საინფორმაციო-საკომუნიკაციო სისტემებში ინფორმაციის ვირუსული შეტევებისგან დაცვის შეფასების არსებული კონცეფციების ანალიზი

გიორგი კოხრეიძე
ეროვნული თავდაცვის აკადემიის ინფორმატიკის მიმართულების აფელირებული ასისტენტ-პროფესორი

აბსტრაქტი

საინფორმაციო-საკომუნიკაციო სისტემებში ვირუსული შეტევებისგან დაცვის მეთოდების მახასიათებლების ანალიზი და ანტივირუსული სისტემების სრულყოფის განვითარების მიმართულება იძლევა საშუალებას ითქვას, რომ ინფორმაციული უსაფრთხოების საფრთხეების, მათ შორის ვირუსული შეტევებისგან მომდინარე საფრთხეებთან დაკავშირებული ინფორმაციული ობიექტების დაცვის შეფასების მეთოდები, რომლებიც დღესდღეობით ინფორმაციული უსაფრთხოების მეთოდოლოგიაში წარმოიშვა, სამი ძირითადი კონცეფციის ფარგლებში ხორციელდება:

- **კონცეფცია, რომელიც ეფუძნება ვირუსული შეტევებისგან ინფორმაციის დაცვის უზრუნველსაყოფის შესაძლებლობების შეფასებას, რომელიც მოითხოვს არაავტორიზებული დაშვებისგან ინფორმაციის დაცვის მარეგულირებელი დოკუმენტის მოთხოვნებთან შეესაბამისობას.**
- **კონცეფცია, რომელიც ეფუძნება ინფორმაციული ინფრასტრუქტურის საკვანძო ობიექტებში ინფორმაციის უსაფრთხოების საფრთხეების აქტუალურობის შეფასებას.**
- **კონცეფცია, რომელიც ეფუძნება მოვლენების ალბათური განვითარების შეფასებას, რომელიც ასახავს ანტივირუსული დაცვის სისტემების მიერ ინფორმაციულ სისტემაზე ვირუსული შეტევებისას რეაგირების დინამიკას.**

ნაშრომში განხილულია არესბული კონცეფციების მოდელები და წარმოჩენილია სსს-ის ინფორმაციული რესურსების ვირუსული შეტევებისგან დაცვის საშუალებების მახასიათებლების მეთოდური აპარატის აუცილებელობა.

საკვანძო სიტყვები: საინფორმაციო-საკომუნიკაციო სისტემები, ვირუსული შეტევები, დაცვის სისტემები, ინფორმაციული ობიექტების დაცვის შეფასების მეთოდები

Analysis of existing concepts of assessment of information protection against viral attacks in information-communication systems

Giorgi Kokhreidze
Assistant Professor of Informatics at the
National Defense Academy

Abstract

Analysis of the characteristics of methods of protection against virus attacks in information and communication systems and the development of antivirus systems allow to say that methods of assessing information security threats, including threats from virus attacks, are currently the main information. Within the framework of the concept:

- A concept based on the assessment of the ability to provide information protection against virus attacks, which requires compliance with the requirements of the document regulating the protection of information from unauthorized access.
- A concept based on the assessment of the urgency of information security threats in key objects of information infrastructure.
- A concept based on the assessment of the probable development of events that reflects the dynamics of response to viral attacks on an information system by antivirus protection systems.

The paper discusses the models of concepts and demonstrates the need for a methodological apparatus for the characteristics of the means of protection of information resources from virus attacks.

Key words: Information and Communication Systems, Virus Attacks, Security Systems, Information Object Protection Assessment Methods

საინფორმაციო-საკომუნიკაციო სისტემებში (სსს) ვირუსული შეტევებისგან დაცვის მეთოდების მახასიათებლების ანალიზი და ანტივირუსული სისტემების სრულყოფის განვითარების მიმართულება იძლევა საშუალებას ითქვას, რომ ინფორმაციული უსაფრთხოების საფრთხეების, მათ შორის ვირუსული შეტევებისგან მომდინარე საფრთხეებთან დაკავშირებული ინფორმაციული ობიექტების დაცვის შეფასების მეთოდები, რომლებიც დღესდღეობით ინფორმაციული უსაფრთხოების მეთოდოლოგიაში წარმოიშვა, სამი ძირითადი კონცეფციის ფარგლებში ხორციელდება[1]:

