ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

საინფორმაციო-საკომუნიკაციო სისტემების საიმედოობის შეფასების სამხედრო აქტუალობა და მათემატიკური მოდელირება

გიორგი კოხრეიძე[1]
https://doi.org/10.61446/pa.3.2025.10334

აბსტრაქტი

თანამედროვე ციფრულ გარემოში, სადაც საინფორმაციო-საკომუნიკაციო სისტემების (სსს) მდგრადობა და უწყვეტობა მნიშვნელოვანი წინაპირობაა როგორც სახელმწიფო, ისე სამხედრო უსაფრთხოებისთვის, კიბერსაფრთხეებზე დროული და ზუსტი რეაგირების საკითხი განსაკუთრებულ მნიშვნელობას იძენს. მავნე პროგრამებზე დაფუძნებული ვირუსული შეტევების ინტენსიური ზრდა ართულებს მონაცემთა კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფას, ხოლო არსებული შეფასების მეთოდები ხშირად ვერ ასახავს საფრთხის დროით დინამიკასა და შემთხვევითი მოვლენების ზემოქმედებას. სტატიაში წარმოდგენილია მათემატიკურად დასაბუთებული მეთოდოლოგია, რომელიც აღწერს მავნე პროგრამების გამოყენებით განხორციელებული ინფორმაციული დარღვევების შვიდ მოდელს და ავითარებს ეფექტურობის ახალი ტიპის ინდიკატორს, რომელიც ეფუძნება რეაგირების, აღმოჩენისა და საფრთხის არსებობის დროითი პარამეტრების ერთიან შეფასებას. მოდელი ითვალისწინებს ალტერნატიული მოვლენების ურთიერთდამოკიდებულებას, მონაცემებში არსებულ გაურკვევლობასა და რეაგირების პროცესების ალბათურ ბუნებას, რაც მნიშვნელოვნად ზრდის ანალიზის სიზუსტეს. ექსპერიმენტულმა კვლევამ აჩვენა, რომ შემუშავებული მოდელები არსებითად ამცირებს გადაჭარბებულ შეფასებებს, რაც დამახასიათებელია გამარტივებული მიდგომებისთვის (32–58%-მდე პოზიტიური ცდომილება). გარდა ამისა, იდენტიფიცირებულია ის კრიტიკული პროცედურები, რომლებიც ყველაზე მეტად ახდენენ ზემოქმედებას რეაგირების ეფექტურობაზე და რომელთა სრულყოფა აუცილებელია სამხედრო უსაფრთხოების უზრუნველყოფის კონტექსტში. მიღებული შედეგები ხელს უწყობს ანტივირუსული დაცვის მექანიზმების გაუმჯობესების სამეცნიერო საფუძვლების ჩამოყალიბებას და სსს-ის საიმედოობის ამაღლებას თანამედროვე კიბერ-საფრთხეებთან წინააღმდეგობის პირობებში.

საკვანძო სიტყვები: საინფორმაციო-საკომუნიკაციო სისტემები; კიბერსაფრთხეები; მავნე პროგრამები; ვირუსული შეტევები; მათემატიკური მოდელირება; რეაგირების ეფექტურობა; საიმედოობის შეფასება; სამხედრო კიბერუსაფრთხოება; ანტივირუსული დაცვა.

[1] სსიპ დავით აღმაშენებლის სახელობის საქართველოს, ეროვნული თავდაცვის აკადემიის ბაკალავრიატის ინფორმატიკის მიმართულების ასისტენტ პროფესორი

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

Military Relevance and Mathematical Modeling of Reliability Assessment of Information and Communication Systems

Giorgi Kokhreidze[2]

Abstract

In the contemporary digital environment, the reliability and resilience of information and communication systems (ICS) represent a critical prerequisite for national and military security. The growing intensity and sophistication of cyber threats—particularly malware-based attacks—significantly challenge the confidentiality, integrity, and availability of sensitive information resources. Due to the complex and dynamic behavior of malicious code, traditional assessment approaches frequently fail to capture the temporal characteristics and probabilistic nature of cyberattack scenarios. This article presents a mathematically grounded methodology for evaluating the effectiveness of antivirus defense mechanisms in ICS, with a particular emphasis on military-oriented infrastructures. The study develops formalized models describing seven types of security-violation scenarios associated with malware activities and proposes a unified probabilistic indicator for assessing timely response to viral threats. The enhanced modeling framework incorporates alternative events, uncertainty factors, and temporal dependencies—including threat emergence, detection, and response intervals—which existing simplified models often ignore. Experimental simulations demonstrate that the proposed approach significantly improves the accuracy of effectiveness assessments, eliminating the 32–58% overestimation commonly observed in conventional models. The research also identifies the most critical adversarial procedures influencing response efficiency and formulates targeted recommendations for strengthening military cybersecurity capabilities. The findings contribute to the development of scientifically substantiated strategies aimed at increasing the reliability and resilience of ICS against modern malware-driven threats.

