

აკადემიური საზოგადოების როლი კიბერუსაფრთხოების ცნობიერების ამაღლებაში

ავთანდილ ბიჩნიგაური¹, იოსებ ქართველიშვილი¹, ზებურ ბერიძე²

¹საქართველოს ტექნიკური უნივერსიტეტი,

²ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტი

bichnigauri_av@gtu.ge, s.kartvelishvili@gtu.ge, zazaber2020@gmail.com

რეზიუმე

კიბერუსაფრთხოება თანამედროვე ციფრულ ეპოქაში ერთ-ერთი ყველაზე მნიშვნელოვანი გამოწვევაა, რომელიც ეხება როგორც ინდივიდებს, ისე სახელმწიფოებსა და საერთაშორისო ორგანიზაციებს. მოცემულ სტატიაში განხილულია აკადემიური საზოგადოების – კერძოდ, ლექტორებისა და სტუდენტების – კრიტიკული როლი კიბერუსაფრთხოების ცნობიერების ამაღლების პროცესში. კვლევის საფუძველზე დასკვნა გაკეთდა, რომ აკადემიური საზოგადოების აქტიური ჩართულობა უზრუნველყოფს ცოდნის გავრცელებას, კიბერჰიგიენის კულტურის გაძლიერებას და ქვეყნის კიბერმდებლობის ზრდას. სტატიაში გამოვლინდა ინსტიტუციური მექანიზმები, რომლებიც ხელს უწყობენ უსაფრთხო ციფრული გარემოს ჩამოყალიბებას, და შემოთავაზებულია კოლაბორაციული მოდელი ლექტორებისა და სტუდენტების ურთიერთთანამშრომლობისთვის.

საკვანძო სიტყვები: კიბერუსაფრთხოება, აკადემიური საზოგადოება, ცნობიერება, კიბერჰიგიენა, პედაგოგიკა, სასწავლო პროგრამა, CTF ღონისძიებები, ფიშინგი, კოლაბორაცია.

1. შესავალი.

თანამედროვე ციფრულ სამყაროში კიბერუსაფრთხოება ეროვნული და გლობალური უსაფრთხოების ერთ-ერთ მთავარ გამოწვევად იქცა. კიბერშეტევების მასშტაბები და სიხშირე განუწყვეტლივ იზრდება, რაც საფრთხეს უქმნის კრიტიკულ ინფრასტრუქტურას, ბიზნესს და პირად მონაცემთა კონფიდენციალურობას. ამ პირობებში, მხოლოდ ტექნიკური გადაწყვეტილებები არასაკმარისია, აუცილებელია ცნობიერების ამაღლება და კიბერჰიგიენის კულტურის ჩამოყალიბება.

აკადემიური საზოგადოება, როგორც ცოდნის გენერატორი და გადამცემი, ამ პროცესში გადამწყვეტ როლს ასრულებს. უნივერსიტეტები და სასწავლო დაწესებულებები წარმოადგენენ იმ სივრცეებს, სადაც ყალიბდებიან მომავალი სპეციალისტები და მიმდინარეობს სამეცნიერო კვლევები. ლექტორებისა და სტუდენტების აქტიური ჩართულობა უზრუნველყოფს არა მხოლოდ სპეციალისტების მომზადებას, არამედ ცოდნის გავრცელებას უფრო ფართო საზოგადოებაში.

კვლევის მიზანია ლექტორებისა და სტუდენტების ჩართულობის ანალიზი კიბერუსაფრთხოების ცნობიერების ამაღლების პროცესში და იმ ინსტიტუციური მექანიზმების გამოვლენა, რომლებიც უზრუნველყოფენ უსაფრთხო ციფრული გარემოს ჩამოყალიბებას.

2. მეთოდოლოგია.

