ინფორმაციული სისტემების რისკების ანალიზი და კონტროლი საგამოცდო ლაბორატორიებში

თამარ წერეთელი, ნონა ოთხოზორია, დავით კაპანაძე
საქართველოს ტექნიკური უნივერსიტეტი
t_tsereteli@gtu.ge, n.otkhozoria@gtu.ge, david@gtu.ge

რეზიუმე

სტატიაში განხილულია ISO/IEC 17025 სტანდარტით აკრედიტებული ლაბორატორიების ინფორმაციული სისტემების რისკების ანალიზისა და კონტროლის თანამედროვე მიდგომები. განსაკუთრებული ყურადღება გამახვილებულია ტრანსფორმატორების ელექტრული მახასიათებლების გაზომვებთან დაკავშირებულ მონაცემთა სანდოობაზე, რომლის დარღვევაც ენერგოსექტორის უსაფრთხოებასა და ეკონომიკურ მდგრადობაზე მნიშვნელოვან გავლენას ახდენს. კვლევის სიახლე მდგომარეობს ინტეგრირებულ მოდელში, რომელიც აერთიანებს საერთაშორისო სტანდარტებს (ISO/IEC 27001, ISO/IEC 17025, NIST, ENISA), მათემატიკურ-მოდელირების მეთოდებს (ბაიესის ქსელი, შეუსაბამობათა ხის ანალიზი (FTA), მონტე-კარლოს სიმულაცია) და უსაფრთხოების პრევენციულ და რეაქციულ მექანიზმებს (MFA, SIEM, სარეზერვო აღდგენის გეგმები). მიღებული შედეგები აჩვენებს, რომ შემოთავაზებული მოდელი მნიშვნელოვნად ამცირებს რისკების წარმოშობის ალბათობასა და პოტენციურ ეკონომიკურ ზარალს, ზრდის იდენტიფიცირებული საფრთხეების რაოდენობას და უზრუნველყოფს კრიტიკული მიზეზ-შედეგობრივი კავშირების უკეთ გააზრებას. წარმოდგენილი მიდგომა წარმოადგენს ეფექტიან ინსტრუმენტს აკრედიტებული ლაბორატორიების ინფორმაციული სისტემების მდგრადობისა და უსაფრთხოების გასაუმჯობესებლად.

საკვანძო სიტყვები: ინფორმაციული სისტემები, რისკების ანალიზი, რისკების კონტროლი, ISO/IEC 17025, ISO/IEC 27001

1. შესავალი.

ინფორმაციული სისტემების უსაფრთხოება თანამედროვე ციფრულ ეპოქაში წარმოადგენს ერთ-ერთ უმნიშვნელოვანეს გამოწვევას როგორც კერძო კომპანიებისთვის, ასევე სახელმწიფო სექტორისთვის. ციფრული ტრანსფორმაციის პროცესმა მნიშვნელოვნად გაზარდა ორგანიზაციებში არსებული მონაცემთა ნაკადების მოცულობა, მათი სენსიტიურობა და ღირებულება, რის გამოც იზრდება კიბერთავდასხმების, ტექნიკური ავარიების და ინფორმაციის გაუმართავი მართვის რისკები.

განსაკუთრებით მნიშვნელოვანია ეს საკითხი აკრედიტებულ საგამოცდო ლაბორატორიებში, რომლებიც მუშაობენ ISO/IEC 17025 სტანდარტის მიხედვით. აღნიშნული ლაბორატორიები უზრუნველყოფენ საკონტროლო და საზომი პროცესების სანდოობას, რომელთა შედეგებზე დაფუძნებით ხდება მრავალი ტექნიკური და ეკონომიკური გადაწყვეტილების მიღება. განსაკუთრებული ყურადღება გვინდა გავამახვილოთ ტრანსფორმატორების ელექტრული მახასიათებლების გაზომვებთან დაკავშირებულ მონაცემთა სანდოობაზე, რომლის დარღვევაც ენერგოსექტორის უსაფრთხოებასა და ეკონომიკურ მდგრადობაზე მნიშვნელოვან გავლენას ახდენს. ტრანსფორმატორების ტესტირებისას გაზომილი პარამეტრები - უქმი სვლის დანაკარგები, გრაგნილების იზოლაციის წინაღობა, გრაგნილების წინაღობა მუდმივი დენის მიმართ, დიელექტრიკული დანაკარგების კუთხე და ტრანსფორმაციის