Keywords: information and communication systems, malware, cybersecurity, military security, mathematical modeling, threat response effectiveness, reliability assessment, antivirus defense mechanisms.

[2] Assistant Professor of Bachelor's Program in Informatics of LEPL David Aghmashenebeli National Defence Academy of Georgia Doctoral Student

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

შესავალი

თანამედროვე ციფრულ ეპოქაში, სადაც ორგანიზაციები და სახელმწიფო სტრუქტურები მნიშვნელოვანწილად ეყრდნობიან საინფორმაციო-საკომუნიკაციო სისტემების (სსს) უწყვეტ ფუნქციონირებას, ინფორმაციული უსაფრთხოების უზრუნველყოფა რჩება ერთ-ერთ ყველაზე მნიშვნელოვან და მწვავე გამოწვევად. კიბერსაფრთხეების, განსაკუთრებით მავნე პროგრამებზე დაფუძნებული ვირუსული შეტევების ინტენსიური ზრდა, არსებით საფრთხეს უქმნის მონაცემთა კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის (CIA) დაცვის დონეს. მავნე პროგრამების მრავალფეროვანი და რთული ბუნება, მათ შორის თვითგამრავლებითი, პოლიმორფული და ვარიანტულობაზე დაფუძნებული მახასიათებლები, მნიშვნელოვნად ართულებს მათი აღმოჩენისა და პრევენციის პროცესს. ეს გარემოებები საჭიროებს მოწინავე, მათემატიკურ მიდგომებზე აგებულ დაცვით მოდელებს, რომლებიც უზრუნველყოფენ კიბერსაფრთხეებზე უფრო ეფექტიან და ადაპტურ რეაგირებას.

სამხედრო დანიშნულების სისტემებისთვის, რომლებიც ხშირად კრიტიკული საინფორმაციო ინფრასტრუქტურის ნაწილს წარმოადგენენ, უსაფრთხოების საიმედოობა გადამწყვეტ მნიშვნელობას იძენს. მართვის ოპერატიულობისადმი მზარდი მოთხოვნების პირობებში, განსაკუთრებული ყურადღება უნდა დაეთმოს სსს-ში ანტივირუსული თავდაცვის მექანიზმების ეფექტიანობასა და საიმედოობას. სამხედრო სტრუქტურებში სსს-ის საინფორმაციო რესურსებზე ვირუსული შეტევების ერთ-ერთი ყველაზე ნეგატიური შედეგი შეიძლება იყოს უსაფრთხოების უზრუნველყოფის პროცესებზე მართვის დროებითი დაკარგვა, რასაც შესაძლოა მოჰყვეს მონაცემთა კონფიდენციალურობის დარღვევა ან ოპერაციული პროცესების პარალიზება, რაც კრიტიკულია სახელმწიფოებრივი მდგრადობისთვის. შესაბამისად, საჭიროა ისეთი მეთოდური აპარატის შემუშავება, რომელიც ხელს შეუწყობს ანტივირუსული დაცვის მექანიზმების სრულყოფის მიმართულებების მეცნიერულ დასაბუთებას.

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

ამ კონტექსტში, უსაფრთხოების ეფექტურობის შეფასების მოდელების სიზუსტის ამაღლება, რომელიც ითვალისწინებს მავნე პროგრამების ზემოქმედების დინამიკასა და ანტივირუსული დაცვის მექანიზმების ურთიერთგავლენას, ცენტრალური ამოცანაა.