კონცეფცია, რომელიც ეფუძნება ვირუსული შეტევებისგან ინფორმაციის დაცვის უზრუნველსაყოფის შესაძლებლობების შეფასებას, რომელიც მოითხოვს არაავტორიზებული დაშვებისგან ინფორმაციის დაცვის მარეგულირებელი დოკუმენტის მოთხოვნებთან შეესაბამისობას.

კონცეფცია, რომელიც ეფუძნება ინფორმაციული ინფრასტრუქტურის საკვანძო ობიექტებში ინფორმაციის უსაფრთხოების საფრთხეების აქტუალურობის შეფასებას.

კონცეფცია, რომელიც ეფუძნება მოვლენების ალბათური განვითარების შეფასებას, რომელიც ასახავს ანტივირუსული დაცვის სისტემების (ადს) მიერ ინფორმაციულ სისტემაზე ვირუსული შეტევებისას მასზე რეაგირების დინამიკას.

პირველი კონცეფცია გულისხმობს შეფასდეს გამოყენებული ანტივირუსული საშუალებების ვირუსული შეტევების წინააღმდეგ უსაფრთხოების ეფექტურობა, ანტივირუსული საშუალების სერტიფიკატის საფუძველზე.

დაცვის სისტემების ინფორმაციის დაცვის გაცხადებული შესაძლებლობების არასანქცირებული წვდომების კლასებთან შესაბამისობის ძირითად მახასიათებლად მიღებულია ანტივირუსული დაცვის საშუალებების შესაძლებლობები. თუკი გაცხადებული ფუნქციიდან ერთ-ერთი მაინც არ მუშაობს მაშინ ადს ითვლება არაფექტურად.

მეორე კონცეფცია ეფუძნება სახელმწიფოს ტექნიკური კონტროლის დებულებების დოკუმენტებს, რომლებიც აღწერს ინფორმაციული ინფრასტრუქტურის საკვანძო ობიექტებში ინფორმაციული უსაფრთხოების საფრთხეების მოდელებს და მათი აქტუალურობის დადგენის პროცედურებს. კონცეფციის არსი მდგომარეობს ინფორმაციის საფრთხის წყაროსა და მის მოწყვლადობას ასეთის სახის საფრთხეების მიმართ და მათ შორის ურთიერთკავშირის დადგენასა და შეფასებაში[2]. შესაბამისი მეთოდების რეალიზაციისთვის გამოიყენება ექსპერიმენტები რომელთა არსიც მდგომარეობს შემდეგში:

- საფრთხეების წყაროების აღმოჩენა
- სსს-ის მოწყვლადობების აღმოჩენა რომლებიც ხელს უწყობენ საფრთხის რეალიზებას.
- საფრთხის წყაროსა და სისტემის უსაფრთხოების მოწყვლადობას შორის კავშირის აღმოჩენა.
- სისტემის მოწყვალდაბოსა და მის საფრთხეებს შორის კავშირის აღმოჩენა.

წარმოშობის მახასიათებლები	**წყარო**
სსს-ში გაწთავსებული ინფორმაციისადმი ჰაკერების ინტერესი	ჰაკერები
სადას დაკავშირებული ისეთი სუბიექტების არსებობა რომლებიც უკმაყოფილო არიან სამუშაო პირობებით, ხელფასით აწ ემუქრებათ განთავისუფლება	სსს თანამდებობის პირები
სსს ისეთი თანამდებობის პირები რომლებიც თვითნებურად ახორციელებენ მის ტექნიკურ მომსახურეობას	
სსს ისეთი თანამდებობის პირები რომელთაც შეუძლიათ შექმნან ინფორმაციის დაცვითი მექანიზმების გატმტეხავი პროგრამული საშუალებები	
სსს თანამდებობის პირებისთვის სამუშაო კომპიტერებზე პროგრამული უზრუნველყოფის თვითნებურად დაყენების უფლების შესაძლებლობა	
სსს-ში არასერტიფიცირებული პროგრამული უზრუნველყოფის გამოყენება	სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრ. უზრუნ. მწარმოებლები
გარე ორგანიზაციების მიერ სსს-ის ტექნიკური მომსახურება	

ცხრილი 1 ექსპერტ-სპეციალისტების მოსაზრებები რომლებიც ასახავენ ვირუსული საფრთხეების წყაროებს და მათი წარმოშობის შასაბამისობას.

