

UDC 004; 3; 351.746

SCOPUS CODE 1700; 3300; 3320

<https://doi.org/10.36073/1512-0996-2024-1-108-120>

აკადემიური სამეცნიერო კვლევების სფეროსა და არეალის გაფართოება ინფორმაციულ ეპოქაში

ჰენრი კუპრაშვილი პოლიტიკისა და საერთაშორისო ურთიერთობების დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 77
E-mail: kuprashvilihenri07@gtu.ge

რეცენზენტები:

ო. შონია, სტუ-ის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის პროფესორი, ტექნიკის მეცნიერებათა დოქტორი

E-mail: o.shonia@gtu.ge

დ. ხუფენია, სტუ-ის სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტის ასისტენტ-პროფესორი, საერთაშორისო ურთიერთობების დოქტორი

E-mail: khupenia.d@gtu.ge

ანოტაცია. თემა ეხება სამეცნიერო კვლევების სფეროსა და არეალის გაფართოების მიმდინარე პროცესის ანალიზს. ინტერნეტტექნოლოგიებმა შეცვალა პოლიტიკური, ეკონომიკური, სოციალური რეალობა. მრავალსვლიანი კომბინაციური სამიზნე უშიშროების უზრუნველყოფის მექანიზმები აღმოჩნდა. მონაცემები მიუთითებს, რომ არაპროგნოზირებად საშიშროებებთან გამკლავებამ მოითხოვა ყველა დონეზე სერიოზული სოციალურ-პოლიტიკური გადაწყვეტილებების მიღება, პოლიტიკური, სამართლებრივი, ეკონომიკური, სამხედრო-თავდა-

ცვითი და სოციალური ღონისძიებების გატარება, ახალი ნორმატიული რეგულირების სისტემების შემუშავება. შესაბამისად, კიბერსივრცის პრობლემებმა წინ წამოსწია მეცნიერების სხვადასხვა დარგის მკვლევრების როლი, გააფართოვა აკადემიური სამეცნიერო კვლევების სფერო და არეალი. აქტუალური გახდა ამ მიმართულებით მიმდინარე სამეცნიერო-კვლევით პროცესებში ქართველ მკვლევართა აქტიური ჩართულობა. ამასთან ერთად, გამოიკვეთა ქართველ მკვლევართა მიერ სოციალურ-პოლიტიკურ კონტექსტში კიბერსივრცის პრობლემების კვლევის დროს ტერმინების გამოყენების დაზუსტე-

ბის საკითხიც. კიბერუსაფრთხოების, როგორც ტექნიკური პრობლემის განხილვიდან მის სოციალურ-პოლიტიკურ ამოცანად, კიბერუშიშროებად ტრანსფორმირების შემდეგ, ანუ როდესაც გაზრდილი საშიშროების თავიდან ასარიდებლად იცვლება საქმიანობის შინაარსი, საჭირო ხდება ტერმინების სოციალური მეცნიერებების სფეროს კონტექსტით გამოყენება, რადგან ცვლილებები ეხება არა მხოლოდ უსაფრთხოების ტექნიკასთან დაკავშირებულ საქმიანობას, არამედ ადამიანის, საზოგადოებისა და სახელმწიფოს სოციალურ-პოლიტიკურ მოღვაწეობას, სოციალურ-პოლიტიკური ხასიათის ღონისძიებათა დასახვასა და განხორციელებას (პოლიტიკის შემუშავება, კონცეფცია, დაგეგმვა და სხვ.). საკვლევად ამ პრობლემის ცალკე გამოყოფა ესადაგება სოციალურ მეცნიერებებში არსებული ვითარების საჭიროებებს. შესაბამისად, შეტანილია კონკრეტული წვლილი შესაძლო ტენდენციების სტრატეგიული შეფასებების კვლევაში.

საკვანძო სიტყვები: განათლების სტანდარტული კლასიფიკაცია; კიბერსივრცე; კიბერუსაფრთხოება; კიბერუშიშროება; მეცნიერული ცოდნის სისტემა; სამეცნიერო კვლევა; ტერმინი.

შესავალი

ბოლო ათწლეულების მოვლენების შესწავლამ დაგვანახა, რომ ინფორმაციულ ეპოქაში სოციალურ-პოლიტიკური სისტემის განვითარების ერთ-ერთი მთავარი ფაქტორი გახდა ინფორმაციის წარმოება და გამოყენება. ის გადამწყვეტ როლს ასრუ-

ლებს არა მხოლოდ საზოგადოებრივი და სახელმწიფო ინსტიტუტების, არამედ თითოეული ადამიანის ცხოვრებაშიც და მსოფლიოსთან კომუნიკაციის ერთადერთი რეალობაა. კომპიუტერები და საინფორმაციო-სატელეკომუნიკაციო ციფრული სისტემები გამოიყენება ყოველდღიურობაში, ადამიანის, საზოგადოებისა და სახელმწიფოს საქმიანობის ყველა სფეროში - ეროვნული უშიშროების უზრუნველყოფასა თუ მთლიანად სახელმწიფო მმართველობაში (ჯანდაცვა, განათლება, საბინაო და კომუნალური მომსახურება, საჰაერო და სარკინიგზო კომუნიკაციები, ვაჭრობა და სხვ.).

