European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.03.60

FETDE 2020

International Conference on Finance, Entrepreneurship and Technologies in Digital Economy

AN OPTIMAL SET OF INFORMATION SECURITY TOOLS

Sergey Olegovich Ivanov (a)*, Dmitry Vladimirovich Ilyin (b), Larisa Alekseevna Ilyina (c)
*Corresponding author

(a) I. N. Ulianov Chuvash State University, Russia, Cheboksary, v101-11@mail.ru
(b) I. N. Ulianov Chuvash State University, Russia, Cheboksary, destr@mail.ru
(c) I. N. Ulianov Chuvash State University, Russia, Cheboksary, larisai2009@gmail.com

Abstract

The article presents an approach to choose an effective information security system, taking into account the current threats and requirements in the last two years. Statistics on vulnerabilities, threats, and security tools for 2018-2019 from Russian and foreign sources are gathered. For the main categories of threats, a table is presented with evaluation of their relevance, implementation capabilities due to vulnerabilities, and the amount of approximate damage is also provided. The leading products are selected among the various means of information security tools. The evaluation of approximate cost of each product and its impact on various aspects of the threat is made. The assessment methods for information security systems are considered on the security level as the value of possible damage reduction, on the total average annual cost of used funds, and their effectiveness through investment return (ROSI). The indicators for various security systems are calculated using the obtained data and evaluation methods. Data on the certain information security tools and one of the best combinations are presented. The obtained results are used to compare and justify the choice of information security system that meets modern requirements and can change depending on the activity specifics of the organization. The method of efficiency calculation is described, and the results obtained for various security systems are evaluated. Conclusions on the composition of security systems that meet modern requirements are made.

Keywords: Information security tools, information security threats, system vulnerabilities, organization security, cost-effectiveness assessment, return on security investment (ROSI)

https://doi.org/10.15405/epsbs.2021.03.60
Corresponding Author: Sergey Olegovich Ivanov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

At present, the choice of information security tools (IST) is an urgent problem. For Russian organizations, it must meet the requirements of the FSS and FSTEC, the recommendations of information security (IS) standards and provide protection against current threats. There is an official list of documents that IST must meet in our country as well as abroad, and their implementation is not a big problem. As for the current list of threats, such information can be obtained from various analytical reports and expert reviews, which are regularly updated. An information security specialist has to analyse the current state of threats by comparing and combining a lot of data which may differ in qualitative characteristics. Consider the possible composition of the information security system of an organization, taking into account threats and incidents over the last two years. The available incident statistics is used to determine the optimal set of IST for an organization.

2. Information Security Incident Statistics

At present, the choice of information security tools is an urgent problem. For Russian organizations, it must meet the requirements of the FSS and FSTEC, the recommendations of information security standards and provide protection against current threats. There is an official list of documents that IST must meet in our country as well as abroad, and their implementation is not a big problem. As for the current list of threats, such information can be obtained from various analytical reports: Cisco information security report for 2018 (2018), Is cybersecurity about more than protection?..., (2019), Common Weakness Enumeration (2020), Data bank of information security threats of the FAA, GNII PTZI FSTEC of Russia (2020), Vulnerabilities, Infographics. Data bank of information security threats (2020) and expert reviews: Bissell et al. (2019), Sobers (2019), Chebyshev et al. (2019), Zangre (2019), which are regularly updated. An information security specialist has to analyse the current state of threats by comparing and combining a lot of data which may differ in qualitative characteristics. Consider the possible composition of the information security system of an organization, taking into account threats and incidents over the last two years. The available incident statistics is used to determine the optimal set of IST for an organization.

Table 1. Information security threats

№	Name of threat	Relevance	Vulnerability	Approximate damage, million rubles
	Malicious programs	0,21	0,10	169
	Cryptographers and wipers	0,14	0,07	46
	DDoS-attack, Cyber attacks (to disorganise activity)	0,10	0,07	111
	Unauthorized access to information	0,09	0,19	65
	Outflow of confidential data, Cyber attacks (to steal an intellectual property)	0,15	0,18	91
	Cryptocurrency mining, Fraud	0,07	0,04	26
	Data loss (not Cryptographers)	0,02	0,07	91
	Hacking of web resources	0,08	0,13	145
	Phishing	0,10	0,07	91
	Internal attacks	0,02	0,09	104

https://doi.org/10.15405/epsbs.2021.03.60
Corresponding Author: Sergey Olegovich Ivanov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

3. Protection Means for IS

The market currently presents IST offering a variety of features to protect against cyber threats. According to the protection purposes, they can be divided into categories when each of them has lead products used for certain threats. From the materials of the research by «Anti-Malware.ru», we select popular brands (Table 2) (Shabanov, 2019a,b), supplemented with data on the approximate cost of the selected product and its impact on various aspects of the threat. The influence of security tools on relevance, vulnerability and damage is indicated by numbers (the threat number is taken from Table 1), where «1» and «0» indicate that the presented measure provides protection for three aspects of the risk.