კოეფიციენტი - წარმოადგენს კრიტიკულ ინფორმაციას ენერგეტიკული ინფრასტრუქტურის მდგრადობისთვის. ამ მონაცემების დაკარგვა, შეცვლა ან არასწორი ინტერპრეტაცია შეიძლება გახდეს მნიშვნელოვანი ეკონომიკური ზარალისა და ენერგოსისტემების ავარიების მიზეზი.

ამიტომ, ინფორმაციული სისტემების რისკების ანალიზი და კონტროლის თანამედროვე მეთოდების გამოყენება ლაბორატორიებში არა მხოლოდ აკრედიტაციის მოთხოვნების დაკმაყოფილების მიზნით არის აუცილებელი, არამედ ენერგოსექტორის ზოგადი საიმედოობისა და ქვეყნის ენერგეტიკული უსაფრთხოების დაცვის სტრატეგიული კომპონენტიც. აღნიშნული კვლევა სწორედ ამ საჭიროებას პასუხობს და მიზნად ისახავს ისეთი მეთოდებისა და საშუალებების წარმოჩენას, რომლებიც გააძლიერებს ISO/IEC 17025 სტანდარტით აკრედიტებული ლაბორატორიების ინფორმაციული სისტემების მდგრადობას, უსაფრთხოებასა და ეფექტიანობას.

კვლევის მიზანია საგამოცდო ლაბორატორიებში (ISO/IEC 17025-ის მიხედვით აკრედიტებულებში) ინფორმაციული სისტემების რისკების ანალიზისა და კონტროლის თანამედროვე მეთოდების შესწავლა და მოდელირება, კვლევა აქცენტირებულია ისეთ ლაბორატორიებზე, რომლებიც ახორციელებენ ტრანსფორმატორების ელექტრული მახასიათებლების გაზომვებს.

2. ლიტერატურული მიმოხილვა.

ინფორმაციული სისტემების რისკების ანალიზისა და კონტროლის თანამედროვე მიდგომები ბოლო ათწლეულებში მნიშვნელოვნად განვითარდა, რაც კიბერსაფრთხეების ზრდამ, მონაცემთა მოცულობის მატებამ და სისტემების რთულმა ინტეგრაციამ განაპირობა. როგორც ISO/IEC 27001 სტანდარტი მიუთითებს, ინფორმაციული უსაფრთხოების მართვა უნდა ეფუძნებოდეს რისკებზე ორიენტირებულ მიდგომას, სადაც თითოეული აქტივი შეფასებულია მისი ღირებულებისა და შესაძლო ზარალის თვალსაზრისით (ISO, 2022a). ამ მიდგომას ადასტურებს NIST Cybersecurity Framework-იც, რომელიც ხაზს უსვამს საფრთხეების იდენტიფიკაციის, დაცვის, აღმოჩენის, რეაგირების და აღდგენის ციკლურ მოდელს (NIST, 2018).

ENISA-ს ბოლო ანგარიშებში განსაკუთრებული ყურადღება ეთმობა კრიტიკული ინფრასტრუქტურის (Critical Infrastructures) რისკების მართვას, სადაც ენერგოსექტორი ერთერთ ყველაზე მოწყვლად სფეროდ არის მიჩნეული (ENISA, 2023). კვლევები მიუთითებს, რომ ენერგეტიკული სისტემების უსაფრთხოებაზე პირდაპირ გავლენას ახდენს საზომი და საკონტროლო ლაბორატორიების მიერ მოწოდებული მონაცემების სანდოობა, რაც ISO/IEC 17025 სტანდარტით აკრედიტებულ გარემოში ინფორმაციული რისკების მართვის განსაკუთრებულ მნიშვნელობას უსვამს ხაზს.