მსოფლიო ქსელის გაჩენასთან ერთად, სახელმწიფო თანდათან კარგავს გარკვეულ ფუნქციებს, მცირდება მისი როლი და გავლენა ადამიანთა ურთიერთობებზე, სახელმწიფო საზღვარი იცვლის პირვანდელ დანიშნულებას. მაგალითად, კიბერტერორისტებს შეუძლიათ „შეიჭრან“ სხვა სახელმწიფოს ფარგლებში, ჩაატარონ დანაშაულებრივი ოპერაციები და დიდი ზარალი მიაყენონ ქვეყანას. ასევე შეიცვალა ომის რაობა, მისი გაგების სტანდარტები.

ამდენად, მე-20 საუკუნის მეორე ნახევრიდან სამხედრო შეიარაღებული ომებისა და კონფლიქტების კლასიკურ სახეებს თანდათან ენაცვლება დაპირისპირების ახალი ფორმები, მათ შორის არის კიბერტერორიზმი, კიბერომი. საომარი მოქმედებისა და დაპირისპირების არეალი კი გახდა კიბერსივრცე – საინფორმაციო-სატელეკომუნიკაციო ტექნოლოგიური ინფრასტრუქტურის ურთიერთკავშირის კომპლექსი, რომელიც მოიცავს ინტერნეტის გლობალურ ქსელს, კომპიუტერულ სისტემებს,

სატელეკომუნიკაციო ქსელებსა და პროცესორებს. კიბერსივრცე არ არსებობს რაიმე ფიზიკური ფორმით, იგი ურთულესი ვირტუალური გარემოა, რომელიც წარმოიქმნება ადამიანებს, პროგრამულ უზრუნველყოფას, ინტერნეტმომსახურებას, ტექნოლოგიურ მოწყობილობებს, ქსელებსა და ქსელური კავშირების საშუალებებს შორის ურთიერთქმედების შედეგად.

ომის მეხუთე ფორმამ – კიბერომმა (სახმელეთო, საზღვაო, საჰაერო და კოსმოსური განზომილებების გვერდით), ინფორმაციულ ეპოქაში საინფორმაციო-ტექნოლოგიური უპირატესობის მოპოვების მცდელობებმა წარმოშვა ახალი საშიშროებანი, სადაც არავინ ემორჩილება დაწესებულ შეზღუდვებსა და აკრძალვებს.

კიბერსივრცის დაცვის პრობლემის აქტუალურობა განპირობებულია საინფორმაციო-საკომუნიკაციო და კიბერტექნოლოგიების არნახული განვითარების ფონზე კიბერთავდასხმების განუსაზღვრელი მასშტაბების შეუქცევადი პროცესებით, რომლებიც მთელი მსოფლიოს წინაშე აყენებს უშიშროების უზრუნველყოფის ზომების გაძლიერების აუცილებლობას. წარმოქმნილ საშიშროებასთან გამკლავებამ თავისთავად მოითხოვა ეროვნული და საერთაშორისო დონის სერიოზული სოციალურ-პოლიტიკური გადაწყვეტილებები, ასევე, აკადემიური კვლევები, ახალი პოლიტიკური თეორიების, ახალი ნორმატიული მოთხოვნების, რეგულირების სისტემების, სოციალური ნორმებისა და სხვ. შემუშავება.

პრობლემის გადასაჭრელად, თუ მანამდე, კომპიუტერის დაბადების შემდგომ მოკლე პერიოდში, საკმარისი იყო ინფორმაციკის სპეციალისტების

მიერ მიღებული ტექნიკური ზომები, დღეს უკვე პოლიტიკური, სამართლებრივი, ეკონომიკური, სამხედრო-თავდაცვითი და სოციალური ღონისძიებების გატარებაა საჭირო.

მირიამ დან კაველტი (Myriam Dunn Cavelty), **ქრისტინე ერიკსენი** (Christine Eriksen) და **ბენჯამინ შარტე** (Benjamin Scharte) ერთობლივ სტატიაში – „კიბერუშიშროების მდგრადობის გაზრდა: ტექნოლოგიური გამართულობა მოითხოვს სოციალურ მოსაზრებებს“, აღნიშნავენ: იმის ნაცვლად, რომ ვიფიქროთ კიბერუშიშროებაზე, როგორც „ტექნიკურ პრობლემაზე + ადამიანებზე“, ჩვენ ვთავაზობთ კიბერუშიშროების კონცეპტუალიზაციას, როგორც „სოციალური პრობლემა + ტექნოლოგია“. ჩვენ გამოვყოფთ მკვლევართა, პოლიტიკის „მკეთებელთა“ და პრაქტიკოსთა წარმატების სამ გზას: ინტერდისციპლინური კვლევა, საჯარო დებატები არაერთი ნორმატიული საკითხის შესახებ და პოლიტიკასა და პოლიტიკის შემუშავებაში გაურკვევლობის თავიდან ასაცილებლად განხილვების აუცილებლობა [1].

21-ე საუკუნეში შექმნილი ახალი რეალობიდან გამომდინარე კიბერსივრცის კვლევაში ინფორმაციკოსებთან ერთად ჩაებნენ კვლევების საკუთარი სპეციფიკის შესაბამისად უკვე სოციალური, ჰუმანიტარული, სამართლის, სამხედრო და სხვა სამეცნიერო სფეროების სპეციალისტებიც.

კიბერუშიშროებისა და კიბერდაცვის შვეიცარიელი სპეციალისტი, დოქტორი **რობერტ დიუარი** (Robert Dewar) აღნიშნავს, რომ სულ უფრო მზარდია კიბერსივრცისადმი ყურადღება პოლიტიკოსებისა და სამხედროების მხრიდან, რადგან კიბერუშიშროება უკვე სამართლებრივი, სამხედრო და ეკონომი-

მიკური გამოწვევაა. ამ გლობალურ პრობლემას ვერც ერთი სახელმწიფო დამოუკიდებლად, მხოლოდ საკუთარი ძალებითა და რესურსებით ვერ გაუმკლავდება [2]. ბოლო ათწლეულში დასავლეთ ევროპის სამეცნიერო წრეებში გაჩნდა პლეადა კიბერუმიშროების პრობლემებზე მომუშავე მკვლევრებისა, რომლებიც ამ თვალსაზრისს ავითარებენ [3,4].