1 Written by Eric Knight, C.I.S.S.P.; Last Revision: March 9, 2000 Original Publication: March 6, 2000; Computer Vulnerabilities Abdulrahaman OkinoOtuoze; Mohd WazirMustafa; Journal of Electrical Systems and Information Technology, December 2018, Smart grids security challenges: Classification by sources of threats;

2 U.S. Department of Commerce Carlos M. Gutierrez, Secretary National Institute of Standards and Technology Dr. Patrick D. Gallagher, Deputy Director; September 2008; Technical Guide to Information Security Testing and Assessment;

ამ კონცეფციაში ვირუსული შეტევების საფრთხეების წყაროების გამოვლენა ხდება ასეთი ტიპის წყაროებისა და მათი წარმოშობის მახასიათებლების იმპირიული შესაბამისობის განსაზღვრით.

სსს-ში მოწყვლადობების აღმოჩენა ხორციელდება ვირუსის შეტევების საფრთხეების და მათი გამოვლენის ნიშნებს შორის შესაბამისობის ემპირიული განსაზღვრით. ცხრილ 2-ში სისტემატიზირებული სახით მოცემულია მოსაზრებები რომლებშიც ასახულია მავნე პროგრამების კავშირი სსს-ის მოწყვლადობზე.

მოყვლადობის წყარო	მოწყვლადობა	პირობითი აღნიშვნა
კომპიუტერული ტექნიკა	ინფორმაციის შეტანის მოწყობილობების დრაივერები	VM_1
	ინფორმაციის გამოტანი მოწუბილობების დრაივერები	VM_2
	ინფორმაციის დამმუშავებელი მოწყობილობების დრაივერები	VM_3
	BIOS ის მიკროსქემების დრაივერები	VM_4
თავისუფალი ფიზიკური დაშვებების მქონე სერვერები	სსს-ის თავისუფალი ფიზიკური დაშვებების მქონე სერვერების პროგრამული უზრუნველყოფა	VM_5
კომუნიკაციო საშუალებები თავისუფალი ფიზიკური წვდომით	კომუნიკაციო საშუალებების პროგრამული უზრუნველყოფა	VM_6
სსს-ის მოწყობილობების კაბელები	სსს-ის მოწყობილობების კაბელები ის მონაკვეთების სადაც მათზე შესაძლებელია ფიზიკური წვდომა	VM_7
ქსელთაშორისი ურთიერთკავშირის სერვისები	TCP/IP პროტოკლების სტეკები	VM_8
	ინტერნეტში გამავალი gateway	VM_9
	ქსელთაშორისი ურთიერთკავშირის გამოყენებითი დონის პროტოკოლები	VM_{10}
	ქსელთაშორისი ურთიერთკავშირის არადოკუმენტირებული კვანძები	VM_{11}
საერთო მოხმარებისთვის დაყენებული ღია ქსელური რესურსები	საერთო ღია ქსელური რესურსები	VM_{12}
არასერთიფიცირებული პროგრამული უზრუნველყოფების გამოყენება	პროგრამული უზრუნველყოფის არასერთიფიცირებული კომპონენტები	VM_{13}
ინტერნეტის ძირითადი სერვისების გამოყენება	ელექტრონული ფოსტა	VM_{14}
	Web ბრაუზერი	VM_{15}

ცხრილი 2. მავნე პროგრამების კავშირი სსს-ის მოწყვლადობზე და მათზე მინიჭებული პირობითი აღნიშვნები (VM).