უსაფრთხოების სისტემების საიმედოობის თეორიული მიმოხილვა

კიბერსაფრთხეების მზარდი დინამიკა

კიბერშეტევების რაოდენობა გლობალურ და ეროვნულ დონეზე ყოველწლიურად მზარდ დინამიკას ინარჩუნებს. სტატისტიკური მონაცემები აჩვენებს, რომ კიბერშეტევების რაოდენობა 30%-ით არის მომატებული გლობალურად, ხოლო ყოველკვირეულად საშუალოდ 1,636 ორგანიზაცია ხდება კიბერშეტევის სამიზნე.[3]

მავნე პროგრამები (Malware) წარმოადგენს საერთო ტერმინს, რომელიც აერთიანებს ყველა პროგრამას, რომელიც შექმნილია არასანქცირებული ქმედებების შესასრულებლად, როგორიცაა კომპიუტერული სისტემების ან ქსელების გაუმართაობა ან განადგურება, პირადი მონაცემების მოპარვა ან სისტემის დაზიანება. მავნე პროგრამული უზრუნველყოფა სამ ძირითად მავნე ქმედებას ასრულებს: არასანქცირებული წვდომა მონაცემებზე, ინფორმაციის დამახინჯება და ინფორმაციაზე წვდომის დაბლოკვა, რაც საფრთხეს უქმნის CIA ტრიადას.

განსაკუთრებით სერიოზული გამოწვევაა გამოსასყიდი პროგრამებით (Ransomware) განხორციელებული შეტევები, რომელთა მსხვერპლიც ყოველი 14 წამში საშუალოდ ერთი კომპანია ხდება. კიბერშეტევების ძირითადი ტიპები მსოფლიო მასშტაბით ასე ნაწილდება:[4] (Verizon, 2024)

Ransomware - გამოსასყიდი პროგრამა	**68.42%**
Network breach - ქსელის გარღვევა	18.42%
Data exfiltration - მონაცემების უკანონო გატანა	3.95%
Loader - ჩამტვირთავი პროგრამა	3.29%
Data extortion - მონაცემებით გამოძალვა	2.63%

[3] N.Kumar, 83 Cybersecurity Statistics 2025 (Worldwide Data & Trends). (2025, 07 25). Retrieved from demandsage.com: https://surl.li/rkjvin, (Accessed 08.12.25)
[4] Verizon. Data Breach Investigations Report. (2024). https://surl.li/oaobct, (Accessed 08.12.25)

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

Web shell - ვებ-შელი	2.63%
Coinminer - კრიპტოვალუტის მაინერი	0.66%

ცხრილი1 მსოფლიო მასშტაბით გამოვლენილი კიბერშეტევების ტიპები

მავნე პროგრამების გავრცელების არხები მრავალფეროვანია (USB, დისკები, მეილები, მავნე საიტები). კლასიფიკაცია მოიცავს:

- **კომპიუტერული ჭიები (Worms):** ვრცელდებიან ქსელის საშუალებით ოპერაციული სისტემების მოწყვლადობების გამოყენებით, შეუძლიათ თვითგამრავლება და გავრცელება ადამიანის ჩარევის გარეშე.
- **ტროიანები (Trojans):** შენიღბულნი არიან როგორც უსაფრთხო ფაილები, იძლევიან დისტანციური კონტროლის საშუალებას.
- **რუტკიტები (Rootkits):** შექმნილია ფარული დისტანციური წვდომის მოსაპოვებლად, მათი აღმოჩენა რთულია.
- **შანტაჟის/გამომძალველი პროგრამები (Ransomware):** ჩუმად შიფრავენ მონაცემებს და ითხოვენ გამოსასყიდს.[5]

სამხედრო სისტემებში განსაკუთრებული საფრთხის მატარებელია ისეთი ვირუსული ტექნოლოგიები, როგორიცაა „მომსახურებაზე უარის“ ტიპის შეტევები (DoS/DDoS), ტრაფიკის ანალიზატორები (Sniffer), კაცი შუაში (MITM), სეანსის გადამჭერი პროგრამები (HTTP) და ექსპლოიტები, რადგან მათ შეუძლიათ ოპერაციული პროცესების პარალიზება, რაც საბრძოლო მოქმედებების ან კრიტიკული ინფრასტრუქტურის მართვის შეფერხებას გამოიწვევს.[6]

დაცვის მექანიზმების შეფასების არსებული კონცეფციები

უსაფრთხოების სისტემების ეფექტურობის შეფასების მეთოდოლოგია ეფუძნება სამ ძირითად კონცეფციას,:

1. **სერტიფიცირებაზე დაფუძნებული კონცეფცია:** ეს მიდგომა აფასებს ანტივირუსული საშუალებების ეფექტურობას მათი სერტიფიკატის საფუძველზე. უსაფრთხოება ეფექტურად ითვლება, თუ დეკლარირებული ფუნქციონალური შე-

[5] H. S. Joshua Saxe, Malware Data Science: Attack Detection and Attribution. U.S: No Starch Press. (2018). Retrieved from https://archive.org: Malware Data Science: Attack detection and attribution
[6] C.Easttom, Network defense and countermeasures: Principles and practices. U.S: Pearson . (2021).