კვლევის ჰიპოთეზა ემყარება ავტორის ვარაუდს, რომ დღეს კიბერსივრიდან მომდინარე გლობალურმა საშიშროებამ მსოფლიოში პრობლემის გადასაჭრელად აქტუალური გახადა პოლიტიკოსების, სამხედროების და მეცნიერების სხვადასხვა დარგის მკვლევრების ძალისხმევის გაზრდა ერთობლივი საქმიანობის გააქტიურების მიმართულებით.

ამ პირობებში აუცილებელია საქართველოში პოლიტიკოსების, სამხედროებისა და მეცნიერების სხვადასხვა დარგის მკვლევრების საერთო ძალისხმევა მათ საქმიანობაში სინქრონიზმის მიღწევისა და მისი სრულყოფისათვის.

ძირითადი ნაწილი

მეთოდოლოგია

ნაშრომის თეორიული ბაზა მოიცავს სისტემების ზოგად თეორიას (Systems theory), რადგან იგი ეფუძნება კვლევის ობიექტების, მოვლენების ან პროცესების ერთიან ხედვას და წარმოადგენს უნივერსალურ და ადეკვატურ მეთოდს ზოგადად მეცნიერებაში ანალიზისა და გამოკვლევისათვის.

ეროვნული უშიშროებისათვის, მათ შორის – კიბერუმიშროებისათვის, მისი უზრუნველყოფის პროცესებისათვის საფრთხეების, მუქარებისა და რისკების პრევენცია ვერ მიიღწევა პროცესებზე გარ-

კვეული საინფორმაციო და მმართველობითი უემოქმედების გარეშე. დიალექტიკის უმნიშვნელოვანესი მოთხოვნა არის რეალობისადმი მიდგომა, მისი ურთიერთგამომრიცხავი განვითარებისა და მრავალფეროვანი კავშირების გათვალისწინებით. პრაქტიკის წინააღმდეგობებისა და უშიშროების საკითხებზე მისი ამსახველი თეორიის გამოვლენა და ანალიზი, რომელიც ასახავს მას, საფუძვლად უდევს კვლევის მთელ პროცესს და განსაზღვრავს სხვა მეთოდების ბუნებას.

სოციალური მეცნიერებების და ეროვნული უშიშროების თეორიები წარმოდგენილია სისტემური ანალიზის მეთოდების გამოყენების გარეშე [5, 97-99]. ამ მეთოდების არსენალი საკმაოდ ფართოა და თითოეულს აქვს დადებითი და უარყოფითი მხარეები, ასევე გამოყენების სფერო, როგორც ობიექტის ტიპთან, ისე მისი კვლევის სტადიასთან მიმართებით.

ზოგადად წარმოდგენილი კვლევის თეორიულ-მეთოდოლოგიური საფუძველია სოციალური მეცნიერებების, საერთაშორისო ურთიერთობებისა და ეროვნული უშიშროების თეორიების ძირითადი იდეები და დებულებები; ამ სამეცნიერო მიმართულებებში დამკვიდრებული პოლიტიკური ანალიზისა და სინთეზის, კლასიფიკაციისა და სისტემატიზაციის, თეორიული განზოგადების, აღწერის მეთოდები.

მზარდი საშიშროება და სამეცნიერო-კვლევითი არეალის გაფართოება

საინფორმაციო ეპოქაში კიბერუსაფრთხოების უზრუნველყოფის ტექნიკური პრობლემა ტექნიკური ხასიათის საქმიანობიდან თანდათან გაფარ-

თოვდა, გამრავალფეროვნდა და გადაიქცა პოლიტიკური ამოცანების გადაჭრის პრობლემად. შესაბამისად, ინფორმაციული ტექნოლოგიის სამეცნიერო სფეროს გარდა, საქმეში ებმება სოციალური და ჰუმანიტარული მეცნიერებების სფეროებიც. ამის დასტურია კიბერსივრცის „საფრთხეების პოლიტიკის“ აღიარებული მკვლევრის, ციურიხის უშიშროების კვლევის ცენტრის ვიცე-მენეჯერის, პროფესორ **მირიამ დან კაველტისა** (Myriam Dunn Cavelty) და ამავე ცენტრის დირექტორის, პროფესორ **ანდრეას ვენგერის** (Andreas Wenger) რედაქტორობით ნიუ-იორკში ახლახან გამოცემული წიგნი „კიბერუშიშროების პოლიტიკა: სოციალურ-ტექნოლოგიური გარდაქმნები და პოლიტიკური ფრაგმენტაცია“. მასში სხვადასხვა სამეცნიერო სფეროს 22 ავტორი განიხილავს კიბერუშიშროების ახალ და რთულ პოლიტიკურ ასპექტებს და წარმოადგენს მას, როგორც სოციალურ-ტექნოლოგიური გაურკვევლობისა და პოლიტიკური ფრაგმენტაციის მიერ განსაზღვრულ საკითხს. წიგნი არის მნიშვნელოვანი თემის ირგვლივ სტრუქტურირებული და მასში მოტანილია ემპირიული მაგალითები, თუ როგორ ურთიერთქმედებაშია სოციალურ-ტექნიკური ცვლილებები და სახელმწიფო და არასახელმწიფო აქტორების მიერ მიღებული პოლიტიკური ზომები დღევანდელ, გაურკვევლობითა და კიბერსაშიშროებით სავსე გარემოში [6].