სსს-ის მოწყვლადობების მავნე პროგრამებისადმი რაოდენობრივი მახასიათებლების განსაზღვრა - ხელსაყრელი პირობების ალბათური არსებობის განსაზღვრა მისი ვირუსული შეტევების საფრთხის კუთხით ხორციელდება დარგის სპეციალისტების მიერ ანკეტირების გზით. ცხრილ 3-ში სისტემატიზირებული სახით მოცემულია ზემოაღნიშნული მახასიათებლებზე მოსაზრებები და მათზე მინიჭებული პირობითი აღნიშვნები[1].

1 Paul Rebstock, NRC Program Manager,U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Division of Engineering, Digital Instrumentation & Control Branch, Washington; January 27, 2012; Cyber Security Assessment Tools and Methodologies for the Evaluation of Secure Network Design at Nuclear Power Plants

მოწყვლადობის იდენტიფიკატორი	საფრთხის წყაროს იდენტიფიკატორი	კითხვა	პასუხი	პირობის არსებობის ალბათობა
VM1	A1	არის თუ არა მოწყვლადობა ხელმისაწვდომი ჰაკერებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{1,1}^{(VM)}$
	A2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის		$p_{1,2}^{(VM)}$
	A3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{1,3}^{(VM)}$
VM2	A1	არის თუ არა მოწყვლადობა ხელმისაწვდომი ჰაკერებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{2,1}^{(VM)}$
	A2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის		$p_{2,2}^{(VM)}$
	A3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{2,3}^{(VM)}$
VM3	A1	არის თუ არა მოწყვლადობა ხელმისაწვდომი ჰაკერებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{3,1}^{(VM)}$
	A2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის		$p_{3,2}^{(VM)}$
	A3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{3,3}^{(VM)}$
VM4	A1	VM4 მოწყვლადობა ვერ იქნაბა რეალიზებული როგორც A1 ვირუსული შეტევის საფრთხის წყარო		
	A2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{4,2}^{(VM)}$
	A3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{4,2}^{(VM)}$
VM5	A1	არის თუ არა მოწყვლადობა ხელმისაწვდომი ჰაკერებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{5,1}^{(VM)}$
	A2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის		$p_{5,2}^{(VM)}$
	A3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{5,3}^{(VM)}$
VM6	A1	არის თუ არა მოწყვლადობა ხელმისაწვდომი ჰაკერებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{6,1}^{(VM)}$
	A2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის		$p_{6,2}^{(VM)}$
	A3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{6,3}^{(VM)}$
VM7	A1	არის თუ არა მოწყვლადობა ხელმისაწვდომი ჰაკერებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$Pp_{7,1}^{(VM)}$
	A2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის		$p_{7,2}^{(VM)}$
	A3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{7,3}^{(VM)}$
VM8	A1	VM8 მოწყვლადობა ვერ იქნაბა რეალიზებული როგორც A1 ვირუსული შეტევის საფრთხის წყარო		
	A2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის	დიახ;	$p_{8,2}^{(VM)}$

