Journal of Engineering and Applied Sciences 12 (Special Issue 6): 7776-7778, 2017
ISSN: 1816-949X

Definition of the Method of Determination of the Violator of Information Security in Process of Modeling the Threats of Information Security in the Information Systems of Processing Personal Data

Roman Zhuk and Alexandra Vlasenko
Institute of Computer Systems and Information Security,
Kuban State Technological University, Krasnodar, Russia

Abstract: In the study, the researcher's method is given and the criteria allowing determining the type and kind of the violator of information security listed as well as its potential in modeling information security threats in information systems for processing personal data.

Key words: Information system for processing personal data, violator, potential, threat, vulnerability, security

INTRODUCTION

In 2011, after the processing and updating of the legislation of the Russian Federation regulating the protection of personal data (Federal Law, 2006) a number of normative and methodological documents establishing the requirements for the organization of the protection of information containing Personal Data (hereinafter, PD) with its automated processing in Information Systems (hereinafter, ISPD).

METHOD OF DETERMINATION OF THE VIOLATOR OF INFORMATION SECURITY

The primary task that must solved in the process of organizing PD protection is the construction of a model of information security threats for ISPD. The main reason influencing the definition of threats to Information Security is the violator of information security (hereinafter, IS).

Classification of the violator IS is presented by FSTEC (2008) and includes two types of the intruder, about the possibility of physical access to the controlled zone where the assets of the ISPD are located. In turn, the types of violators divided into categories, for each of which there are certain possibilities. Proceeding from this, based on the expert method, involving an expert in the field of information security, an assessment of the capabilities of violators made and, based on the expert's conclusion; the type and category of violators that are relevant to the ISPD are established.

However, now, the Federal Service for Technical and Export Control of the Russian Federation (hereinafter, referred to as FSTEC of Russia) recommends that ISPD operators when modeling IS threats in ISPD use the database of IS threats and vulnerabilities (FSTEC., 2017). It should note that this information resource created using Common Weakness Enumeration (CWE., 2006) and Common Vulnerability Scoring System (First, IST., 1995).

When using this resource to decide the IS threats to the ISPD operator, it is enough to choose the source of threat and the violated properties of information security (confidentiality, integrity, availability). The main problem in the process of selecting threats to the IS which is met by the ISDN operator is the lack of a technique for establishing the type of violator and its potential.

At the beginning of 2015, the FSTEC of Russia published a draft methodological document describing the method for determining IS threats for information systems (FSTEC., 2008). According to FSTEC (2008), the IS violator is divided into 2 types and 11 categories which have possible goals (motivation) and potential, depending on the capabilities to show and implement the vulnerability of the assets of ISDN. According to FSTEC (2008), the vulnerability identification capability includes the following parameters which assigned numerical values:

- Identification time
- Technical competence
- Knowledge of the characteristics of ISDN
- Equipment
- Availability of access to the ISDN

The value of each parameter assigned during the expert evaluation and tied to the period; however, a number of parameters such as equipment, technical competence should established by statistics.

Corresponding Author: Roman Zhuk, Institute of Computer Systems and Information Security, Kuban State Technological University (KubSTU), Turgeneva St., 199, Vladimirovich, 350078 Krasnodar, Russia

At present, there is no necessary statistics for determining these parameters, because of which the percentage of subjectivity increases when the operator decides on the ISDN. Parameter identification time, depending on the above parameters can also be determined incorrectly. Based on the foregoing, this technique does not allow to unify the process of determining the potential of the offender and to reduce the degree of subjectivity in making a decision.

In addition, the method for determining the level of protection of ISDN (DGRF., 2012) provides for determining the type of real threats associated with the presence of undeclared capabilities in the ISDN software which not taken into account when describing the method for determining the potential of the offender. On the basis of the foregoing, taking into account the "best practices" (First, IST., 1995), the following processes analyzed to develop a method for determining infringe of information security:

- Definitions of significant assets of ISDN by the algorithm for assessing the significance of the asset presented in the methodical document (ISO and IEC., 2010)
- Identification of the vulnerabilities of the asset, through monitoring of vulnerability databases or using vulnerability scanners

Proceeding from the prepared list of vulnerabilities for significant assets of ISPD, we will outline the following criteria for determining infringe of IS in ISPD:

- The availability of physical access to the asset, the indicator assigned the values: "through the public network", "through the local area network", "physical access"
- The need for interaction with the user, the indicator assigned the values: "necessary", "no need"
- Availability of information on the vulnerability in the general access, the indicator assigned the values: "there is no description", "partly described" is "fully described"
- The need to use special tools to exploit the vulnerability, the indicator is assigned the values: "it is necessary to use special means", "no special means are required"

Based on the above, we build a table and assign numerical values to the parameters. In accordance with the values defined in Table 1, we set up the following gradation of the potential of the offender:

Table 1: Numerical values of parameters

Parameters	Names	Numeric values
Physical access to the asset:	Through public networks	1
	With the help of a local-area network	0.5
	Physical access	0
The need for interaction with the user	Required	0
	No need	1
Availability of vulnerability information in general access	Missing description	1
	Partially described	0.5
	Fully described	0
The need for special tools to exploit the vulnerability	It is necessary to use special tools	1
	Application of special means does not require	0

- The violator will have a high potential if the sum of the value is equal to or greater than 3
- The average potential violator will have for a sum of value in the range of >1 and <3
- A low potential intruder will have for a sum of value in the range ≤1

It should note that for each type of offender the potential calculated separately. The advantage of this method is that the parameters used to decide the type and potential of the intruder established at the stage of vulnerability identification which completely eliminates the human factor and automates the process.

CONCLUSION

However, despite the automation of this process, it is necessary to take into account the increasing role of parameter accuracy in identifying the vulnerabilities of ISPD assets and the need to describe in more detail the information structure and technologies used to process the PD.

REFERENCES

CWE., 2006. Overview: What is CWE?. Common Weakness Enumeration, USA. https://cwe.mitre.org/about/index.html.

DGRF., 2012. On the approval of the requirements for the protection of personal data when processing them in information systems of personal data. Decrees of the Government of the Russian Federation, Moscow, Russia.

FSTEC., 2008. The basic model of threats to the security of personal data under their: Processing in the information systems of personal data. Federal Service for Technical and Export Control, Russia.

FSTEC., 2015. Methodology definitions of threats security information in information systems. Federal Service for Technical and Export Control, Russia. http://fstec.ru/component/attachments/download/812.

FSTEC., 2017. State research institute of problems of technical protection of information. Federal Service for Technical and Export Control, Russia. http://bdu.fstec.ru/

Federal Law, 2006. On personal data. Federal Law, Russia. https://iapp.org/media/pdf/knowledge_center/Russian_Federal_Law_on_Personal_Data.pdf.

First, IST., 1995. Common vulnerability scoring system SIG. FIRST-Improving Security Together, Tempe, Arizona, USA. https://www.first.org/cvss/

ISO and IEC., 2010. Information technology methods and means of ensuring security: Risk management information security. International Organization for Standardization, International Electrotechnical Commission, Geneva, Switzerland.