ცნობილია, რომ გასული საუკუნის ბოლოდან ვირუსები არა მხოლოდ კომპიუტერების ვიწრო სამიზნედ, არამედ არაპროგნოზირებად დამაზიანებელ იარაღად იქცა და მსოფლიოსათვის კატასტროფული შედეგების მომტანი უზარმაზარი პრობლემა

გახდა. ვირუსების შემქმნელთათვის კიბერსივრცის ბრძოლის ველზე კომპიუტერი უკვე არა მიზანი, არამედ საშუალება ხდება, ხოლო მრავალსვლიანი კომბინაციური სამიზნე – ეროვნული უშიშროების უზრუნველყოფის მექანიზმები, სახელმწიფო და თავდაცვის სამხედრო ინფრასტრუქტურები.

საშიშროების წინაშე აღმოჩნდა როგორც სახელმწიფოები, ისე ცალკეული ქვეყნების ეროვნული უშიშროების უზრუნველყოფა, უფრო მეტიც, მთლიანად კაცობრიობა. ფაქტია, ინფორმაციულ ეპოქაში, კომპიუტერული სფეროს კომპონენტების დამაზიანებელი ციფრული ტექნოლოგიების არნახულად განვითარების კვალობაზე, კომპიუტერული ვირუსებისაგან წარმოქმნილი უზომოდ გამრავალფეროვნებული და არაპროგნოზირებადი საფრთხეები გასცდა კომპიუტერის ვიწრო მოქმედების ფარგლებს და საშიშროება შეუქმნა სახელმწიფოებრივი და საზოგადოებრივი ცხოვრების ყველა სფეროს, დაემუქრა ეროვნული უშიშროების ფუნდამენტურ ღირებულებებს: პიროვნების უშიშროებას, საზოგადოების უშიშროებასა და სახელმწიფო უშიშროებას, ეროვნული უშიშროების უზრუნველყოფის სისტემას.

ამ პრობლემაზე სულ უფრო მეტი მკვლევარი ამახვილებს ყურადღებას: „რამდენადაც ეს ტექნიკური სისტემები მჭიდრო კავშირშია და აერთიანებს საზოგადოებისა და ეკონომიკის მეტ ასპექტს, კიბერუშიშროებასთან დაკავშირებული პრობლემები გარდაუვლად გავრცელდება პოლიტიკის სულ უფრო მეტ სფეროებში როგორც ეროვნულ, ისე საერთაშორისო დონეზე. ეს მოვლენები შექმნის ახალ მოთხოვნებს ტექნიკური და ორგანიზაციული

კვლევებისათვის, რომლებიც უკეთესად უნდა იყოს ინტეგრირებული სოციალური და პოლიტიკური მეცნიერებების მიდგომებთან“ [7, 22-23]. მ. დან კაველი და ა. ვენგერი ხაზგასმით აღნიშნავენ, რომ „სულ უფრო თვალსაჩინო ხდება პოლიტიკური და სოციალური ასპექტები, რომლებიც გავლენას მოახდენს თანამშრომლობისა და კონფლიქტის მოდელებზე პოლიტიკასა და საზოგადოებაში ეროვნულ და საერთაშორისო დონეებზე“ [7, 23].

ცხადია, პრობლემა გასცდა ინფორმატიკის დარგის სპეციალისტების მიერ კომპიუტერების ტექნიკურად დაცვისათვის ანტივირუსების შექმნის ვიწრო სფეროს. გლობალურმა საშიშროებამ ბრძოლის ველზე გამოიყვანა პოლიტიკოსები და სამხედროები, ასევე მეცნიერების სხვადასხვა დარგში მომუშავე მკვლევრები, მნიშვნელოვნად გაფართოვდა აკადემიური სამეცნიერო კვლევების სფერო და არეალი. შექმნილია რეალობა:

პირველი, კომპიუტერების ტექნიკურად დაცვის საკითხებს ძირითადად იკვლევდნენ და იკვლევენ მხოლოდ ინფორმატიკის სპეციალისტები;

მეორე, კიბერუშიშროების პრობლემების კვლევაში ფართოდ ჩაებნენ სოციალური, ჰუმანიტარული, სამართლის, სამხედრო და სხვა სფეროების სპეციალისტები.

ამ პროცესში საქართველოც არის ჩართული. კიბერსივრცის პრობლემებს იკვლევენ არა მხოლოდ ინფორმაციისა და კომუნიკაციის ტექნოლოგიების სამეცნიერო დისციპლინის სფეროში, არამედ საგრძნობლად გაიზარდა „არაინფორმატიკოს“ მკვლევართა რიცხვი და მნიშვნელოვნად გაფართოვდა სხვადასხვა სამეცნიერო დისციპლინის არეალი (სოციალური, ჰუმანიტარული და სხვ.), მრავალი