მოწყვლადობის იდენტიფიკატორი	საფრთხის წყაროს იდენტიფიკატორი	კითხვა	პასუხი	პირობის არსებობის ალბათობა
	A_3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის	სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{8,3}^{(VM)}$
VM_9	A_1	VM_9 მოწყვლადობა ვერ იქნება რეალიზებული როგორც A_1 ვირუსული შეტევის საფრთხის წყარო		
	A_2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{9,2}^{(VM)}$
	A_3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{9,3}^{(VM)}$
VM_{10}	A_1	VM_{10} მოწყვლადობა ვერ იქნება რეალიზებული როგორც A_1 ვირუსული შეტევის საფრთხის წყარო		
	A_2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{10,2}^{(VM)}$
	A_3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{10,3}^{(VM)}$
VM_{11}	A_1	VM_{11} მოწყვლადობა ვერ იქნება რეალიზებული როგორც A_1 ვირუსული შეტევის საფრთხის წყარო		
	A_2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{11,2}^{(VM)}$
	A_3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{11,3}^{(VM)}$
VM_{12}	A_1	VM_{12} მოწყვლადობა ვერ იქნება რეალიზებული როგორც A_1 ვირუსული შეტევის საფრთხის წყარო		
	A_2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{12,2}^{(VM)}$
	A_3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{12,3}^{(VM)}$
VM_{13}	A_1	VM_{13} მოწყვლადობა ვერ იქნება რეალიზებული როგორც A_1 ვირუსული შეტევის საფრთხის წყარო		
	A_2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{13,2}^{(VM)}$
	A_3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{13,3}^{(VM)}$
VM_{14}	A_1	არის თუ არა მოწყვლადობა ხელმისაწვდომი ჰაკერებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{14,1}^{(VM)}$
	A_2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის		$p_{14,2}^{(VM)}$
	A_3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{14,3}^{(VM)}$
VM_{15}	A_1	არის თუ არა მოწყვლადობა ხელმისაწვდომი ჰაკერებისთვის	დიახ; სავარაუდოა; შესაძლებელია; ნაკლებ სავარაუდოა; არა;	$p_{15,1}^{(VM)}$
	A_2	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ის თანამდებობისი პირებისთვის		$p_{15,2}^{(VM)}$
	A_3	არის თუ არა მოწყვლადობა ხელმისაწვდომი სსს-ისთვის კომპიუტერული ტექნიკისა და პროგრამული უზრუნველყოფის მწარმოებლებისთვის		$p_{15,3}^{(VM)}$

ცხრილ 3-ის მონაცემები საშუალებას იძლევა გაკეთდეს მოწყვლადობების რაოდენობრივი შეფასება. ანუ განისაზღვროს ალბათობა $P_i^{(VM)}$ სადაც i=1,2…15, მოწყვლადობის წარმოქმნა ყველა შესაძლო ვირუსული შეტევის საფრთხის წყაროდან გამოისახება ფორმულით:

$$P_i^{(VM)} = 1 - \prod_{j=1}^{3}(1 - \alpha_{ij} * p_i^{(VM)}) \quad (1)$$

სადაც α_ij არის 1 თუ VMi რეალიზდება Aj, ხოლო წინაღმდეგ შემთხვევაში არის 0. ცხრილი 2-ში განსაზღვრული ვირუსის შეტევების საფრთხის წყაროების და ცხრილი 3-ის სსს-ის მოწყვლადობებზე მავნე პროგრამების ზემოქმედების განსაზ¬ღვრებების შესაბამისობა შესაძლებლობას იძლევა შეიქმნას საფრთხეების სიმრავლე:

VMA1 - მავნე პროგრამის დაყენების საფრთხე, რომელსაც გაფართოებული უფლებამოსილების მქონე ალტერნატიული ოპერაციული სისტემის ფუნქციები გააჩნია.

VMA2 - ინფორმაციის დაკოპირების საფრთხე.

VMA3 - ინფრომაციის შეცვლის საფრთხე.

VMA4 – „ინსაიდერი“-ს ჩანერგვის საფრთხე.

VMA5 - სისტემური პროგრამული უზრუნველყოფის შეცვლის საფრთხე.

VMA6 - ქსელური ტრაფიკის გადამისამართების საფრთხე.

VMA7 – დაშორებულ რეჟიმში ინფორმაციის პირდაპირი მანიპულირების საფრთხე.

VMA8 - ელექტრონული საფოსტო ყუთის (იმეილი) გატეხვის საფრთხე.

VMA9 - იმეილის დაბლოკვის საფრთხე.

VMA10 - Web-ბრაუზერების მოწყვლადობებზე დაფუძნებული შეტევების საფრთხე.

VMA11 - გამოყენებითი პროგრმების ალგორითმებში დაშვებუბული შეცდომების გამოყენების საფრთხე.

VMA12 - მომხმარებლების ჰოსტების ბლოკირების საფრთხე.

VMA13 - მარშუტიზატორის ბლოკირების საფრთხე.

VMA14 - ქსელთაშორისი ეკრანისთვის გვერდის ავლის საფრთხე.

ვირუსული შეტევების საფრთხისას სსს-ის მოწყვლადობებზე მავნე პროგრამული უზრუნველყოფის ზემოქმედების განსასაზღვრად შესაძლებელია ცხრილი 4.

