element High=⊕M and the lower element Low=⊗M. In this case, the upper element of High lattice will be K_{iTS} and lower element will be Low i.e. K_{iNS}.

On determining the values of information components according to chosen ordinal scale for the given corporative information system the next stage of making SP is definition of threats for data security and their analysis. By threats we can consider actions or factors which might lead to disturbance of secrecy, integrity and data availability incorporative information systems. So according to [4–6] the less of secrecy can be caused by the following threats, i.e. unreliable associates, enemy intelligence, non-high quality policy of information security, unnoticed taking of information, transfer of confidential information, data identification and connection to communication channels. The disturbance of data integrity, its destruction or modification can be defined by the following factors: mistakes of staff, human factor, access to the ground connection, fines, disasters and also different virus attacks. Different breaks, disturbances in the transmission channel and other factory can result in the less of data availability and possibility of its obtaining.

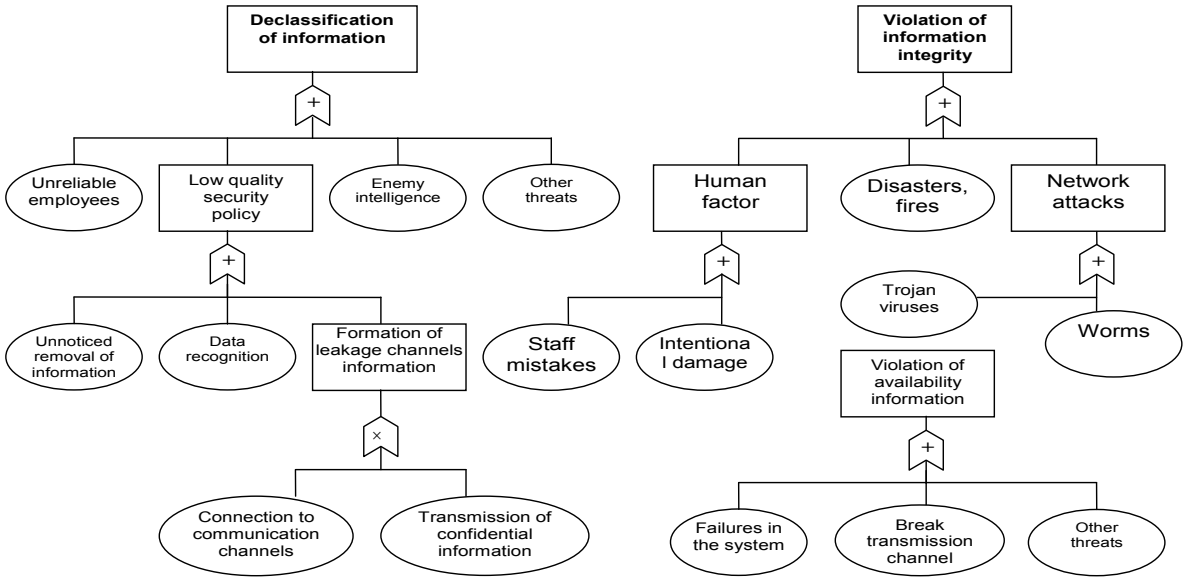

Figure1. Hierarchical models of information security threats to corporate information systems.

Taking into account the presented review of threats, the so called declassification of information, description of its integrity and availability are considered to be the main events and the ones bringing them about are the proper factors of these events.

Provided threats independence, probability of appearance of main events can be found in the following way [6]:

- in the case of the main event providing the logic multiplication of events ensuring it:

$$P = \prod_{i=1}^{k} P_i ;$$

- in the case of the main event providing the logic addition of all events ensuring it:

$$P = 1 - \prod_{i=1}^{k} (1 - P_i),$$

where P_i is the probability of i-th event which causes the appearance of the given main event and k is the total number of events which bring about the main event.

Having examined some threats or events which result in the loss of data security in corporative information systems and having defined the main events we can represent them as a hierarchic tree pattern of refusals risk (Fig.1).