სამეცნიერო სტატია გამოქვეყნდა და არაერთი დისერტაციაა დაცული [8]. ამ სხვადასხვა დისციპლინის სპეციალისტები საკუთარი სამეცნიერო დისციპლინის „გადასახედიდან“ „შეიჭრნენ“ სრულიად განსხვავებულ ტექნიკურ მეცნიერებათა სფეროში, სადაც ტექნიკური შინაარსის ტერმინი „უსაფრთხოება“ ძირითადად გამოიყენება ამ დისციპლინაში დამკვიდრებულ შესაბამის ტრადიციულ კონტექსტში, ანუ როდესაც კომპიუტერული და საინფორმაციო-სატელეკომუნიკაციო სფეროში შემავალი კომპონენტების (ქსელები, კომპიუტერები, პროგრამები, მონაცემები, მოწყობილობები) კიბერშეტევებისაგან (ციფრული თავდასხმები, დაზიანება, არაავტორიზებული წვდომა და სხვ.) ტექნიკურად დაცვაზეა საუბარი. კიბერუსაფრთხოების უზრუნველყოფა ამ შემთხვევაში უფრო „ტექნიკის“ საქმეა, „ტექნიკური“ საფრთხისაგან დაცვაა. მაგალითად, იგი უფრო ცნობილი „შრომის უსაფრთხოების დაცვასთან“ ასოცირდება და არა სოციალურ-პოლიტიკური მიზნების დასახვასთან. ე. ი. მოცემულ ობიექტზე კიბერუსაფრთხოების უზრუნველსაყოფად მისაღებია შესაბამისი ორგანიზაციულ-ტექნიკური ზომები: უნდა განისაზღვროს კომპიუტერული და საინფორმაციო-სატელეკომუნიკაციო სფეროს (ქსელები, კომპიუტერები, მოწყობილობები, პროგრამები, მონაცემთა ბაზები) ექსპლუატაციის უსაფრთხოებაზე პასუხისმგებელი პირი და დაინერგოს შესაბამისი ტექნიკური ინფრასტრუქტურა და უსაფრთხოების სისტემა [9] ანუ საქართველოში კომპიუტერული სამეცნიერო სფეროს დისციპლინები (ინფორმაციისა და კომუნიკაციის ტექნოლოგიები, კომპიუტერული ტექნოლოგიები, გამოთვლითი მანქანებისა და სისტემე-

ბის თეორია და სხვ.) იყენებენ ტექნიკური შინა-არსის ტერმინს „უსაფრთხოება“ (კომპიუტერული უსაფრთხოება, საინფორმაციო უსაფრთხოება, კიბერუსაფრთხოება), რომელშიც იგულისხმება კომპიუტერული და საინფორმაციო-სატელეკომუნიკაციო სფეროში შემავალი კომპონენტების (ქსელები, კომპიუტერები, პროგრამები, მონაცემები, მოწყობილობები) კიბერშეტევებისაგან (ციფრული თავდასხმები, დაზიანება, არავტორიზებული წვდომა და სხვ.) ტექნიკურად დაცვის ტექნოლოგიების, მეთოდებისა და პროცესების ერთობლიობა.

ცხადია, რომ კომპიუტერული სამეცნიერო სფეროს დისციპლინებისაგან განსხვავებით, **სოციალური, ჰუმანიტარული და სხვა მეცნიერებების წინაშე დგას ამოცანა საკუთარი დარგის სამეცნიერო სფეროში შეიტანოს წვლილი არა ტექნიკის, არამედ სოციალური, პოლიტიკური, ეკონომიკური და სხვ. თეორიის განვითარების კონტექსტით. ამ რეალობამ აშკარა გახადა საქართველოს სამეცნიერო სფეროს მკვლევართა მიერ კიბერსიფერში ტერმინების გამოყენების საკითხის დაზუსტების საჭიროებაც**, რადგან ინფორმატიკის კონტექსტში გამოყენებული **ტექნიკური ტერმინი „უსაფრთხოება“** ვერ ჯდება სოციალური მეცნიერების თეორიისათვის დამახასიათებელ შინაარსობრივ და ფუნქციურ დატვირთვაში.

ცნობილია, რომ რუსული ენიდან თარგმნილი და ხელოვნურად შემოტანილი ტექნიკური ტერმინი „უსაფრთხოება“ ქართულ ენაში პირველად გაჩნდა საბჭოთა პერიოდში. მანამდე ქართველთა მეტყველებაში ეს სიტყვა საერთოდ არ არსებობდა,

შესაბამისად არ არის შეტანილი ილია აბულაძის „ძველი ქართული ენის ლექსიკონში“ [10] და ზურაბ სარჯველაძის „ძველი ქართული ენის ლექსიკონში“ [11] ასევე, ნიკო ჩუბინაშვილის „ქართულ ლექსიკონში“ [12], დავით ჩუბინაშვილის „ქართულ-რუსულ ლექსიკონში“ [13] და, საერთოდ, 1957 წლამდე გამოცემულ ლექსიკონებში [14]. ტერმინ „უსაფრთხოების“ შემოღებამდე მისი ფუძე სიტყვა „უსაფრთხო“ პირველად დაფიქსირდა ტექნიკურ ლექსიკონებში 2-ჯერ, ისიც როგორც ტექნიკური ტერმინი: 1920-1921 წლებში გამოცემულ საქართველოს ტექნიკური საზოგადოების სატერმინო სექციის მიერ შექმნილ რუსულ-ქართული ტექნიკურ ლექსიკონში: Безопасный порох - უსაფრთხო დენთი და 1925 წელს გამოცემულ რუსულ-ქართული საგზაო ტექნიკურ ლექსიკონში: Безопасное движение – უსაფრთხო მოძრაობა; Безопасный порох - უსაფრთხო დენთი [15,16,17].