ვირუსული შეტევის საფრთხე	სსს-ის მოწყვლადობა (VMj, j =1, 2, …, 15)მავნე პროგრამული უზრუნველყოფის ზემოქმედებისას														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
VMA1	■				■	■						■	■	■	■
VMA2					■			■	■	■	■	■	■	■	■
VMA3	■	■	■		■			■	■	■	■	■	■	■	■
VMA4	■	■	■		■	■	■	■	■	■	■	■	■	■	■
VMA5	■	■	■										■	■	■
VMA6	■	■	■		■	■	■	■	■	■			■	■	■
VMA7	■	■	■				■						■		
VMA8	■	■	■			■			■				■	■	
VMA9	■		■			■			■				■	■	
VMA10	■	■	■			■			■				■		■
VMA11	■	■									■		■		
VMA12	■					■		■				■			
VMA13	■					■		■		■	■	■			
VMA14	■	■	■										■		

ცხრილი 4

ცხრილ 4-ის მონაცემები ვირუსული შეტევების საფრთხის რაოდენობრივი შეფასების საშუალებას იძლევიან, რაც გულისხმობს განისაზღვროს $P_k^{(VMA)}$ საფრთხეების აღმოენების ალბათობა ყველა შესაძლო მოწყვლადობის რეალიზებისას. [1] გამოსახულება 2

$$P_k^{(VMA)} = 1 - \prod_{j=1}^{315}(1 - \beta_{kj} * P_{ki}^{(VM)}) \qquad (2)$$

სადაც β_{ij} არის 1 თუ VMi გამოიყენება VMAk საფრთხის რეალიზებისას, ხოლო წინაღმდეგ შემთხვევაში არის 0.

ვირუსული შეტევების საფრთხის სსს-ის ინფორმაციულ რესურსებზე მავნე ზემოქმედების განსაზღვრა ხდება ემპარიული მეთოდის გამოყენებით რომლისთვისსაც საჭიროა ცხრილ 5-ში მოცემული მონაცემები. ცხრილში პირობითი დასახელებები აღნიშნავენ: UC - ინფორმაციის არასანქცირებული კოპირება, DI- ინფორმაციის დამახინჯება, BI- ინფორმაციის ბლოკირებას.

საფრთხის კოდი	საფრთხის დასახელება	მავნე ზემოქმედება		
		UC	DI	BI
VMA1	მავნე პროგრამის დაყენების საფრთხე, რომელსაც გაფართოებული უფლებამოსილების მქონე ალტერნატიული ოპერაციული სისტემის ფუნქციები გააჩნია.	+	+	+
VMA2	ინფორმაციის დაკოპირების საფრთხე.	+		
VMA3	ინფორმაციის შეცვლის საფრთხე.		+	
VMA4	„ინსაიდერი“-ს ჩანერგვის საფრთხე.	+	+	+
VMA5	სისტემური პროგრამული უზრუნველყოფის შეცვლის საფრთხე.		+	
VMA6	ქსელური ტრაფიკის გადამისამართების საფრთხე.		+	
VMA7	დაშორებულ რეჟიმში ინფორმაციის პირდაპირი მანიპულირების საფრთხე.	+	+	+
VMA8	ელექტრონული საფოსტო ყუთის (იმეილი) გატეხვის საფრთხე.	+		
VMA9	იმეილის დაბლოკვის საფრთხე.			+
VMA10	Web-ბრაუზერების მოწყვლადობებზე დაფუძნებული შეტევების საფრთხე.	+	+	+
VMA11	გამოყენებითი პროგრმების ალგორითმებში დაშვებებული შეცდომების გამოყენების საფრთხე.	+	+	+
VMA12	მომხმარებლების ჰოსტების ბლოკირების საფრთხე.			+
VMA13	მარშუტიზატორის ბლოკირების საფრთხე.			+
VMA14	ქსელთაშორისი ეკრანისთვის გვერდის ავლის საფრთხე.	+	+	+

ცხრილი 5

ცხრილ 5-ის მონაცემები სსს-ის ინფორმაციული გარემოს მავნე პროგრამული უზრუნველყოფისადმი მგრძნობელობის რაოდენობრივი შეფასების საშუალებას იძლევიან, რაც გულისხმობს თითოეული გზნხილული საფრთხის ტიპისთვის განისაზღვროს $P_k^{(v)}$ ინფორმაციაზაე მავნე ზემოქმედების ალბათობა. გამოსახულება 3

$$P_k^{(V)} = 1 - \prod_{l=1}^{3}(1 - \gamma_{kl} * P_{kl}^{(VMA)}) \qquad (3)$$

სადაც:

k=1,2,...14; l=1,2,3.