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

საძლებლობები შეესაბამება დადგენილ სტანდარტებს და დაცულობის კლასებს (მაგალითად, I, II, III კლასი). თუ გაცხადებული ფუნქციიდან ერთი მაინც არ მუშაობს, მაშინ დაცვის საშუალება არაეფექტურად ითვლება.

დაცვის მექანიზმები	I კლასი (დაბალი დაცულობა)	II კლასი (საშუალო დაცულობა)	III კლასი (მაღალი დაცულობა)
წვდომის მართვის საშუალებები	ნაწილობრივ შეესაბამება	სრულად შეესაბამება	სრულად შეესაბამება
იდენტიფიკაცია, ავთენტიფიკაცია, კონტროლი	ნაწილობრივ შეესაბამება	სრულად შეესაბამება	სრულად შეესაბამება
ინფორმაციული ნაკადების მართვა	არ შეესაბამება	ნაწილობრივ შეესაბამება	სრულად შეესაბამება
რეგისტრაციისა და აღრიცხვის საშუალებები	არ შეესაბამება	ნაწილობრივ შეესაბამება	სრულად შეესაბამება
დეტალური რეგისტრაცია და აღრიცხვა	არ შეესაბამება	ნაწილობრივ შეესაბამება	სრულად შეესაბამება
ინფორმაციის მატარებლების აღრიცხვა	არ შეესაბამება	ნაწილობრივ შეესაბამება	სრულად შეესაბამება
მეხსიერების უბნების გასუფთავება	არ შეესაბამება	ნაწილობრივ შეესაბამება	სრულად შეესაბამება

ცხრილი 2. ინფორმაციის დაცვის მექანიზმების დეკლარირებული შესაძლებლობების შესაბამისობა ინფორმაციული სისტემების დაცულობის კლასებთან

2. **ინფორმაციული საფრთხეების აქტუალურობის შეფასება:** ეს კონცეფცია იყენებს ექსპერტულ შეფასებებს რისკის მართვისთვის, კრიტიკულად მნიშვნელოვან კომპონენტებში საფრთხეების მოწყვლადობისა და ზემოქმედების ალბათობის დასადგენად. ამ მეთოდის არსი მდგომარეობს საფრთხის წყაროსა და სისტემის მოწყვლადობას შორის კავშირის დადგენაში. ეს გამოიყენება ეროვნულ კიბერუსაფრთხოების სტრატეგიებში, სადაც კრიტიკული ინფრასტრუქტურის ობიექტები განსაკუთრებულ კონტროლს ექვემდებარებიან.
3. **მოვლენათა ალბათური მოდელირება:** ეს თანამედროვე მიდგომა მიზნად ისახავს ანტივირუსული დაცვის სისტემების რეაგირების პროცესის ანალიზს ვირუსული

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

თავდასხმის სცენარების დინამიკის ფარგლებში. თუმცა, არსებულ მოდელებში (როგორიცაა $P(\tau(p) \leq \tau(M))$) ხშირად მხედველობაში მიიღება მხოლოდ საფრთხეზე რეაგირების დრო ($\tau(p)$) და მისი არსებობის დრო ($\tau(M)$), მაგრამ უგულებელყოფილია ისეთი კრიტიკული ფაქტორები, როგორიცაა საფრთხის წარმოშობის დრო და რეაგირების დაწყების მომენტი.

არსებული მეთოდების ნაკლოვანებები და სამხედრო სექტორის გამოწვევები

მიუხედავად იმისა, რომ პირველი ორი კონცეფცია მარტივად გამოიყენება, მათ გააჩნიათ დაბალი სიზუსტე, რადგან ეფუძნება ექსპერტების ემპირიულ შეფასებებს. უფრო მეტიც, მათ არ გააჩნიათ ფორმალიზებული მოდელი, რომელიც დეტალურად აღწერს დამრღვევის ქმედებებს, ანუ არ არის გათვალისწინებული მავნე პროგრამების ზემოქმედების დინამიკა და რეაგირების პროცესების ფორმალიზებული წარმოდგენა.

