Impact Factor: 9.9 ISSN-L: 2544-980X

Methods of Calculating Threats to Information Security in Critical Information Infrastructures

Jorayev Jahangir Nurmakhamadovich [1]

Annotation: Threat assessment is an important tool in building defenses as a key part of information security (IA) direction (threat management). The threat assessment process is intended to identify security measures in organizations and agencies, to take measures to reduce threats.

Key words: Assessment of threats , assets (resources) , level of threats , level of vulnerabilities .

A classic view of threats is the likelihood of threats to information security. Threat assessment includes modeling of recording all negative factors representing threats. From a mathematical point of view, when analyzing threats, such factors can be considered as input parameters. Therefore, it is necessary to take into account the many sources of information and the uncertainty of the information itself. The threat assessment phase focuses on direct formulas and input data needed to calculate threat values.

This paragraph provides an analysis of several methods for estimating threats, and a specific method is referenced. The purpose of the work is to have an array of actual threats and to develop a formula of threats to information security that is used to estimate monetary equivalent losses.

Threats to information security are classically defined by three variable functions:

- likelihood of threats ;
- the probability of the existence of vulnerabilities (vulnerabilities);
- hidden effects .

If any one of these three variables approaches 0, then the threat starts to change towards 0 completely.

Threat assessment methods. ISO/IEC 27001 "Information technologies. Methods of ensuring security. Information security management systems. In accordance with the requirements, the chosen methodology must guarantee that the assessment of threats is comparable and provides the obtained results. Therefore, this standard does not provide specific calculation formulas.

NIST 800-30 "Risk management guide for information technology systems" provides the following classic formula for calculating threats:

$R = P(t) \cdot S (1)$

here:

R is the value of the threat;

P (t) is the probability of threats to information security (a mixture of qualitative and quantitative scales is used);

S is the degree of impact of the threat on assets (valuation of assets on qualitative and quantitative scales).

In the final calculation process, the relative unit value of the threats that can be regulated according to the value level for the management procedure of threats to information security is calculated [2].

[1] Tashkent University Ferghana branch Muhammad Al- Khorazmi in the name of information technologies

GOSTRISO/MEK TO 13335-3-2007 "Information technologies. Methods and means of ensuring security. Part 3. Methods of security management of information technologies, calculating threats in accordance with NIST 800-30 "Risk management guide for information technology systems. It differs from the "Recommendations of the National Institute of Standards and Technology " standard by the following formula :

$R = P(t) \cdot P(v) \cdot S(2)$

$P\ (\ t\ )$ is the probability of threats to information security;

$P\ (\ v\ )$ is the probability of the presence of weaknesses ;

C is the value of assets .

$P\ (\ t\ )$ and $P\ (\ v\ )$ are given as an example of a three-level quality scale (low, medium and high). C is represented by numerical values in the range from 0 to 4 to evaluate the unit of asset value.

According to BS 7799-2:2005 "Specification for information security management systems", the level of threats is determined by taking into account the following indicators: the value of resources, the level of threats and the level of vulnerabilities. As these parameters increase, so does the threat. In this case, the formula can be expressed in the following form:

$R = S \cdot L(t) \cdot L(v)(3)$

here:

C - value of assets (resources) ;

$L\ (\ t\ )$ – level of threats ;

$L\ (\ v\ )$ – level of weaknesses .

In practice, the calculation of threats to information security is carried out through tables representing the value of the level of threats, the probability of vulnerabilities and the value of assets. The value of threats can vary between 0 and 8, resulting in a list of threats with different values for each asset. According to the standard, it is proposed to sort the threats using the following scales: low (0-2), medium (3-5) and high (6-8). This allows you to identify the most serious threats.

RS BR IBBS-2.2-200 "Ensuring information security of banking system organizations of the Russian Federation. In accordance with the methods of assessment of threats of information security violations", the assessment of the level of implementation possibilities of threats to information security is expressed using the following qualitative and quantitative scales: non-implementable threats - 0%, average threats from 21% to 50%, etc. It is proposed to assess the severity of the consequences for various information assets using a qualitative-quantitative scale, i.e. minimum - 0.5% of the organization's capital , high - from 1.5% to 3% of the organization's capital.

For a qualitative assessment of threats to information security, a table of compatibility of the severity of consequences and the probability of threat implementation is used. If there is a need for a quantitative assessment, then the following formula is used:

$R = P(v) \cdot S(4)$

here:

C - value of assets (level of severity of consequences).

Having considered the part of calculating the values of threats to information security of all the methods of calculating threats listed above, it can be said that the threats are calculated using the values of threats and the value of assets. The main disadvantage of these methods is that the cost of assets (the amount of losses) is in the form of conditional units. Conditional values are not considered a unit of measurement, including, when used in practice, cannot be expressed in the form of monetary equivalent. As a result, it does not provide a realistic representation of the level of threats to the assets of real protection objects.

In this case, it is suggested to divide the threat calculation procedures into the following stages:

- calculating the value of technical threats;
- calculation of hidden damages.

Technical threats mean the likelihood of threats to information security and the value of each component of information infrastructures, which includes the presence of vulnerabilities, taking into account their confidentiality, integrity and admissibility.

The use of this algorithm allows for a detailed assessment of threats, as a result of which each information asset's threats of compromise in a separate form are divided into non-dimensional values of the probability of occurrence.

Based on this, it becomes possible to measure the value of damages. For this, the total average value of threats and the amount of hidden losses (damages) of each information asset are used. The loss value (L) is calculated by the following formula:

$L = R_{o'r} \cdot S$, (9)

here:

$R_{o'r}$– total average value of threats;

S – losses (losses), in conditional units.

The proposed method provides a high-precision assessment of threats to information security and the possibility of calculating economic losses in the event of security events (incidents). The KMO list of critical objects identified in the proposed analysis does not include traditional types of military objects - missile bases and ranges, air bases, high state and military administration bodies, because according to the researchers' assessment, these objects have a sufficiently high level of protection and cannot be used by ordinary weapons. is not considered vulnerable to its effects.

REFERENCES

1. Воронов К.В. Глобальная интерсистема: Эволюция, структура, перспективы / К. В. Воронов // Мировая экономика и международные отношения. - 2007. -№ 1. - с 18-19.
2. Бусыгина И.М. Политическая регионология / И.М. Бусыгина - М., 2006.–с 46-49.
3. Ахметьянова А.И., Кузнецова А.Р. Проблемы обеспечения информatsiонной безопасности в России и ее регионах // Фундаментальные исследования. – 2016. – № 8-1. – с 82-86;
4. Андреев О.О. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организatsiи противодействия `под ред. В.А.Васенина]. – М.: МЦНМ, 2008. – с 398.