კვლევა ეფუძნება შემდეგ მეთოდოლოგიურ მიდგომებს:

1. **ლიტერატურის ანალიზი:** გაანალიზებულია სამეცნიერო ნაშრომები, სტატიები და შემაჯამებელი ანგარიშები, რომლებიც ეხება კიბერუსაფრთხოების პედაგოგიკას, საზოგადოებრივ ცნობიერებას და აკადემიური საზოგადოების როლს.

2. **საქმის შესწავლა (Case Study):** შესწავლილი იქნა რამდენიმე უნივერსიტეტის გამოცდილება, სადაც წარმატებითაა დანერგილი კიბერუსაფრთხოების საგანმანათლებლო პროგრამები და სტუდენტური ინიციატივები.
3. **პრაქტიკული ინსტრუმენტების ანალიზი:** განხილულია კონკრეტული პრაქტიკული ინსტრუმენტები, როგორცაა ფიშინგის სიმულაციები, CTF (Capture The Flag) შეჯიბრებები, ჰაკათონები და კიბერუსაფრთხოების სასწავლო მოდულები.

3. მსჯელობა.

1. კიბერუსაფრთხოება, როგორც პედაგოგიური და სოციალური პროცესი

ტრადიციულად, კიბერუსაფრთხოება განიხილებოდა, როგორც ტექნიკური დისციპლინა. თუმცა, თანამედროვე გაგებით, ის უფრო ფართო პედაგოგიური და სოციალური პროცესია. ეფექტური კიბერუსაფრთხოება მოითხოვს არა მხოლოდ ტექნიკურ უნარებს, არამედ ქცევით ცვლილებებს და კრიტიკულ აზროვნებას. აკადემიური საზოგადოება სწორედ ის პლატფორმაა, სადაც შესაძლებელია ამ ცვლილებების განხორციელება. ლექტორებს შეუძლიათ შეიმუშაონ პედაგოგიური მიდგომები, რომლებიც ხელს შეუწყობენ სტუდენტებში პასუხისმგებლიანი ციფრული ქცევის ჩამოყალიბებას.

2. ლექტორებისა და სტუდენტების კოლაბორაციული მოდელი

კვლევა ასკვნის, რომ ყველაზე ეფექტური მიდგომაა ლექტორებისა და სტუდენტების კოლაბორაციული მოდელის დანერგვა. ეს მოდელი გულისხმობს:

- **ლექტორების როლი:** ლექტორები არიან მენტორები და ცოდნის წყარო. მათი მოვალეობაა კიბერუსაფრთხოების პრინციპების ინტეგრაცია სხვადასხვა საგნების სასწავლო პროგრამებში, არა მხოლოდ ტექნიკურ დისციპლინებში. მაგალითად, იურიდიულ საგნებში შესაძლებელია კიბერკრიმინალის საკითხების განხილვა, ხოლო ბიზნეს-ადმინისტრირებაში – რისკების მენეჯმენტის.
- **სტუდენტების როლი:** სტუდენტები არიან არა მხოლოდ პასიური მსმენელები, არამედ აქტიური მონაწილეები. მათ შეუძლიათ ჩამოაყალიბონ სტუდენტური კლუბები, ორგანიზება გაუწიონ CTF შეჯიბრებებს და ჰაკათონებს, რაც ხელს უწყობს პრაქტიკული უნარების განვითარებას და თანატოლებს შორის ცოდნის გაზიარებას.

ეს თანამშრომლობა ქმნის დინამიკურ გარემოს, სადაც თეორიული ცოდნა პრაქტიკულ გამოცდილებას ემატება.

3. აკადემიური ჩართულობის გავლენა საზოგადოებრივ ცნობიერებაზე

აკადემიური საზოგადოების გავლენა არ შემოიფარგლება უნივერსიტეტის კედლებით. სტუდენტები და ლექტორები არიან საზოგადოების განუყოფელი ნაწილი. მათ მიერ მიღებული ცოდნა და ჩამოყალიბებული უნარები ნაკადად ვრცელდება ოჯახებში, მეგობრების წრეში და სამუშაო გარემოში. ლექტორები, როგორც ექსპერტები, მონაწილეობენ საზოგადოებრივ ლექციებში, კონსულტაციებში და მედიაში, რითიც ხელს უწყობენ ფართო საზოგადოების ინფორმირებას. ამრიგად, აკადემიური საზოგადოება ასრულებს "მულტიპლიკატორის" როლს კიბერუსაფრთხოების ცოდნის გავრცელებაში.