γ_{kl} არის 1 როდესაც მავნე ზემოქმედება V წარმოადგენს VMA საფრთხის რეალიზაციის შედეგს , წინაღმდეგ შემთხვევაში არის 0.

სსს-ის საინფორმაციო სივრცეზე ვირუსული შეტევების ზემოქმედებისადმი მგრძნობელობის შეფასება (3) გამოსახულებების საშუალებით უნდა განიხილოს როგორც ბოროტმოქმედის მიერ სსს-ის ინფორმაციული რესურსებისადმი კანონსაწინაღმდეგო ქმედებების რეალიზების შესაძლებლობების ინტეგრალური შეფასების წინაპირობა. ასეთი ტიპის შესაძლებლობების მახასიათებელეს წარმოადგენს ყველა ზემოთ ჩამოთვლილ საფრთხეებისადმი სსს-ის საინფორმაციო სივრცის მგძნობელობის $P^{(m)}$ ალბათობა.

$$P_k^{(M)} = 1 - \prod_{k=1}^{14}(1 - P_k^{(V)}) \qquad (4)$$

1 А.С. Марков, В.Л. Цирлов, А.В. Барабанов; Москва «Радио и связь» 2012; Методы оценки несоответствия средств защиты информации;

სადაც:

k=1,2,...14.

გამოსახულება (18) უნდა ჩაითვალოს როგორც სსს-ის ინფორმაციულ რესურსებზე ვირუსული შეტევების რეალიზაციის ინტეგრალური შეფასების მათემატიკური მოდელი. ამ მოდელს ეფუძნება აღნიშნული ტიპის საფრთხეებისგან სსს-ის ინფორმაციის უსაფრთხოების დაცვის მოდელები.

მესამე კონცეფცია მიმართულია ინფორმაციული უსაფრთხოების საფრთხეების (მათ შორის ვირუსული შეტევების საფრთხისგან ინფორმაციის უსაფრთხოების) შეფასებას და ამ ნაკლოვანებების აღმოფხვრას. ამ კონცეფციას საფუძვლად უდევს მიზნების მისაღწევად სისტემის ფუნქციონირების ეფექტურობის სისტემური ინტერპრეტაცია. სსს-ის ვირუსული შეტევებისგან დაცვის მექანიზმების ეფექტურობის მაჩვენებელი უნდა განიხილოს როგორც ანტივირუსული დაცვის მექანიზმების ერთობლიობის სუბიეტური შეფასება რომელიც სსს-ის უსაფრთხოების და ფუნქციონირების კონკრეტულ ხარისხს და დონეს უზრუნველყოფს.

იმის გათვალისწინებით, რომ სსს წარმოადგენს საქმიანობის ინფორმაციულ უზრუნველყოფას, ინფორმაციული უსაფრთხოების საფრთხეები მათ შორის ვირუსული შეტევების საფრთხეები წარმოადგენენ სიტუაციურ ცვლილებებზე ორგანიზაციიის დროული რეაგირების შემამცირებელ ფაქტორებს. აქედან გამომდინარე სსს-ის ინფორმაციის დაცვის მექანიზმების მაჩვენებლები უნდა განიხილებოდეს როგორც ინფორმაციული უსაფრთხოებებზე მომდინარე მსგავს საფრთხეებზე დროული რეაგირების მაჩვენებელი.