Table 2. Information security tools

Category	Protection measures	Cost of IST	Protection
Malware protection	Kaspersky Lab (leader), Dr.Web, ESET, Avast and Microsoft.	Kaspersky Endpoint Security standard: 20000 rubles/year	1: 0,0,0 2: 0,1,0
Network perimeter protection	Cisco (leader), Check Point, Fortinet, Palo Alto Networks, Microsoft; «InfoTeCS», «Security code», «Factor-TS» products are mentioned.	Cisco ASA 5500-X: 25000 rubles	3: 0,1,1 5: 1,0,1
Protection against targeted attacks	Kaspersky Lab (leader) and Trend Micro. Check Point, Palo Alto Networks, Cisco and Microsoft are singly mentioned.	Kaspersky Anti Targeted Attack Platform Advanced Russian Edition: 10000000 rubles/year	4: 1,0,0 5: 1,1,0 9: 1,0,0 10: 1,0,0
Protection against DDoS-attacks	Qrator Labs, Kaspersky Lab, Cloudflare, Cisco, Check Point	QRATOR SMB 1Gb/s: 19000 rubles/month Kaspersky DDoS Prevention, Basic Level Russian Edition. 1-Resource 1 year Renewal License: 580 644,78 rubles/year	3: 1,0,0 3: 1,0,0
Security analysis tools	Positive Technologies (leader), Nessus, «Scanner-BC» from the NGO «Echelon», singly Qualys, Rapid7 and products of open sourse.	XSpider 7.8, license for 4 hosts, warranty for 1 year: 14000 rubles/year	4: 1,0,1 5: 1,0,1 8: 1,0,1
Account management system (IDM/IGA)	Microsoft (leader), «Outpost», One Identity, Blitz.	Microsoft AD (included in OS, at the price of Microsoft Windows Server 2012 x64 Standard 2CPU / 2VM): 50000 rubles	4: 0,1,1 10: 0,1,1
Outflow protection (DLP)	Rostelecom-Solar, «SearchInform», InfoWatch, Zecurion, «Garda Technologies», Falcongaze and Kaspersky Lab.	CIC SearchInform: 187750 rubles	5: 0,0,1
Protecting web resources from hacking (WAF)	Positive Technologies, Wallarm.	Software Positive Tecnologies Application Firewall: 750 000 rubles Qrator Wallarm (Web Application Firewall): 30000 rubles/month	8: 0,0,1 8: 0,0,1
Event monitoring and incident analysis system (SIEM)	IBM, Micro Focus (previously HPE) and «Echelon». Positive Technologies, Splunk, McAfee, AlienVault and NeuroDAT are singly mentioned.	MaxPatrol SIEM MPX-SIEM-Base-H1000-EXT: 3 000 000 rubles	4: 1,1,0 5: 1,1,0 6: 0,1,1 9: 1,0,0 10: 0,0,1
Management system of IS	Self-developed systems	Course on Information security management system: 35 000 rubles	4: 1,0,1 5: 1,0,1 6: 0,1,1 7: 0,1,0 9: 0,0,1 10: 0,0,0

https://doi.org/10.15405/epsbs.2021.03.60
Corresponding Author: Sergey Olegovich Ivanov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

4. Evaluation of economic efficiency of the security system

The obtained data can be used to calculate possible damage to the organization, taking into account the used information security tools (Ivanov et al., 2015). The obtained values will be superficial but can be used for ranking and comparing of information security systems while choosing.

The main indicator of information security is a reduction of damage due to protective measures. In general case, the protection indicator (3) can be determined:

$$Z = U_0 - U, \quad (1)$$

where U_0 is an expected damage in the absence of security tools, U is a value of damage, taking into account the impact of security tools.

For calculation of the cost of a security system consisting of n funds:

$$C = \sum IST_i.C, i = 1..n, \quad (2)$$

where $IST_i.C$ is a cost per year of the i-th security tool.

For security tools purchased once, their value should be divided along the depreciation period of 5 years. For evaluation of efficiency, we use the ROSI coefficient (Biryukov, 2012; Piskunov, 2013), which determines the time it takes to return the investments. The ROSI value is calculated by the formula:

$$ROSI = (Z - C) / C, \quad (3)$$

where C is a cost of a security system for the period (a year), Z is a value of damage reduction due to protective measures.

5. Evaluation results of the sets of security tools

Using Tables 1 and 2, we research the various configurations of security systems consisting of various sets of IST. $2^{12} = 4096$ combinations are obtained in total.

Supposing that vulnerability and damage are completely eliminated, and the relevance decreases by 2 times while using the protective measures, we get the formula to calculate the damage to the **security** system consisting of a combination of protective measures k:

$$U_k = \sum(Threat_i.A * 0,5\ IST_i.A * Threat_i.У * IST_i.U) * Threat_i.П * IST_i.P, i = 1..10$$

where the $Threat_i.A$, $Threat_i.U$, $Threat_i.P$ are relevance, vulnerability, and damage from the threat i,

$IST_i.A$, $IST_i.U$, $IST_i.P$ are reduction, prevention and compensation of an incident of the threat i.