სამხედრო დანიშნულების სისტემებისთვის, სადაც ინფორმაციული პროცესების უწყვეტობა და სენსიტიური მონაცემების დაცვა უმნიშვნელოვანესია, **დროული რეაგირება** არის კრიტიკული საიმედოობის მაჩვენებელი. რადგანაც მყისიერი რეაგირება ნაკლებად სავარაუდოა, აუცილებელია მათემატიკური აპარატის შექმნა, რომელიც ზუსტად აღწერს ყველა შესაძლო დროით პარამეტრს (რეაგირების დრო, არსებობის დრო, წარმოშობის დრო, რეაგირების დაწყებამდე გასული დრო).

უსაფრთხოების საიმედოობის შეფასების მათემატიკური მოდელირება

კვლევის ძირითადი მეცნიერული მიზანი იყო ვირუსული შეტევებისგან დაცვის ეფექტურობის შეფასების პროცესში, მუქარებზე რეაგირების დროითი დინამიკის, მავნე კოდის მოქმედებისა და ანტივირუსული დაცვის მექანიზმების ურთიერთგავლენის ერთიანი მათემატიკური ფორმალიზაცია. ეს მიდგომა მიმართულია მოდელების სიზუსტის ამაღლებაზე, არასრული ან შეცდომებით მიღებული მონაცემების გავლენის შესაფასებლად.

კვლევა ეფუძნება სისტემურ ანალიზს, მათემატიკური მოდელირების მეთოდოლოგიას, ალბათობის თეორიას და მათემატიკურ სტატისტიკას. შემუშავებული

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

მეთოდოლოგია ითვალისწინებს გაურკვევლობის მრავალ წყაროს: არასრულ მონაცემებს, არაზუსტ პერიოდულ პარამეტრებს და ექსპერტული შეფასებების ცდომილებებს.

ვირუსული შეტევების მართლსაწინააღმდეგო ქმედებების მოდელები

იმის გათვალისწინებით, რომ დამრღვევის ქმედებებს გააჩნია მიზნობრივი მოტივაცია, მავნე პროგრამების გამოყენებით ინფორმაციის უსაფრთხოების დარღვევის შვიდი მოდელია შემუშავებული, რომლებიც ერთმანეთისგან განსხვავდებიან ინფორმაციის დაცულობის დარღვევის შესაძლებლობებით (კონფიდენციალურობა, მთლიანობა, ხელმისაწვდომობა),:

1. **პირველი ვარიანტი:** ვირუსული შეტევა კონფიდენციალური ინფორმაციის არასანქცირებული კოპირების მიზნით.

2. **მეორე ვარიანტი:** ვირუსული შეტევა ინფორმაციის მოდიფიკაციის ან განადგურების მიზნით.

3. **მესამე ვარიანტი:** ვირუსული შეტევა სსს-ის საინფორმაციო რესურსების ხელმისაწვდომობის ბლოკირების მიზნით.

4. **მეოთხე ვარიანტი:** კოპირება და შემდგომი მოდიფიკაცია ან განადგურება.

5. **მეხუთე ვარიანტი:** კოპირება და ხელმისაწვდომობის შემდგომი ბლოკირება.

6. **მეექვსე ვარიანტი:** მოდიფიკაცია/განადგურება და ხელმისაწვდომობის შემდგომი ბლოკირება.

7. **მეშვიდე ვარიანტი (უდიდესი ზიანი):** კოპირება, შემდგომი მოდიფიკაცია/განადგურება და ხელმისაწვდომობის ბლოკირება.

თითოეული მოდელი დეტალურად აღწერს დამრღვევის ქმედებების თანმიმდევრობას (ანალიზი, დაძლევა, ცრუ სანდო ობიექტად მოქმედება, ინფორმაციის ანალიზი და დარღვევა) და შესაბამის პროცედურებს. (Rebstock, 2012)

ეფექტურობის ინდიკატორის ფორმალიზებული წარმოდგენა

სსს-ში ვირუსულ შეტევებზე რეაგირების ეფექტურობის მაჩვენებელი (*Epi*) ფორმალიზებულია, როგორც ანტივირუსული დაცვის მექანიზმების დროული აღმოჩენის, იდენტიფიცირების და ჩახშობის შესაძლებლობა.