ამ მოდელის მდგომარეობა ეფუძნება წინაპირობების ალბათური მოდელს

$$P(\overline{\tau_{(p)}} \leq \tau_{(M)}) \qquad (5)$$

სადაც

$\tau_{(p)}$ და $\tau_{(M)}$ არის საფრთხეზე რეაგირების და მისი არსებობის შემთხვევითი დროითი სიდიდეებია.

$\overline{\tau_{(p)}}$ - $\tau_{(p)}$ შემთხვევითი სიდიდის მათემატიკური ლოდინია.

მოცემული გამოსახულებიდან გამომდინარე ცხადია, რომ ინფორმაციის უსაფრთხოების საფრთხეებზე დროული რეაგირების მსგავსი ფორმალიზირებული წარმოდგენა ასახავს ოთხიდან მხოლოდ ორ პარამეტრს, რომლებიც ახასიათებენ ანტივირუსული დაცვის საშუალებების ვირუსული შეტევების საფრთხეებზე რეაგირების დიანამიკას: საფრთხეზე რეაგირების დრო და საფრთხის არსებობის დრო. ხოლო დანარჩენი ორი პარამეტრს: საფრთხის წარმოშობის დროს და საფრთხეზე რეაგირების დაწყების დროს მოცემული კონცეფცია არ ითვალისწინებს. ინფორმაციის დაცულობის მაჩვენებლები რომლებიც ასახავენ მის უსაფრთხოებაზე დროული რეაგირების მახასიათებლებს და ამასთანავე რომელთა საფუძველსაც წარმოადგენს გამოსახულება (5) მხოლოდ მყისიერი რეაგირების შემთხვევაშია სწორი.

პრაქტიკაში სსს-ის ანტივირუსული დაცვის მექანიზმების საფრთხეებზე მყისიერი რეაგირება რათქმაუნდა ნაკლებ სავარაუდოა. აქედან გამომდინარე ამ მათემატიკური მოდულების პირობებზე დაყრდნობით სსს-ზე ვირუსულ შეტევებზე დროული რეაგირების აგება ვერ უზრუნველყოფს სიზუსტის საჭირო დონეს.

ყოველივე ზემოთქულიდან გამომდინარე გამოწვეულია სსს-ის ინფორმაციული რესურსების ვირუსული შეტევებისგან დაცვის საშუალებების მახასიათებლების მეთოდური აპარატის აუცილებელობა, რომელიც მათემატიკური მოდელირების ტერმინებით ფორმალურად წარმოადგენს ყველა შესაძლო პირობას, რომლებიც ახასიათებენ ვირუსული საფრთხის წარმოშობაზე ანტივირუსული დაცვის მექანიზმების რეაგირების დინამიკას. ასეთი მათემატიკური აპარატის შექმნა შესაძლებელია მხოლოდ იმ შემთხვევაში თუ მოხდება შემდეგი პარამეტრების გათვალისწინებით:

საფრთხეზე რეაგირების დრო.

საფრთხის არსებობის დრო.

საფრთხის წარმოშობის დრო.

საფრთხის წარმოშობიდან მასზე რეაგირებამდე დრო.

გამოყენებული ლიტერატურა

John Ay cock University of Calgary Canada; Springer 2006; Computer Viruses and Malware;

Written by Eric Knight, C.I.S.S.P.; Last Revision: March 9, 2000 Original Publication: March 6, 2000; Computer Vulnerabilities

U.S. Department of Commerce Carlos M. Gutierrez, Secretary National Institute of Standards and Technology Dr. Patrick D. Gallagher, Deputy Director; September 2008; Technical Guide to Information Security Testing and Assessment;

Paul Rebstock, NRC Program Manager,U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Division of Engineering, Digital Instrumentation & Control Branch, Washington; January 27, 2012; Cyber Security Assessment Tools and Methodologies for the Evaluation of Secure Network Design at Nuclear Power Plants

А.С. Марков, В.Л. Цирлов, А.В. Барабанов; Москва «Радио и связь» 2012; Методы оценки несоответствия средств защиты информации;

Abdulrahaman OkinoOtuoze; Mohd WazirMustafa; Journal of Electrical Systems and Information Technology, December 2018, Smart grids security challenges: Classification by sources of threats; https://www.sciencedirect.com/science/article/pii/S2314717218300163