3. RESULTS AND DISCUSSION

Let's define the ranks for the given threats models. It makes possible to reveal the essence of the mentioned threats for the general data security in corporative information systems. The definition of events ranks is performed according to methodology proposed in [6]. It provides for calculation as for the difference between the probability of the main event P and P^i which is probability in the case of extraction of the i-th event whose rank is calculated according to:

$$\Delta P_i = P - P^i$$

Table 1. Calculation of ΔP_i and obtained ranks of events

Event No.	Name of event	Difference probability	Ranks of events
Declassification in formation			
1.	Unreliable employees	0,45	1
2.	Enemy intelligence	0,1	3
3.	Unnoticed removal of information	0,05	4
4.	Transmission of confidential information	0,05	4
5.	Data recognition	0,15	2
6.	Connection to communication channels	0,15	2
7.	Other threats	0,05	4
Violation of information integrity			
1.	Human factor	0,75	1
2.	Disasters	0,03	5
3.	Fires	0,07	3
4.	Network attacks	0,09	2
5.	Other threats	0,06	4
Violation of availability information			
1.	Failures in the system	0,5	1
2.	Break transmission channel	0,45	2
3.	Other threats	0,05	3

Using probabilities of appearance of different events given in [6] we can perform calculation of a difference between probability appearance of main events and that of extraction of a given event.

On arranging the calculated differences ΔP_iin the order of increase we can obtain threats ranks of data security. Table 1 presents calculated results ΔP_i and obtained ranks.

As it is obvious from table 1, the highest rank belong to the threats connected with human factor, i.e. unreliability of associates, their mistakes and deliberate actions as for information damage which shows their prominent influence on data security in corporative information systems.

Taking into account the defined values of information components and calculated ranks of threats which influence the general data security we can derive the basic SP theses given in [2, 3, 7-14].

1. Determination of access rules. It is important for those persons, who don't have the appropriate range of powers for the staff in order to prevent their access to confidential information:

- data concerning activities of structural subsections and the corporation on the whole;
- messages from structural subsections which are transmitted to Web-server of the corporation;
- instructions of control which are transmitted in the opposite direction, etc.

The definition of access rules is carried out by means of mandate check which makes it possible to conduct inspection of all addresses to system information components. It is also desirable to provide for possibility of getting access to data for the staff if there is a necessity and proper approval of authorizes.

2. Identification of information objects of the system. To perform control for data access in accordance with mandate check it is necessary to mark each information component of a system. It allows to identify an object definitely. It may be a defined value of a component or access procedures which are given to persons who can make inquiry for getting valuable information.

3. Check of inquires for valuable information. To avoid unauthorized access to information it is necessary to check if certain persons are allowed to have access to different kinds of valuable information.

4. Check of risks for data security. It is necessary to register events related to system security to ensure the effective analysis of risks for data security.

Let's consider the ways of information security policy based on the given rules and requirements for providing secrecy, integrity and availability of information. As it was mentioned above, the check of access to valuable information can be performed by means of mandate policy. It is carried out by some protection subsystem on the lowest hardware and software level which allows to make protected area for mandate check. A mandate check device which performs other additional functions is called application monitor. Mandate check is also called obligatory since it characterized each application of a subject to an object, if a subject and an object are under the protection of a security system. Let's consider a method of arranging mandate check in a corporative information system. Each information component K_{ir} obtains some mark about class (value) $C(K_{ir})$.Each subject S has also mark which includes information about its access class C(S). Mandate check compares marks and satisfies subject's application to K_{ir} object for reading, if $C(S)>C(K_{ir})$. If mandate check is realized in a system, with U_i user's application to the data base for reading it I allowed to form the "review" of only such information whose class is $C(U_i)<C(U)$.

By analogy, mandate check and decomposition rules permit to support information currents in the proper direction in the process of data base functioning. Thus, with mandate policy available the relation multi-level data base will be protected by means of access control to valuable information.

Next stage of realization of information security policy is choice of procedures and class of protection system of information resources. According to [2, 5, 7] in complicated computer systems the following protection classes are used:

- class D: minimal protection. It is used for systems which were evaluated from the point of view of defense. However, they couldn't achieve the requirements for higher classes of protection;
- class C1: protection is based on access control. Guarantee protected system of C1 class includes control means of access restriction to protect projects and private information to avoid unauthorized reading or extraction;
- class C2: protection is based on managed access control. All the requirements to class C1 are transferred to class C2. Besides, there is registration of events in the system of class C2. They are related to the security system and derision of resources. There is also a special requirement concerning "purification" of system resources with repeated usage by other processes;
- class B1: mandate protection based on giving marks to objects and subjects with are checked. Requirements for class B1 system assume all the requirements which were necessary for class C2. Besides it is necessary to define the model which comprises security policy, assigning marks to data and mandate control for access to named objects;
- class B2: structural protection. The systems of class B2 propose all therequirements for data protection for class B1 systems. The given protection system is based on strictly defined and formally documented model in which access control is widely distributed to all subjects and objects of the automated data processing system;
- class B3: using of security domains. It is for introduction of administrator of security system. Check mechanisms are expanded to provide obligatory message about all the events connected with possible violation of safety rules for the system. The procedure of renovation is obligatory;
- class A1: verification project. Class A1 systems are functionally equivalent to class B3 systems because there aren't any new requirements to security policy. The characteristic feature, of this class systems is formal specification of the project and protection verification, i.e. the highest level of confidence that guarantee protected computer base is realized in the connect way.