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

ეს მაჩვენებელი წარმოდგენილია ალბათობითი ფორმით, რომელიც ითვალისწინებს რეაგირების დროით დინამიკას:

$Epi=P(\tau(d)(i)\leq\tau(ma)(i)-\tau(p)(i))$(2.26) სადაც:

- $\tau(d)(i)$ არის ვირუსული შეტევის აღმოჩენის დროის მათემატიკური მოლოდინი.
- $\tau(ma)(i)$ არის ვირუსული შეტევის რეალიზაციის (არსებობის) დროის მათემატიკური მოლოდინი.
- $\tau(p)(i)$ არის ვირუსულ შეტევაზე რეაგირების დროის მათემატიკური მოლოდინი,.

თეორიულად დამტკიცდა, რომ მოდელირებისას აუცილებელია ალტერნატიული მოვლენების ფორმალური წარმოდგენა, რომლებიც ურთიერთდამოკიდებულია მყისიერი რეაგირების მოვლენასთან. მხოლოდ რეაგირების დროისა და საფრთხის არსებობის დროის გათვალისწინება იწვევს რეაგირების დროული შესრულების ინდიკატორის გადაჭარბებულ შეფასებას. ამიტომ, სიზუსტის ამაღლების მახასიათებელი (ΔEi) განისაზღვრა, როგორც სხვაობა ეფექტურობის მაჩვენებლის მნიშვნელობას შორის, რომელიც ითვალისწინებს ყველა შესაძლო პარამეტრს, და იმ მნიშვნელობას შორის, რომელიც ითვალისწინებს მხოლოდ ცალკეულ პარამეტრებს.

სიმულატორზე ჩატარებული ექსპერიმენტის შედეგად დადგინდა, რომ შემუშავებული მათემატიკური მოდელები და ფორმალიზებული მიდგომები მნიშვნელოვნად აუმჯობესებენ სსს-ში ვირუსული შეტევების მუქარებზე რეაგირების სიზუსტესა და ეფექტიანობას.

მათემატიკური მოდელების სიზუსტის შეფასებამ აჩვენა, რომ ძველი, გამარტივებული მოდელები (რომლებიც არ ითვალისწინებდნენ შემთხვევით მოვლენებს) **დროული რეაგირების შეფასებას 32%–დან 58%–მდე ზრდიდა** (გადაჭარბებულად აფასებდა). ეს ნიშნავს, რომ მხოლოდ ახალი, კომპლექსური მოდელი, რომელიც ითვალისწინებს მუქარის წარმოქმნის, აღმოჩენის და რეაგირების დინამიკას, იძლევა საიმედო სურათს სისტემის რეალურ მდგომარეობაზე.

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

ინფორმაციის დარღვევის მოდელი	ეფექტურობის მაჩვენებლის მნიშვნელობები, მიღებული, დისერტაციაში შემუშავებული მოდელების მეშვეობით	ეფექტურობის მაჩვენებლის მნიშვნელობები, მიღებული (4.17) მოდელის მეშვე ობით	სიზუსტის მაჩვენებელი	მომატებული შეფასების პროცენტი
1	0,478	0,918	0,440	48
2	0,431	0,884	0,453	51
3	0,409	0,964	0,555	58
4	0,557	0,814	0,257	32
5	0,530	0,900	0,370	41
6	0,478	0,870	0,392	45
7	0,615	0,852	0,237	39

ცხრილი. 3 შემუშავებული მათემატიკური მოდელირების აპარატის სიზუსტის შეფასების შედეგები

მაგალითად, ინფორმაციის უსაფრთხოების დარღვევის 7-ე მოდელისთვის (უდიდესი ზიანის მომტანი), შემუშავებული მოდელის ეფექტურობის მაჩვენებელი იყო 0,615, მაშინ როცა გამარტივებული მოდელით მიღებული მნიშვნელობა 0,852 იყო. სიზუსტის მაჩვენებელი ამ შემთხვევაში 0,237-ს შეადგენდა.

დასკვნები და რეკომენდაციები სამხედრო უსაფრთხოებისათვის

უსაფრთხოების სისტემების საიმედოობა, განსაკუთრებით სამხედრო დანიშნულების საინფორმაციო-საკომუნიკაციო სისტემებში, პირდაპირპროპორციულია კიბერსაფრთხეებზე დროული და ზუსტი რეაგირების შესაძლებლობებთან.