4. შედეგები.

კვლევისა და პრაქტიკული გამოცდილების ანალიზის საფუძველზე, შემდეგი შედეგები იქნა მიღებული:

1. **კვლევითი შედეგები:** ჩატარებული გამოკითხვები აჩვენებს, რომ საგანმანათლებლო დაწესებულებებში, სადაც კიბერუსაფრთხოების თემები ინტეგრირებულია სასწავლო

პროგრამაში, სტუდენტებს შორის ცნობიერების დონე მნიშვნელოვნად მაღალია. მაგალითად, ფიშინგის სიმულაციის ჩატარების შემდეგ, მონაწილე სტუდენტებმა დაიწყეს უფრო ფრთხილად მიუდგნენ ელექტრონული ფოსტის გახსნას და საეჭვო ბმულებზე დაწკაპუნებას.

2. **სასწავლო მოდულების ეფექტურობა:** კიბერპიგიენის სასწავლო მოდულები, რომლებიც მოიცავს პაროლების მენეჯმენტს, ორფაქტორიან აუტენტიფიკაციას და სოციალური ინჟინერიისგან თავდაცვას, პრაქტიკულად ეფექტური აღმოჩნდა სტუდენტების ყოველდღიურ ციფრულ ცხოვრებაში.
3. **პრაქტიკული ღონისძიებების წარმატება:** CTF შეჯიბრებებმა და ჰაკათონებმა აჩვენა, რომ ისინი არა მხოლოდ ავითარებენ პრაქტიკულ უნარებს, არამედ აღძრავენ სტუდენტების ინტერესს კიბერუსაფრთხოების სფეროსთან მიმართებაში და ხელს უწყობენ გუნდური მუშაობის განვითარებას.
4. **ლექტორების პროფესიული განვითარება:** ლექტორების მიერ რეალური ქეისების ანალიზი და სპეციალიზებულ სემინარებში მონაწილეობა ხელს უწყობს მათი კვალიფიკაციის ამაღლებას, რაც პირდაპირ აისახება სასწავლო პროცესის ხარისხზე.
5. **ინსტიტუციური თანამშრომლობა:** დადგინდა, რომ აკადემიის, ინდუსტრიის და სახელმწიფო ორგანოების (მაგ., კიბერუსაფრთხოების ცენტრების) თანამშრომლობა ქმნის მდგრად ეკოსისტემას, რომელიც უზრუნველყოფს რესურსებს, აქტუალურ ინფორმაციას და სტაჟირების შესაძლებლობებს.

5. დასკვნა.

აკადემიური საზოგადოების ჩართულობა კრიტიკული ფაქტორია კიბერუსაფრთხოების ცნობიერების ამაღლებისთვის. ლექტორებისა და სტუდენტების ერთობლივი ძალისხმევა ქმნის მდგრად და დაცულ ციფრულ ეკოსისტემას. მათი როლი სტრატეგიულია და ღრმა გავლენა აქვს როგორც საგანმანათლებლო სისტემის შიგნით, ასევე მის ფარგლებს გარეთ, ფორმირდება საზოგადოებრივი აზროვნება და ქცევა ციფრულ სივრცეში.

კვლევამ აჩვენა, რომ კიბერუსაფრთხოება უნდა განიხილებოდეს როგორც მულტიდის-ციპლინარული და სოციალურ-პედაგოგიური საკითხი. კოლაბორაციული მოდელი, რომელიც აერთიანებს ლექტორების მენტორულ როლს და სტუდენტების აქტიურ ინიციატივას, არის ყველაზე პერსპექტიული გზა კიბერპიგიენის კულტურის ჩამოყალიბებისთვის.