თანამედროვე სამეცნიერო ლიტერატურა რისკების მოდელირებისა და ანალიზის სხვადასხვა მეთოდს გამოყოფს. მაგალითად, ბაიესის ქსელები გამოიყენება კომპლექსურ სისტემებში რისკების ურთიერთდამოკიდებულების შესაფასებლად (Fenton & Neil, 2019), ხოლო მონტე-კარლოს სიმულაცია ხშირად გამოიყენება ალბათური სცენარების მოდელირებისთვის, რაც შესაძლებელს ხდის რისკის დონის რაოდენობრივ შეფასებას (Hubbard & Evans, 2010). FMEA (Failure Mode and Effect Analysis), რომელიც წარმოებისა და ინჟინერიაშია გავრცელებული, ეფექტიანად გამოიყენება ინფორმაციული სისტემების სუსტი წერტილების იდენტიფიკაციისთვისაც (Stamatis, 2003).

ბოლო წლებში ჩნდება მიდგომები, სადაც ხელოვნური ინტელექტი (AI) და მანქანური სწავლება (ML) გამოიყენება კიბერსაფრთხეების პროგნოზირებისა და რეალურ დროში

ანომალიების აღმოჩენისათვის (Sarker et al., 2021). ასეთი მიდგომები განსაკუთრებით მნიშვნელოვანია აკრედიტებულ ლაბორატორიებში, სადაც მონაცემთა ხარისხი და სანდოობა პირდაპირ განსაზღვრავს კრიტიკული ტექნიკური გადაწყვეტილებების მიღებას.

ამრიგად, არსებული ლიტერატურა აჩვენებს, რომ ინფორმაციული რისკების მართვა უნდა ეფუძნებოდეს ინტეგრირებულ მიდგომას: სტანდარტებზე დაფუძნებულ ჩარჩოებს (ISO/IEC 27001, NIST, ENISA), მათემატიკურ და სტატისტიკურ მოდელებს და ინოვაციურ ტექნოლოგიურ გადაწყვეტილებებს. ასეთი კომბინაცია უზრუნველყოფს ინფორმაციული სისტემების მდგრადობას და მათ ეფექტიან გამოყენებას ISO/IEC 17025 აკრედიტებულ ლაბორატორიებში.

3. მეთოდოლოგია.

ინფორმაციული სისტემების რისკების ანალიზისა და კონტროლის მეთოდოლოგია დაფუძნებულია სტრუქტურირებულ და ეტაპობრივ მიდგომაზე, რომელიც აერთიანებს როგორც სტანდარტიზებულ ჩარჩოებს, ასევე მათემატიკურ-მოდელირების მეთოდებს.

კვლევაში გამოყენებულია შემდეგი ძირითადი ეტაპები (ნახ.1):

ნახ. 1 ინფორმაციული სისტემების რისკების ანალიზისა და კონტროლის მეთოდები

1. რისკების იდენტიფიკაცია - პირველ ეტაპზე ხდება კრიტიკული აქტივების იდენტიფიკაცია ISO/IEC 17025 აკრედიტებულ ლაბორატორიებში. აქ განსაკუთრებული ყურადღება ეთმობა გაზომვის პროცესში გამოყენებულ მოწყობილობებს, მონაცემთა ბაზებს, პროგრამულ უზრუნველყოფას და პერსონალის საქმიანობას. იდენტიფიკაციისას გამოიყენება აქტივების აღრიცხვის და საფრთხის მოდელირების მეთოდები, რომლებიც უზრუნველყოფენ როგორც ტექნიკური, ისე ორგანიზაციული საფრთხეების ჩამონათვალს.
2. რისკების შეფასება - საფრთხეების გამოვლენის შემდეგ ეტაპზე ხდება მათი შეფასება. შეფასება ორ დონეზე ხორციელდება:
   - თვისებრივი შეფასება (Qualitative Assessment), სადაც გამოიყენება ISO 27005 რისკების მატრიცა - ალბათობა და ზემოქმედება ფასდება დაბალი, საშუალო და მაღალი დონეებით.
   - რაოდენობრივი შეფასება (Quantitative Assessment), სადაც გამოიყენება მონტე კარლოს სხვადასხვა სცენარები მოდელირებისთვის, რაც იძლევა რისკის გავრცელების ალბათურ განაწილებას. ეს მეთოდი განსაკუთრებით ეფექტურია ელექტრული პარამეტრების გაზომვისას, სადაც მცირე შეცდომაც კი შეიძლება სერიოზულ ზარალად გადაიქცეს.
3. რისკების კონტროლი და შემცირება - შეფასების შემდეგ შემუშავდება კონტროლის ღონისძიებები, რომლებიც მოიცავს:
   - პრევენციულ ზომებს – ქსელის სეგმენტაცია, მრავალფაქტორიანი აუტენტიფიკაცია (MFA), მონაცემთა დაკარგვის პრევენცია (DLP), პერსონალის ტრენინგი.
   - რეაქციულ ზომებს – SIEM სისტემებით მონიტორინგი, ინციდენტებზე სწრაფი რეაგირების პროცედურები, მონაცემთა აღდგენის სარეზერვო გეგმები. ორივე ტიპის მექანიზმი ინტეგრირდება ერთიან მრავალდონიან მოდელში, რომელიც უზრუნ-

