The Information Security System Synthesis Using the Graphs Theory

V. N. Kustov, V. V. Yakovlev, T. L. Stankevich
Emperor Alexander I St. Petersburg State Transport University
St. Petersburg, Russia

***Abstract*—Timely prevention information security threats, provided by specialized software and hardware, is the effective business foundation, allowing to reduce reputational and financial risks for the company. At the same time, protection must be implemented in all detractors' possible attacks areas. If we turn to the Russian Federation leISSlation, then the FSTEC order №31 of March 14, 2014 may be adopted as the basis for "isolating" the protection vectors, according to which the basic measures for protection should be provided at the following levels: access subjects identification and authentication, access delineation, software restriction, computer storage media protection, etc. (There are 21 of them). On the hardware and software complex basis that implement protection at each of these levels, an enterprise information security system is created. To select the most appropriate software and hardware information security, and, therefore, to build an optimal enterprise information protection system, one can turn to graph theory. In this case, the problem is reduced to the ranked descending graph construction and the optimality problem solution, i.e. critical (maximal) path of this graph calculation. Each graph level corresponds to a specific subsystem of the information security system, while the subsystems are located in the alleged overcoming order protection by the attacker; tops - the considered information security tools; the graph is weighted, the each its arcs weight corresponds to the expert evaluation of the preference for using a particular tool.**

Keywords—optimality problem solution on the graph theory basis; graph critical path; information security system synthesis based on graph theory; enterprise information security

Timely prevention information security threats as well as prompt elimination realized threat consequences are the effective business bases. At the same time, protection must be implemented in all detractors possible attacks areas.

If we turn to the Russian Federation leISSlation, then the FSTEC order №31 of March 14, 2014 may be adopted as the basis for "isolating" the protection vectors, according to which the basic measures for protection should be provided at the following levels: access entities identification and authentication, access delimitation, software restriction, computer storage media protection, security events recording, antivirus protection, intrusion detection (prevention), information security monitoring, automated information management system integrity, technical means and information availability, the virtualization environment protection, hardware and equipment protection, automated system and its components protection, safe development and software management, software update management, information security planning, contingency actions provision, personnel information and training, information analysis and risks from their implementation, incident detection and response, automated system management configuration management and its protection system. Thus, the levels number on which protection from the internal and external attacker should be implemented is 21 or 21 subsystems of the information security system (ISS).

To select information security tools most appropriate (from the security required level position and available material capabilities), and, consequently, the optimal enterprise ISS construction, one can turn to graph theory. In this case, the problem is reduced to constructing a ranked descending graph and solving the optimization problem, i.e. this graph critical (maximal) path calculation. Each graph level corresponds to a ISS specific subsystem, while the subsystems are located in the protection alleged overcoming order by the attacker; vertices – information security means adopted for comparison; the graph is weighted, each its arcs weight corresponds to the preference for using a particular tool expert evaluation.

I. A THREAT MODEL AND INTRUDER MODEL DEVELOPMENT

As an ISS synthesis preparatory stage using graph theory, we distinguish threat model and intruder model development stages [1].

When intruder model developing, we should not forget that our main regulators information security field approaches, fixed in the documents (Methods) approved by them, differ in this issue. The Russia Federal Security Service (FSS) is responsible for cryptography field regulation, and the methodology approved by it describes the intruder in attacking crypto capabilities [2]. The Russia Federal Service for Technical and Export Control (FSTEC) [3] is broader and describes the offender's ability to attack the system as a whole.

The FSS and FSTEC approaches can be integrated as follows:

- low potential intruder under the FSTEC are intruder H1-H3 according to the FSS classification;
- average potential intruder under the FSTEC are intruder H4-H5 according to the FSS classification;
- high potential intruder under the FSTEC are intruder H6 according to the FSS classification.

978-1-5386-1810-3/17/$31.00 ©2017 IEEE

Further, based on information system class, we choose intruder type from which we need to defend ourselves.

If enterprise system is classified as a state information system, you should refer to clause 25 of FSTEC Order No 17 [4]:

- for security first class information systems – threats neutralization from the intruder with high potential;
- for security second class information systems – threats neutralization from the intruder with an average potential;
- for security third and fourth classes information systems – threats neutralization from the intruder with low potential.

In the event that the system does not fall into the state category, it is necessary to turn to Government Decision No. 1119 [5]:

- the first type threats are related to undeclared capabilities in system software presence – threats neutralization from the intruder with high potential;
- the second type threats are related to undeclared capabilities in system software presence – threats neutralization from the intruder with medium potential;
- the third type threats are related to undeclared capabilities in system software presence – threats neutralization from the intruder with low potential.