ქართულ ენაში ტერმინი „უსაფრთხოება“ ხელოვნურად შექმნეს და ხმარებაში შემოიღეს მაშინ, როდესაც დაიწყო ქართული ენის შევსება თარგმნილი ტექნიკური ტერმინებით, რისი ნაკლებობაც ქვეყნის იდუსტრიალიზაციის ფონზე უკვე იგრძნობოდა ქართულ ტექნიკურ მეტყველებაში. მაგალითად, ამ მიზნით გადმოაქართულეს რუსული ტერმინი „Техника безопасности“ („ტექნიკა ბეზოპასნოსტი“). ამ კონტექსტში „ბეზოპასნოსტის“ შესატყვისად ხელოვნურად მოიგონეს ტერმინი „უსაფრთხოება“ და თარგმანში მიიღეს „უსაფრთხოების ტექნიკა“.¹

¹ უსაფრთხოების ტექნიკა (ინგლ. ენაზე: Safety engineering) – მომუშავე პერსონალის უსაფრთხოების დაცვისაკენ მიმართული ტექნიკური და საორგანიზაციო ღონისძიებათა სისტემა.

ამ ახალ ტექნიკურ ტერმინს ქართულმა ავტორი-ტეტულმა ენათმეცნიერებამ თავიდანვე განუსაზღვრა გამოყენების სფერო და ხმარობდნენ ძირითადად ფიზიკურ და ტექნიკურ დაზიანებებთან დაკავშირებულ კონტექსტში: უსაფრთხოების ტექნიკა, ტექნიკური უსაფრთხოება, შრომის უსაფრთხოება და ა.შ. აქედან გამომდინარეობს ახალშექმნილი სიტყვებიც: უსაფრთხო სამართლებელი, უსაფრთხოების ღვედი, საგზაო უსაფრთხოება და სხვ. ქართულმა ენათმეცნიერებამ შეავსო ქართული ტექნიკური ტერმინოლოგია ხელოვნურად შექმნილი ტექნიკური ტერმინით და დაადგინა მისი გამოყენების არეალიც. რაც შეეხება კომპიუტერულ სამეცნიერო სფეროში მისი გამოყენების საკითხს: როდესაც საქართველოში დაიწყო კომპიუტერული მეცნიერების დანერგვა, გაჩნდა კომპიუტერები, ქსელები და ვირუსები, მაშინ, კომპიუტერების ვირუსებისაგან ტექნიკურად დაცვის უზრუნველყოფის პროცესში, შემოიღეს ტექნიკური ტერმინი „უსაფრთხოება“, რაც ზუსტად შეესაბამებოდა პროცესის შინაარსს და დღესაც სწორად გამოიყენება მეცნიერების ამ სფეროში.

რაც შეეხება სოციალურ, ჰუმანიტარულ და სხვ. მეცნიერებებს, ინფორმაციულ ეპოქაში შექმნილი რეალობიდან გამომდინარე, კარდინალური და მასშტაბური ცვლილებების ფონზე, როდესაც საქმე გვაქვს არსობრივად ახალ პროცესთან, ანუ **ხდება კიბერუსაფრთხოების, როგორც ტექნიკური პრობლემის განხილვიდან მის პოლიტიკურ ამოცანად (კიბერუშიშროებად) გადაწყვეტაზე გადასვლა**, წმინდა ტექნიკური კონცეპტუალური გაგების ტერმინი „**კომპიუტერული (საინფორმაციო, კიბერ-) უსაფრთხოება**“, რომელსაც სწორად იყენებდა და

იყენებს ამჟამადაც ინფორმაციული ტექნოლოგიების სამეცნიერო სფერო, უკვე სოციალური მეცნიერებების კონტექსტში ვეღარ ასახავს სრულად და ვერ გადმოსცემს მომხდარი ცვლილებების არსს და ვერ გამოხატავს მის შინაარსს.

შესაბამისად, ორი განსხვავებული პროცესის გადმოსაცემად ერთი და იმავე ტერმინის გამოყენება იწვევს გაუგებრობას. **რადგან უკვე კვლევის საგანი ხდება არა მხოლოდ ტექნიკური ხასიათის საქმიანობა, არამედ სოციალურ-პოლიტიკური პროცესები, როდესაც ქვეყნის ხელისუფლების - ეროვნული უშიშროების შესაბამისი სამსახურებისა და ინსტიტუტების მიერ მუშავდება კიბერუსაფრთხოებაზე თავდაცვითი რეაგირების სახელმწიფო პოლიტიკა, ყალიბდება ეროვნული ინტერესების დასაცავად კიბერუსაფრთხოების გაუზნებელყოფის ეროვნული უშიშროების სტრატეგია, რომელიც დამყარებულია კიბერსივრცისა (საინფორმაციო სივრცის) და კიბერუსაფრთხოების პრობლემების გადაჭრის სისტემურ გააზრებაზე, რეაგირებისათვის საინფორმაციო-საკომუნიკაციო ტექნოლოგიების სრულყოფილად გამოყენების შესაძლებლობების გაანალიზებაზე და სხვ.** ამდენად, საქმე გვაქვს პროცესთან, როდესაც ხელისუფლებამ უნდა დასახოს სოციალურ-პოლიტიკური ხასიათის ღონისძიებები: მოხდეს კანონების, სამართლებრივი აქტების შემუშავება და მიღება, მათ შორის - ეროვნული ინტერესების დაცვა, მართვის პროცესის სრულყოფა, სახელმწიფო უწყებებს შორის ფუნქცია-მოვალეობების გამიჯვნა, კოორდინაციის, ურთიერთთანამშრომლობისა და ინფორმაციის მიმოცვლის მექანიზმების დახვეწა, კრიტიკული ინფრასტრუქტურის ჩამონათვალის დადგენა და სხვ. ამ პროცესების თეორიული კვლევა სოცია-

ლური მეცნიერებების საგანია და შესაბამისი ტერმინის გამოყენებას თხოვლობს.