ველყოფს როგორც ინციდენტის თავიდან აცილებას, ისე მისი შედეგების მინიმიზაციას.

4. მოდელირება და სცენარების ანალიზი - რისკების მოდელირებისათვის გამოყენებულია ორი მეთოდი:
   - ბაიესის ქსელები, რომელიც აჩვენებს რისკებს შორის ურთიერთდამოკიდებულებას (მაგ., აპარატურული გაუმართაობა ↔ მონაცემთა დაკარგვა ↔ შეცდომაში შემყვანი ტექნიკური გადაწყვეტილება).
   - შეუსაბამობათა ხის ანალიზი (FTA), რომელიც გამოიყენება კრიტიკული ინციდენტების ძირეული მიზეზების იდენტიფიცირებისთვის.
5. ვალიდაცია და შედეგების ანალიზი - შემუშავებული მოდელი ტესტირებულია ლაბორატორიებზე, რომლებიც ახორციელებენ ტრანსფორმატორების ელექტრული მახასიათებლების გაზომვას. თითოეულ სცენარში შეფასებულია, თუ რამდენად ამცირებს მრავალდონიანი მიდგომა ინციდენტების ალბათობასა და პოტენციურ ზარალს.

4. კვლევითი ნაწილი.

კველვა განხორციელდა შემოთავაზებული მეთოდოლოგიის შესაბამისად. პირველ რიგში, გამოვიყენეთ ISO/IEC 27005 რისკების მატრიცა, რომლის საშუალებითაც საფრთხეები ხარისხობრივად დავახარისხეთ მათი ალბათობისა და ზემოქმედების მიხედვით. ეს ეტაპი გვაძლევდა საწყის სურათს, რომელი რისკები იყო კრიტიკული და სად იყო საჭირო უფრო სიღრმისეული ანალიზი.

შემდეგ ეტაპზე გადავედით რაოდენობრივ შეფასებაზე. ამ მიზნით ჩავატარეთ მონტე-კარლოს სიმულაცია, რომლის ფარგლებშიც განვახორციელეთ ასობით სცენარის გენერაცია. სიმულაციამ აჩვენა, როგორ შეიძლება სხვადასხვა პირობებში შეცვლილიყო ინციდენტის წარმოშობის ალბათობა და მასთან დაკავშირებული ეკონომიკური ზარალი. მიღებული შედეგები გვაძლევდა რისკების ალბათური პროფილის უფრო ზუსტ შეფასებას.

რისკებს შორის დამოკიდებულებისა და პირობითი ალბათობების დასადგენად გამოვიყენეთ ბაიესის ქსელები, FTA-ს გამოყენებით კი დეტალურად დავაშალეთ კრიტიკული ინციდენტები და გამოვავლინეთ მათი ძირეული მიზეზები.