The version when protective measures are not used at all, determines the initial possible damage necessary to value the loss reduction – U_0.

Maximum possible damage is 5 478 970,88 **rubles**.

Using the formulas (1-3), we calculate the indicators for the certain *IST* (Table 3).

https://doi.org/10.15405/epsbs.2021.03.60
Corresponding Author: Sergey Olegovich Ivanov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Table 3. Indicators for the certain security tools

Combination	Security system	Protection, rubles	Cost, rubles	ROSI
1	Kaspersky Endpoint security	1 965 478,36	20 001,00	97,27
2	Cisco ASA5505-K8	1 436 025,66	5 001,00	286,15
4	Kaspersky ATA	2 245 545,60	10 000 001,00	-0,78
8	QRATOR SMB	397 641,70	228 001,00	0,74
16	Kaspersky DDoS Prevention	397 641,70	580 001,00	-0,31
32	Xspider	2 583 531,06	14 001,00	183,52
64	Microsoft AD	345 950,24	10 001,00	33,59
128	KiB SearchInform	1 237 204,81	37 551,00	31,95
256	PT WAF	757 389,57	750 001,00	0,01
512	Qrator Wallarm	757 389,57	360 001,00	1,10
1024	MaxPatrol SIEM	2 263 408,45	600 001,00	2,77
2048	ISMS Course	2 340 598,38	35 001,00	65,87

Taking into account the protection value, the best result on the ROSI coefficient is provided by the combination: XSpider, Cisco ASA5505-K8, Kaspersky Endpoint security (35) – 120,74. Low effectiveness of a system: MaxPatrol SIEM and Kaspersky ATA, indicates that they perform similar tasks, but from different sides.

Taking into account the ROSI coefficient, the best result on protection value is shown by the combination: ISMS Course, XSpider, QRATOR SMB, Kaspersky Endpoint security (2089) – 17,39. Providing maximum reduction of damage, the most expensive IST have a negative ROSI coefficient at the same time, so they are redundant and unprofitable. The firewall and vulnerability scanner provide the maximum efficiency, which is confirmed by the fact that the world wide web is the most dangerous.

6. Conclusion

As a result of the analysis of information security tools, the following conclusions are made: the use of a firewall, antiviruses and regular training of staff on information security are effective, they have the highest efficiency at providing with information security, and they have to be completed with a vulnerability scanner taking into account the current threats for the recent years. A certain organization can require the additional security measures which are determined by the relevant threats, due to the specifics and potential damage.

References

Biryukov, A. A. (2012). Okupayemost' IB-sistem. Kakuyu pribyl' mozhet prinesti sistema ib. [Payback of IS-systems. What profit can the IS-system bring]. System administrator. http://samag.ru/blog/art/No_number/16

Bissell, K., LaSalle, A., Ryan, M., & Cin, P. D. (2019). The cost of cybercrime: Ninth annual cost of cybercrime study unlocking the value of improved cybersecurity protection. Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Chebyshev, V., Sinitsyn, F., Parinov, D., Larin, B., Kupreev, O., & Lopatin, E. (2019). Razvitiye informatsionnykh ugroz v pervom kvartale 2019 goda. Statistika [The development of information threats in the first quarter of 2019, Statistics]. (2019). https://securelist.ru/it-threat-evolution-q1-2019-statistics/94021

Cisco information security report for 2018. (2018). CISCO. https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf

Common Weakness Enumeration. (2020). https://cwe.mitre.org

Data bank of information security threats of the FAA, GNII PTZI FSTEC of Russia. (2020). https://bdu.fstec.ru

Is cybersecurity about more than protection? EY international research on information security, 2018-2019. (2019). Ernst & Young (CIS) B.V. https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf

Ivanov, S. O., Ilyin, D. V., & Ilina, L. A. (2015). Metodika analiza riska s ispol'zovaniyem modeli posledstviy [Methods of risk analysis using the consequences model]. *Vestnik of the Chuvash University, 3,* 149-153.

Piskunov, I. (2013). Planirovaniye zatrat na informatsionnuyu bezopasnost' [Information Security Cost Planning]. https://www.anti-malware.ru/analytics/Technology_Analysis/economic_planning#part4

Shabanov, I. (2019a). Analiz rynka informatsionnoy bezopasnosti v Rossii. Chast' 2. [Analysis of the information security market in Russia, Part 2]. Anti-Malware.ru. https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-2

Shabanov, I. (2019b). Analiz rynka informatsionnoy bezopasnosti v Rossii. Chast' 4. [Analysis of the information security market in Russia, Part 4]. Anti-Malware.ru. https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-4

Sobers, R. (2019). 60 Must-Know Cybersecurity Statistics for 2019. https://www.varonis.com/blog/cybersecurity-statistics

Vulnerabilities, Infographics. Data bank of information security threats. (2020). https://bdu.fstec.ru/charts

Zangre, A. (2019). *50 Noteworthy Cybercrime Statistics in 2019.* https://learn.g2crowd.com/cybercrime-statistics