Within this stage, the enterprise information system initial security level (prior to the ISS implementation) is also determined, which is necessary to compile actual information security threats list (Table I).

TABLE I. INITIAL SECURITY LEVEL DETERMINATION

Technical and operational characteristics	Security Level
Location	Low / Medium / High
Information system technical means location concerning controlled zone boundaries	Low / Medium / High
Connection presence with other information systems	Low / Medium / High
Connection presence to the Internet	Low / Medium / High
Built-in (legal) operations with database records	Low / Medium / High
On the information processing mode	Low / Medium / High
Access availability to information	Low / Medium / High
Access nature to information	Low / Medium / High
According to applied software nature for processing information	Low / Medium / High

The protection initial degree is defined as follows:

1. The information system has initial security high level, if at least 70% characteristics correspond to the "high" level (positive decisions on the second column corresponding to the high level security are summarized), and the rest to the average security level (positive decisions for the third column).

2. The information system has initial security an average level if the conditions for item 1 are not met and at least 70% characteristics correspond to a level not lower than "average" (the positive decisions sum ratio for the third column corresponding to the average security level to the decisions total number is taken), and the rest – a low security level.

3. The information system has a low initial security degree if the conditions for items 1 and 2 are not met.

When compiling each degree of initial security actual security threats in the information system list, a numerical coefficient (Y1) is put in correspondence, namely:

0 – for initial security a high degree;

5 – for initial security an average degree;

10 – for initial security a low degree.

The threat realization probability is understood as an expertly determined indicator characterizing how probable is the specific threat implementation to information security for the enterprise information system in the emerging conditions.

The numerical coefficient (Y2) for assessing threat occurrence probability is determined by 4 verbal gradations this indicator:

- unlikely – there are no objective prerequisites for the threat implementation (Y2 = 0);
- low probability – objective prerequisites for the threat implementation exist, but the measures taken make it very difficult to implement it (Y2 = 2);
- average probability – objective prerequisites for the threat implementation exist, but the security measures taken are insufficient (Y2 = 5);
- high probability – objective prerequisites for the threat implementation exist and security measures are not taken (Y2 = 10).

Based on the security level evaluation (Y1) and the threat probability (Y2), the threat realizability factor (Y) is calculated and the threat realization possibility is determined. The threat realizability factor Y will be determined by the relation $Y = (Y_1 + Y_2)/20$.

The information security threat danger assessment is based on expert judgment and is determined by a verbal hazard indicator that has three meanings:

- low risk – if the threat implementation can lead to minor negative consequences;
- medium danger – if the threat implementation can lead to negative consequences;
- high danger – if the threat implementation can lead to significant negative consequences.

In accordance with the assigning rules a security threat to the actual (Table II), the enterprise's information system determines the actual and irrelevant threats.

TABLE II. RULES FOR DETERMINING THE THREAT URGENCY

Threats realization possibility	Threat indicator		
	Low	*Medium*	*High*
Low	Irrelevant	Irrelevant	Actual
Medium	Irrelevant	Actual	Actual
High	Actual	Actual	Actual
Very high	Actual	Actual	Actual

Having defined information system category and class, having threat and intruder models, knowing levels list (subsystems) on which it is necessary to provide protection from an attacker, you can proceed to the software, hardware and firmware market analysis, and choose from the whole variety of optimal just for us for price, quality and functionality.

II. SOFTWARE AND HARDWARE SELECTION FOR EACH ISS SUBSYSTEM

As it was previously determined, information protection should be implemented at 21 level, while the levels are located in the protection alleged overcoming order by the attacker. Protection at each level is provided by a specific tool, which in turn is the future ranked downward graph vertex.

Based on the requirements for the functions assigned to a particular device, as well as the material enterprise capabilities, the expert chooses the funds presented on the market, determining the priority in using one or the other. The priority will correspond to the arc weight.

Thus, we have constructed a ranked top-down graph in which the vertices are expert information security tools located at a specific level (subsystem), which in turn are systematized in the attacker's protection alleged violation order, and the vertices are connected by arcs, the weight of each is determined by priority in the transition to this vertex (Fig. 1).

The weighting factors assigned to the arcs can be the following (given as an example, the values can be changed, the list expanded or shortened):

2 – low integration priority into the information system;

4 – average integration priority into the information system;

6 – high integration priority into the information system;

1 – the arc performs the service function (for example, the transition from one ISS subsystem to the next one behind it).