FTA-მ ნათლად აჩვენა, რომ ერთი ძირითადი ინციდენტი შეიძლება სხვადასხვა მცირე ხარვეზის კომბინაციამ გამოიწვიოს ასევე მოგვცა საშუალება დეტალურად დაგვენახა, რა ძირეული მიზეზები იწვევდა კრიტიკულ ინციდენტებს. აღმოჩნდა, რომ ყველაზე ხშირი სცენარები დაკავშირებული იყო აპარატურულ ხარვეზებთან და ადამიანურ შეცდომებთან, რომლებიც ხშირად ერთიანად ქმნიდნენ კრიტიკულ სიტუაციას. ბაიესის ქსელებმა დაგვანახა, როგორ იზრდებოდა ერთი რისკის ალბათობა სხვების გავლენის ქვეშ. მაგალითად, მოწყობილობის ავარიული გამორთვა მნიშვნელოვნად ზრდიდა მონაცემთა დაკარგვის ალბათობას და, შესაბამისად, არასწორი ტექნიკური დასკვნის რისკიც იზრდებოდა

5. შედეგები და დისკუსია.

კვლევის ფარგლებში შემუშავებული რისკების ანალიზისა და კონტროლის მოდელი აპრობირებული იქნა ISO/IEC 17025 აკრედიტებულ ლაბორატორიებში, რომლებიც ახორციე-ლებენ ტრანსფორმატორების ელექტრული მახასიათებლების ტესტირებას. შედეგების ანალიზმა აჩვენა, რომ მრავალდონიანი (multilayered) მიდგომა მნიშვნელოვნად ამცირებს როგორც კრიტიკული ინციდენტების წარმოშობის ალბათობას, ისე პოტენციურ ეკონომიკურ ზარალს.

ცხრილი 1 ასახავს ტრადიციული მეთოდებისა და შემოთავაზებული მოდელის შედარებით ანალიზს

ცხრილი 1. რისკების მართვის ეფექტიანობის შედარება

მიდგომა	იდენტიფიცირებული საფრთხეების საშუალო რაოდენობა	ინციდენტების საშუალო ალბათობა	ეკონომიკური ზარალის შეფასება
ტრადიციული მიდგომა	12	0.35	მაღალი
შემოთავაზებული მოდელი	20+	0.15	დაბალი

როგორც ცხრილიდან ჩანს, შემოთავაზებულმა მოდელმა მნიშვნელოვნად გაზარდა იდენტიფიცირებული საფრთხეების რაოდენობა (აქტივების ნუსხა + მოდელირება ინტეგრირებული გამოყენებით), რითაც შესაძლებელი გახდა უფრო რეალისტური რისკის შეფასება.

ბაიესის ქსელებისა და შეუსაბამობათა ხის ანალიზის გამოყენებამ შესაძლებელი გახადა რისკებს შორის მიზეზ-შედეგობრივი კავშირების იდენტიფიცირება, რაც ტრადიციულ მეთოდებში ნაკლებად იყო შესაძლებელი. მონტე-კარლოს სიმულაციამ კი უზრუნველყო რისკის რაოდენობრივი გავრცელების უფრო ზუსტი პროგნოზირება, განსაკუთრებით იმ სცენარებში, სადაც მცირე სიზუსტის დაკარგვაც კი ენერგოსისტემისთვის კრიტიკული შედეგის გამომწვევი შეიძლება ყოფილიყო.

გარდა ამისა, ჩატარებულმა მოდელირებამ ცხადყო, რომ პრევენციული და რეაქციული ზომების ერთობლივი ინტეგრაცია (მაგ., MFA, SIEM, სარეზერვო აღდგენის გეგმები) უზრუნველყოფს უფრო მაღალ უსაფრთხოებას, ვიდრე მხოლოდ ერთი ტიპის მექანიზმის გამოყენება.

მიღებული შედეგები ცხადყოფს, რომ შემოთავაზებული მიდგომა არა მხოლოდ თეორიულად გამართლებულია, არამედ პრაქტიკულადაც ამცირებს ლაბორატორიების რისკებს და ზრდის ენერგოსექტორის საერთო საიმედოობას, რაც იძლევა საფუძველს საბოლოო დასკვნების გამოტანისათვის.

6. დასკვნა.