დასკვნა

ჩატარებული კვლევის ფარგლებში განსაზღვრული კრიტიკულობის ანალიზმა გამოავლინა ის მართლსაწინააღმდეგო ქმედებები, რომელთა დროითი მახასიათებლების შეცვლა (შემცირება) ყველაზე დიდ გავლენას ახდენს რეაგირების ეფექტურობაზე. კრიტიკულ პროცედურებად, რომელთა მიმართაც ანტივირუსული

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

დაცვის ზომები უნდა სრულყოფილ იქნეს (კრიტიკულობის ზღვრული მნიშვნელობა $\beta(n) \geq 0,75$-ის ტოლობით), დასახელდა:

- **ვირუსული კოდის პოლიმორფული რესტრუქტურიზაცია:** ეს პროცედურა, რომელსაც მაღალი კრიტიკულობის კოეფიციენტი აქვს (მაგ. მოდელი 4-ისთვის 0,76; მოდელი 6-ისთვის 0,8), საჭიროებს გაუმჯობესებულ ჰევრისტიკულ ანალიზს, პროგრამული უზრუნველყოფის საქმიანობის მონიტორინგს და დასამუშავებელი ფაილების სტრუქტურის შეცვლას მონაცემთა ფორმატების გარდაქმნის გზით.
- **ვირუსული კოდის ასოციაცია პროგრამული უზრუნველყოფის კომპონენტთან:** ამ პროცედურის წინააღმდეგ საჭიროა სერტიფიცირებული პროგრამული უზრუნველყოფის გამოყენება და გამოყენებული ფაილების შეცვლისგან დაცვა.
- **სანდო ობიექტის სტატუსის შეცვლა ყალბზე ARP სერვისის ნაკლოვანებების გამოყენებით:** ეს არის კრიტიკულობის მაღალი მაჩვენებლის მქონე პროცედურა (მაგ. მოდელი 7-ისთვის 0,78). მის გასანეიტრალებლად რეკომენდებულია ქსელთაშორისი ეკრანირება, ARP-შეკითხვების ანალიზი და სერვერების ARP-ცხრილების მდგომარეობის ანალიზი, ასევე ხელით რედაქტირების რეჟიმზე გადასვლა ავტომატური კორექციის აკრძალვისთვის.
- **სანდო ობიექტის სტატუსის შეცვლა ყალბზე დაშორებული ძიების ალგორითმების ნაკლოვანებების გამოყენების საფუძველზე:** ამასთან დაკავშირებით რეკომენდებულია მარშრუტიზაციის მდგომარეობის ანალიზი კომპიუტერულ ქსელში და ხელით რედაქტირების რეჟიმზე გადასვლა ავტომატიზირებული ადრესაციის გამორთვისთვის.

სამხედრო სექტორმა, რომელიც ხასიათდება მაღალი რისკებით და ინფორმაციული ომის პოტენციური საფრთხეებით, უნდა გამოიყენოს ეს მათემატიკურად დასაბუთებული მოთხოვნები ანტივირუსული დაცვის მექანიზმების გაუმჯობესებისა და თავდაცვის სტრატეგიების დახვეწის მიზნით.

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

ბიბლიოგრაფია

Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems.* U.S: Wiley. (2020).

Aycock, J. *Computer viruses and malware.* Canada: Springer. (2006).

Easttom, C.Network defense and countermeasures: Principles and practices. U.S: Pearson . (2021).

Joshua Saxe, H. S., Malware Data Science: Attack Detection and Attribution. U.S: No Starch Press. (2018). Retrieved from https://archive.org: Malware Data Science: Attack detection and attribution

khan, A. (2024, August 30). *Threat Spotlight: How ransomware for rent rules the threat landscape (posted in the subreddit r/BarracudaNetworks).* Retrieved from Reddit: https://surl.li/iydesd, (Accessed 08.12.25)

Kumar, N.83 Cybersecurity Statistics 2025 (Worldwide Data & Trends). (2025, 07 25). Retrieved from demandsage.com: https://surl.li/rkjvin, (Accessed 08.12.25)

Kumar, N. (2025, 07 25). *83 Cybersecurity Statistics 2025 (Worldwide Data & Trends).* Retrieved from demandsage.com: https://surl.li/ekufki, (Accessed 08.12.25)

Rebstock, P. (2012). *Cyber security assessment tools and methodologies for the evaluation of secure network design at nuclear power plants.* U.S: Sandia National Laboratories, New Mexico, USA.

Verizon. Data Breach Investigations Report. (2024). https://surl.li/oaobct, (Accessed 08.12.25)