ამრიგად, ახალ რეალობაში გაჩნდა შესაბამისი ტერმინის გამოყენების აუცილებლობა, როდესაც გავრდილი საშიშროების თავიდან ასარიდებლად კომპიუტერების ტექნიკურად დაცვის პროცესში უკვე გადაწყვეტ როლს თამაშობს შინაარსობრივად განსხვავებული ფართო მასშტაბის სოციალურ-პოლიტიკური საქმიანობა, ხოლო კვლევებში სხვადასხვა სამეცნიერო სფეროს სპეციალისტები არიან ჩართული.

ამ რეალობას კი ზუსტად მიესადაგება ქართულ ენაში არსებული ძირძველი სოციალურ-პოლიტიკური ტერმინი „უშიშროება“, ვიდრე ტექნიკური, კონცეპტუალური გაგების ტერმინი „უსაფრთხოება“. ხაზგასმით უნდა აღინიშნოს, რომ V-XX საუკუნეების ქართულ საისტორიო წყაროებში, სასულიერო მწერლობასა და მხატვრულ ლიტერატურაში, ასევე ჩვენი სახელოვანი პოლიტიკური, სამხედრო და საზოგადო მოღვაწეთა ნაწერებში სოციო-პოლიტიკურ კონტექსტში გამოყენებულია მხოლოდ ტერმინი „უშიშროება“ (უშიშობა). ამ ტერმინს ხმარობდნენ ქართველთა სახელოვანი ჰაგიოგრაფები, მწერლები, მემატიანენი, მეცნიერები, პოლიტიკური, სამხედრო და საზოგადო მოღვაწენი ანუ მე-5 საუკუნიდან 21-ე საუკუნის 10-იან წლებამდე მთლიანად, ერი თუ ბერი - იაკობ ცურტაველი თუ ლეონტი მროველი, დავით აღმაშენებელი თუ შოთა რუსთაველი, სოლომონ დოდაშვილი თუ ილია ჭავჭავაძე, ნოე ჟორდანიას თუ ქაქუცა ჩოლოყაშვილი, ივანე ჯავახიშვილი თუ ამბროსი ხელაია, კონსტანტინე გამსახურდია თუ ოთარ ჭილაძე, არნოლდ ჩიქობავა თუ ლავრენტი

ბერია, ილია მეორე თუ ზვიად გამსახურდია, ედუარდ შევარდნაძე თუ მიხეილ სააკაშვილი თუ ჩვეულებრივი მოქალაქე, ამ ტერმინს იყენებდა მხოლოდ სოციალურ-პოლიტიკურ კონტექსტში. ეს ტერმინია გამოყენებული საქართველოს დემოკრატიული რესპუბლიკის 1921 წლის კონსტიტუციაში (მუხლი. 72) და 1995 წელს მიღებულ საქართველოს კონსტიტუციაში (მუხლები: 3, 22, 24-26, 41, 73, 78, 98, 99). ამ უკანასკნელში 2018 წელს ცვლილებების შეტანის შემდეგ ტერმინი „უშიშროება“ საკანონმდებლო დონეზეც სრულიად დაუსაბუთებლად გააქრეს [19, 92-121].

ამიტომ აუცილებელია აზრობრივი და შინაარსობრივი აღრევისა და მოსალოდნელი გაუგებრობების თავიდან ასაცილებლად სოციალურ-პოლიტიკური პროცესების აღმნიშვნელ ტერმინად დამკვიდრდეს „კიბერუშიშროება“ („საინფორმაციო უშიშროება“). ამავე დროს, კიბერუშიშროების უზრუნველყოფის პროცესი მოაზრებული უნდა იქნეს, როგორც ქვეყნის ეროვნული უშიშროების უზრუნველყოფის ერთიანი სისტემის უმნიშვნელოვანესი ქვესისტემა (სახე, კომპონენტი), ხოლო, რაც შეეხება „კიბერუსაფრთხოებას“ (კომპიუტერული, საინფორმაციო), იგი არის და დარჩება „კიბერუშიშროების“ შემადგენელ კომპონენტად.

ნათელია, რომ ინფორმატიკოსისაგან განსხვავებით, სოციალური მეცნიერების სფეროს მკვლევარმა კიბერსივრცეში ტერმინი „უშიშროება“ უნდა გამოიყენოს მაშინ, თუ მოსალოდნელი საფრთხის (საშიშროების) თავიდან არიდება (გაუვნებელყოფა) მოითხოვს სოციალურ-პოლიტიკურ საქმიანობას, სოციალურ-პოლიტიკური ხასიათის ღონისძიებათა დასახვასა და განხორციელებას (პოლიტიკის შემუ-

შავება, კონცეფცია, დაგეგმვა და სხვ.), ანუ დაკავშირებულია ადამიანის, საზოგადოებისა და სახელმწიფოს სოციალურ-პოლიტიკურ საქმიანობასთან [16].

კიბერსივრცის სხვადასხვა სამეცნიერო სფეროს დისციპლინების კვლევებში, შიფრი უნდა იყოს გამოყენებული შემდეგნაირად:

1. ტერმინი „უსაფრთხოება“ ტრადიციულად უნდა გამოვიყენოთ:

ა) **უნივერსალური ათობითი კოდის იერარქიის მიხედვით:** 004 - ინფორმაციული ტექნოლოგიები. კომპიუტერული ტექნოლოგიები. გამოთვლითი მანქანებისა და სისტემების თეორია.

ბ) **SCOPUS-ის სამეცნიერო ჟურნალების კლასიფიკატორის მიხედვით:** 1700-1708 - კომპიუტერული მეცნიერება (ყველა).