კვლევამ აჩვენა, რომ ინფორმაციული სისტემების რისკების ანალიზისა და კონტროლის თანამედროვე მეთოდების ინტეგრირებული გამოყენება მნიშვნელოვან გავლენას ახდენს ISO/IEC 17025 აკრედიტებული ლაბორატორიების უსაფრთხოებასა და სანდოობაზე.

მთავარი შედეგები:

- შემოთავაზებულმა მოდელმა გააუმჯობესა რისკების იდენტიფიკაცია და რაოდენობრივი შეფასება;
- რისკების წარმოშობის ალბათობა შემცირდა თითქმის ორჯერ, რაც ეკონომიკური ზარალის დონეს მნიშვნელოვნად დაბლა სწევს;
- ბაიესის ქსელებისა და შეუსაბამობათა ხის ანალიზის მეთოდების ინტეგრაციამ შესაძლებელი გახადა კრიტიკული მიზეზ-შედეგობრივი კავშირების იდენტიფიცირება;
- პრევენციული და რეაქციული კონტროლის ზომების ერთიან მოდელში გაერთიანებამ უზრუნველყო უფრო მაღალი მდგრადობა და უსაფრთხოება.

კვლევის მეცნიერული სიახლე მდგომარეობს იმაში, რომ შემუშავებულია ერთიანი მოდელი, რომელიც აერთიანებს საერთაშორისო სტანდარტებს (ISO/IEC 27001, ISO/IEC 17025,

NIST, ENISA), მათემატიკურ მოდელირებასა და თანამედროვე ტექნოლოგიურ ინსტრუმენტებს.

მომავალი კვლევის მიმართულებები შეიძლება მოიცავდეს ხელოვნური ინტელექტისა და მანქანური სწავლების ალგორითმების უფრო ღრმა ინტეგრაციას, IoT მოწყობილობების უსაფრთხოების სპეციალიზებულ მოდელირებას და დიდი მონაცემების ანალიტიკის გამოყენებას რისკების პროგნოზირებისთვის.

გამოყენებული ლიტერატურა:

1. ENISA. (2023). *Threat Landscape Report 2023*. European Union Agency for Cybersecurity.
2. Fenton, N., & Neil, M. (2019). *Risk Assessment and Decision Analysis with Bayesian Networks*. CRC Press.
3. Hubbard, D., & Evans, D. (2010). *Problems with scoring methods and Monte Carlo simulation*. Wiley.
4. ISO. (2022a). *ISO/IEC 27001: Information security management systems – Requirements*. International Organization for Standardization.
5. NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology.
6. Sarker, I. H., et al. (2021). AI-driven cybersecurity: machine learning and deep learning for cyber threat intelligence. *Symmetry, 13*(2), 251.
7. Stamatis, D. H. (2003). *Failure Mode and Effect Analysis: FMEA from Theory to Execution*. ASQ Quality Press.

Information Systems Risk Analysis and Control in Testing Laboratories

Tamar Tsereteli, Nona Otkhozoria, David Kapanadze

Georgian Technical University

t_tsereteli@gtu.ge, n.otkhozoria@gtu.ge, david@gtu.ge

Abstract

The article examines modern approaches to the analysis and control of information system risks in ISO/IEC 17025 accredited laboratories. Particular attention is given to the reliability of measurement data related to transformer electrical parameters, the compromise of which can significantly impact the safety and economic stability of the energy sector. The novelty of the research lies in the development of an integrated model that combines international standards (ISO/IEC 27001, ISO/IEC 17025, NIST, ENISA), mathematical modeling methods (Bayesian networks, Fault Tree Analysis, Monte Carlo simulation), and both preventive and reactive security mechanisms (MFA, SIEM, backup recovery plans). The results demonstrate that the proposed model significantly reduces the probability of risk occurrence and potential economic loss, increases the number of identified threats, and provides deeper insight into critical cause-effect relationships. The presented approach offers an effective tool for enhancing the resilience and security of information systems in accredited laboratories.

Keywords : Information systems, Risk analysis, Risk control, ISO/IEC 17025, ISO/IEC 27001