პირველ რიგში, დადასტურდა, რომ კიბერუსაფრთხოების გაგება, როგორც ტექნიკური დისციპლინისა, არასაკმარისი და მომველბულია. ეფექტურობის მისაღწევად აუცილებელია მისი პედაგოგიური და სოციალური კომპონენტების აღიარება. ეს ნიშნავს, რომ უნივერსიტეტებმა უნდა განიხილონ კიბერუსაფრთხოება, როგორც ცოდნისა და უნარების ერთობლიობა, რომელიც ინტეგრირებული უნდა იყოს სხვადასხვა საგნობრივ კურსებში – იურის-პრუდენციიდან ბიზნეს-მენეჯმენტამდე და სოციოლოგიიდან ჟურნალისტიკამდე. მხოლოდ ამ გზით შეიძლება ჩამოყალიბდეს ყოვლისმომცველი, კრიტიკული აზროვნება, რომელიც აუცილებელია თანამედროვე დაუცველობების გასაგებად და მათ წინააღმდეგ ბრძოლაში.

მეორეც, კვლევამ მკაფიოდ გამოხატა ლექტორებისა და სტუდენტების კოლაბორაციული მოდელის ეფექტურობა. ლექტორები, როგორც მენტორები და ექსპერტები, უზრუნველყოფენ თეორიულ ბაზას, მეთოდოლოგიურ მხარდაჭერას და რეალური მსოფლიოს შემთხვევების ანალიზს, ხოლო სტუდენტები სტუდენტური კლუბების, CTF შეჯიბრებებისა და ჰაკათონების მეშვეობით ავრცელებენ ცოდნას თანატოლებს შორის, ქმნიან ინოვაციურ გადაწყვეტილებებს

და აძლიერებენ საზოგადოების ჩართულობას. ეს ორმხრივი პროცესი ქმნის დინამიკურ და მდგრად გარემოს, სადაც თეორია და პრაქტიკა ერთმანეთს ავსებს.

მესამე, აკადემიური საზოგადოების გავლენა მნიშვნელოვნად სცილდება უნივერსიტეტის კედლებს. სტუდენტები და ლექტორები არიან „ცოდნის მულტიპლიკატორები“. მათ მიერ შეძენილი ცოდნა და უნარები ნაკადად ვრცელდება ოჯახებში, მეგობრების წრეში და, საბოლოოდ, სამუშაო ადგილებზე. ლექტორები, საჯარო ლექციების, მედიასივრცეში გამოსვლების და საზოგადოებასთან თანამშრომლობის მეშვეობით, ხელს უწყობენ ფართო საზოგადოებას კიბერსაფრთხეებისგან თავდაცვაში. ამრიგად, ინვესტიცია აკადემიურ გარემოში იწვევს მულტიპლიკაციურ ეფექტს და ხელს უწყობს მთელი ქვეყნის ცნობიერების ამაღლებას კიბერუსაფრთხოებაში.

სამომავლოდ, ამ პოზიტიური ტენდენციების გასაძლიერებლად აუცილებელია რამდენიმე სტრატეგიული ნაბიჯის გადადგმა:

- **საგანმანათლებლო პოლიტიკის რეფორმა:** კიბერუსაფრთხოება უნდა იქცეს ძირითად კომპეტენციად ყველა საგანმანათლებლო დონეზე, ხოლო უმაღლეს განათლებაში – სავალდებულო მოდულად ან საბაზისო კურსად ყველა სპეციალობისთვის.
- **ლექტორთა განუწყვეტელი პროფესიული განვითარება:** უნდა შეიქმნას სისტემატური პროგრამები ლექტორთა კვალიფიკაციის ასამაღლებლად, მათ შორის სერტიფიცირებული კურსები, სემინარები ინდუსტრიის ექსპერტებთან თანამშრომლობით და მოწინავე სასწავლო მეთოდების დანერგვა.
- **ინფრასტრუქტურული მხარდაჭერა სტუდენტური ინიციატივებისთვის:** უნივერსიტეტმა უნდა უზრუნველყონ ფინანსური, ტექნიკური და ადმინისტრაციული რესურსები სტუდენტური კიბერუსაფრთხოების კლუბებისთვის, ლაბორატორიებისთვის და ღონისძიებებისთვის, რაც ხელს შეუწყობს პრაქტიკული გამოცდილების მიღებას და ინოვაციების წახალისებას.
- **ე.წ. „სამმაგი სპირალის“ მოდელის გაძლიერება:** აკადემიური საზოგადოების, ბიზნეს სექტორის და სახელმწიფო ორგანოების თანამშრომლობა უნდა გახდეს სისტემატური და სტრუქტურირებული. ეს მოიცავს ერთობლივ კვლევით პროექტებს, სტაჟირების პროგრამებს, კონსულტაციებს და ერთობლივი სტანდარტებისა და რეკომენდაციების შემუშავებას.

მხოლოდ კოორდინირებული და კოლექტიური ძალისხმევის შედეგად შევძლებთ ცნობიერების დონე ავამაღლოთ და გავუმკლავდეთ კიბერსაფრთხეების კომპლექსურ გამოწვევებს თანამედროვე ციფრულ სამყაროში.

გამოყენებული ლიტერატურა:

1. ა. ბიჩნიგაური, ი. ქართველიშვილი, ლ. შონია - „ფიშინგისა და მავნე კოდის მქონე ვებგვერდების პრევენციის ეფექტური მექანიზმის მოდელის შემუშავება და რეალიზაცია ვებბრაუზერის გარემოში“, საქართველოს ტექნიკური უნივერსიტეტის საერთაშორისო სამეცნიერო-პრაქტიკული კონფერენცია „თანამედროვე გამოწვევები და მიღწევები ინფორმაციულ ტექნოლოგიებში - 2023“
2. ა. ბიჩნიგაური, ი. ქართველიშვილი, ლ. შონია - Unveiling Quishing: The Dark Side of QR Codes in Cyber attacks, ჟურნალი „თავდაცვა და მეცნიერება“. ტომ. No. 2 (2023), DOI: <https://doi.org/10.61446/ds.2.2023.7412>

3. ა. ბიჩნიგაური, ი. ქართველიშვილი, ლ. შონია - Strengthening Cyber Defenses - The Crucial Role of Phishing Simulation in Modern Security Strategies, ჟურნალი „თავდაცვა და მეცნიერება“. ტომ. No. 3 (2024), DOI: <https://doi.org/10.61446/ds.3.2024.8467>
4. კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების 2025-2030 წლების სტრატეგია - <https://dga.gov.ge/files/mUMPR8s3w59z.pdf>
5. ENISA (European Union Agency for Cybersecurity). (2021). Cybersecurity Education in the EU.

The Role of the Academic Community in Raising Cybersecurity Awareness

Avtandili Bichnigauri¹, Ioseb Kartvelishvili¹, Zebur Beridze²

¹Georgian Technical University

²Batumi Shota Rustaveli State University

bichnigauri_av@gtu.ge, s.kartvelishvili@gtu.ge, zazaber2020@gmail.com

Abstract

Cybersecurity is one of the most important challenges in the modern digital era, affecting both individuals, states, and international organizations. This article discusses the critical role of the academic community – in particular, lecturers and students – in raising awareness of cybersecurity. Based on the research, it was concluded that the active involvement of the academic community ensures the dissemination of knowledge, strengthening the culture of cyber hygiene and increasing the country's cyber resilience. The article identifies institutional mechanisms that contribute to the formation of a safe digital environment, and proposes a collaborative model for interaction between lecturers and students.

Keywords: Cybersecurity, Academic Community, Awareness, Cyber Hygiene, Pedagogy, Curriculum, CTF Events, Phishing, Collaboration.