III. DETERMINING THE CRITICAL PATH OF A GRAPH

According to the constructed graph, the critical path with the all arcs weights maximum total value is calculated when following from the initial graph (source) vertex to the final (sink). This critical path will correspond to the optimal enterprise ISS.

In turn, the critical path calculating process can be automated by developing a simple computational software module.

IV. CONCLUSION

The proposed approach to the enterprise ISS synthesis is labor-intensive and requires the high-quality experts involvement, but such detailed planning and forecasting will help to avoid unnecessary material waste in today's and significant financial losses in the event of a future information security threat.

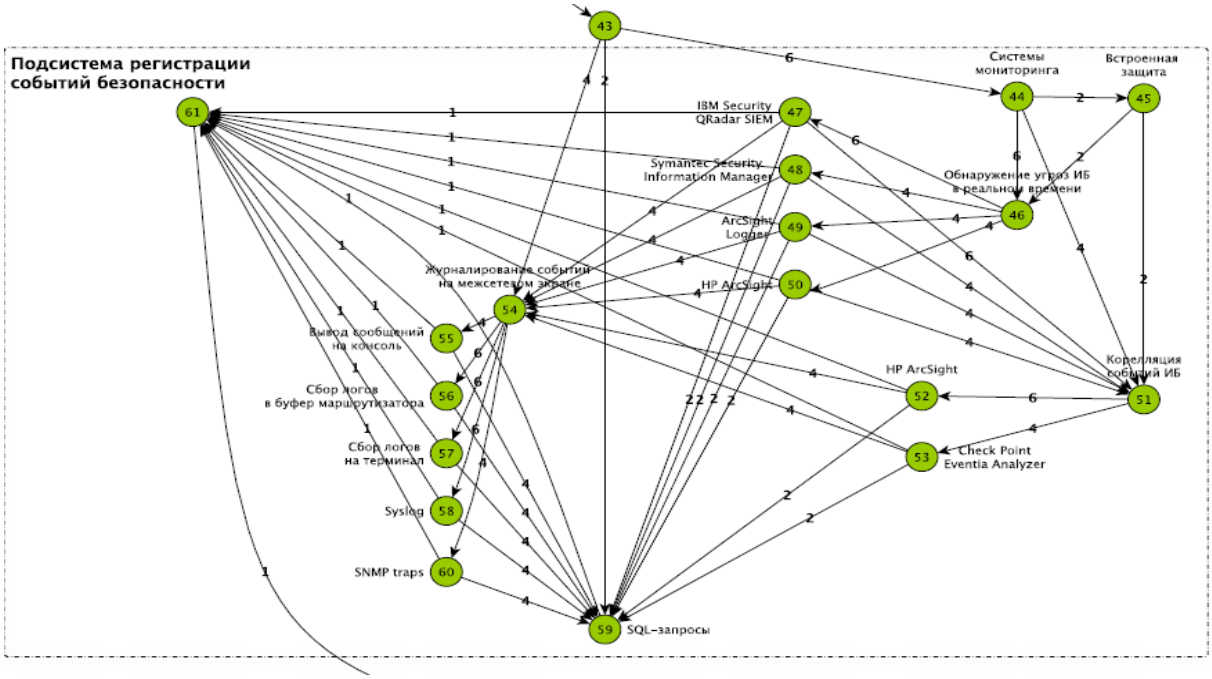

Fig. 1. The ranked descending graph level corresponding to the security events reISStration subsystem

REFERENCES

[1] The threats basic model to the personal data security when processing them in personal data information systems (extract): officer.text. Moscow: FSTEC of Russia, 2008. 69p

[2] Methodological recommendations for the regulatory legal acts development that determine threats to the personal data relevant security to the personal data processing in personal data information systems operated in the relevant activities conduct, approved 8 Center Russia FSS management on March 31, 2015 No. 149/7/2 / 6-432. Moscow .: 2015. 22p.

[3] Identifying threats methodology to information security in information systems (Project). Moscow: Russia FSTEC, 2015. 43p.

[4] The Russia FSTEC order dated February 11, 2013. № 17 “On the requirements approval for the information security that is not a state secret, contained in government information systems” [Electronic resource]. - Access mode: http://fstec.ru (circulation date 07/04/2017).

[5] Russian Government Resolution No. 1119 dated 01.11.2012 "On approving the requirements for the personal data protection when processing them in personal data information systems" [Electronic resource]. - Access mode: http://consultant.ru (circulation date 07/04/2017).