Let's calculate the risk index of data security in the corporative information system for justifiable choice of procedures and classes of protection system. Among assigned levels of secrecy of systems information components the minimum access level for a user R_{min} in a system is FOU, and maximum R_{max} is TS, since in ordinal scale of values FOU=2 and TS=4, then risk index according to [6] is $Risk_{Index}= R_{max} – R_{min}=2$.

Thus, the systems of other class of protection – C1 and C2 corresponding to the defined risk index can provide for access control of users to data resources and ensure check of events related to system security and distribution of resources. Besides, it is necessary to use the procedure of isolated security which makes it possible to achieve high protection of strictly confidential information.

For increasing information resources which need intensified protection it is expedient to use class B systems which provide for introducing security system administrator. According to the requirements of information security policy mentioned above, the check mechanisms in the given class allow to provide obligatory message about possible violation of security rules. For this protection class there are some obligatory procedures which can provide renovation of the system. Thus, application of these class systems will ensure stability and dependability for different efforts of intrusion.

The chosen methods of data protection are reservation, archives and destruction of information. To neutralize the channels of information loss it is important to check information currents as well as to encipher information by cryptographic methods.

4. CONCLUSIONS

The work has solved the problem of designing information resources security rules for corporative information systems. The trends of their realization have been presented. It makes possible to ensure information confidence as well as its availability and protection from outside instruction. For this purpose secrecy levels of system information components have been determined and security information threats have been analyzed. It has given on opportunity to ground requirements for information resources protection system and calculate risk index which provides appropriate protection means.

REFERENCES

[1] Kunchenko-Kharchenko V.I., [Dokumentalistyka], ChDTU, Cherkasy, (2006).
[2] Barychev S.H., [Osnovy sovremennoy kryptolohyy], Telekom, Moscow (2001).
[3] Barmen S., [Razrabotka pravyl ynformatsyonnoy bezopasnosty], Williams Publishing House, Kiev, (2002).
[4] Hlavatiy V., "Metody zashchyty informatsyy," Korporatyvnyie systemy 4(1), 65–69 (2005).
[5] Hrusho A.A., [Teoretycheskye osnovy zashchyty ynformatsyy], Yzdatel'stvo ahentstva Yakhtsmen, Moscow, (2001).
[6] Dudat'yev, A.V., "Rozrobka unifikovanykh modeley systemnoho proektuvannya optymal'nykh system zakhystu informatsiynykh resursiv," Visnyk ChDTU (1), 3-8 (2008).
[7] Kozieł, G., Maluga,J., "Security of hotspots in buses," Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska 4, 53-57 (2016)
[8] Stollynhs, V., [Kryptohrafyya y zashchytasetey: pryntsypy y praktyka], Williams Publishing House, Kiev, (2001).
[9] Shcherbakov, A., Domashev, A., [Prykladnaya kryptohrafyya: Yspol'zovanye y syntez kryptohrynterfeysov], Russkaya Redaktsya, Moscow, (2003).
[10] Rembielińska, A., "The safety procedures on the passenger plane board," Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska 1, 8-12 (2011)
[11] Romanyuk, N., Pavlov, S. V., Dovhaliuk, R. Yu., Babyuk, N. P., Obidnyk M. D., Kisala, P., Suleimenov, B., "Microfacet distribution function for physically based bidirectional reflectance distribution functions," Proc. SPIE 8698, 86980L (2013).
[12] Kostishyn, S., Tymchyk, S., Vyrozyb, R., Zlepko, A., Pavlov, V., "Design features of automated diagnostic systems for family medicine," Proc. TCSET'2016, 774-776 (2016).
[13] Jachimski, M., Mikoś, Z., Wróbel, G., "(Building automation systems performing safety functions - hardware structures," Przegląd Elektrotechniczny 91(4), 109-114 (2015).
[14] Shcherbakov, A., [Vvedenye v teoryyu y praktyku komp'yuternoy bezopasnosty], Nolydzh, Moscow, (2001).