გ) **სწავლის სფეროების კლასიფიკატორის მიხედვით** (საქართველოს განათლების, მეცნიერების, კულტურისა და სპორტის მინისტრის ბრძანება №69/ნ, 10.04.2019): 06 (061: 0611-0613, 0619) - ინფორმაციისა და კომუნიკაციის ტექნოლოგიები.

2. ტერმინი „უშიშროება“ უნდა გამოვიყენოთ:

ა) **უნივერსალური ათობითი კოდის იერარქიის მიხედვით:** 3 - სოციალური მეცნიერებები. სტატისტიკა. პოლიტიკა. ეკონომიკა. ვაჭრობა. სამართალი. მთავრობა. სამხედრო საქმე. დაზღვევა. განათლება. ფოლკლორი; 314/316 - საზოგადოება; 314 - დემოგრაფია. მოსახლეობის სტატისტიკური კვლევა; 316 - სოციოლოგია; 32 - პოლიტიკა; 323 - საშინაო პოლიტიკა; 323.1 - ეროვნული, სახალხო, ეთნიკური მოძრაობები და პრობლემები. ეროვნული და ეთნიკური უმცირესობები; 323.2 - ურთიერთობა სახელმ-

წიფოსა და პიროვნებას შორის. შიდაპოლიტიკური აქტივობები; 327 - საერთაშორისო ურთიერთობანი. გლობალური მსოფლიო პოლიტიკა. საგარეო პოლიტიკა; 33 - ეკონომიკა. ეკონომიკური მეცნიერებანი; 34 - სამართალი. იურიდიული მეცნიერებანი; 341 - საერთაშორისო სამართალი; 341.3 - ომის სამართალი. ომის დროს არსებული საერთაშორისო სამართლებრივი ურთიერთობები; 342.1 - სახელმწიფო. ხალხი. ეროვნება. სახელმწიფოს ძალაუფლება; 342.6 - აღმასრულებელი ხელისუფლება. სახელმწიფო მმართველობის ცენტრალური ორგანოები; 342.7 - ძირითადი უფლებები. ადამიანის უფლებები. მოქალაქეთა უფლება-მოვალეობანი; 35 - სახელმწიფო ადმინისტრაციული მმართველობა. მთავრობა. სამხედრო საქმე; 355/359 - სამხედრო საქმე. სამხედრო ხელოვნება. სამხედრო მეცნიერება. თავდაცვა. შეიარაღებული ძალები; 009 - ჰუმანიტარული მეცნიერებანი მთლიანობაში.

ბ) **SCOPUS-ის სამეცნიერო ჟურნალების კლასიფიკატორის მიხედვით:** 2000 - ეკონომიკა, ეკონომეტრიკა და ფინანსები (ყველა); 3300 - საზოგადოებრივი მეცნიერებები (ყველა) და სხვ.;

გ) **სწავლის სფეროების კლასიფიკატორის მიხედვით** (საქართველოს განათლების, მეცნიერების, კულტურისა და სპორტის მინისტრის ბრძანება №69/ნ, 10.04.2019):

03 - სოციალური მეცნიერებები, ჟურნალისტიკა და ინფორმაცია; 031 - სოციალური და ქცევითი მეცნიერებები; 0311 - ეკონომიკა; 0312 - პოლიტიკის მეცნიერებები და მოქალაქეობრიობის საფუძვლები (0312.1.1 - პოლიტიკის მეცნიერება, 0312.1.2 -საერ-

თაშორისო ურთიერთობები); 0413.1.3 - საქარო მმართველობა; 0421 - სამართალი და სხვ.

სასურველია საქართველოს განათლებისა და მეცნიერების სამინისტრომ გაითვალისწინოს აღნიშნული გარემოება და შესაბამისი ცვლილებები შეიტანოს ეროვნული კვალიფიკაციების ჩარჩოსა და სწავლის სფეროების კლასიფიკატორში.

დასკვნა

წამოვიყენე პირველი სამეცნიერო კვლევა საქართველოში, რომელშიც ხორციელდება ინფორმაციულ ეპოქაში არაპროგნოზირებადი და მზარდი კიბერსაშიშროების პირობებში სამეცნიერო კვლევების სფეროსა და არეალის გაფართოება-განვრცობადობის მიმდინარე პროცესის თეორიული ანალიზი.

შემუშავებულია და დასაბუთებულია ავტორის ჰიპოთეზა, რომ დღეს კიბერსივრციდან მომდინარე გლობალური საშიშროების პრობლემის გადასაჭრელად აუცილებელია საქართველოში პოლიტიკოსების, სამხედროებისა და მეცნიერების სხვადასხვა დარგის მკვლევრების საერთო ძალისხმევა, მათ საქმიანობაში სინქრონიზმის მიღწევა და სრულყოფა.

ახალ ვითარებაში გამოიკვეთა საქართველოს სამეცნიერო სფეროს მკვლევართა მიერ კიბერსივრცეში ტერმინების გამოყენების საკითხის დაზუსტების საჭიროება: 1. კომპიუტერული ვირუსების საფრთხეებისაგან კომპიუტერის (ქსელების) ტექნიკურად დაცვის უზრუნველსაყოფად კვლავ ტრადიციულად გამოყენებული უნდა იქნეს ტექნიკური გაგების ტერმინი „უსაფრთხოება“ (კიბერუსაფრთხოება, საინფორმაციო უსაფრთხოება, კომპიუტერული უსაფრთხოება); 2. ბოლო ათწლეულებში კიბერსაფრთხეების, როგორც ტექნიკური პრობლემის განხილვიდან მის პოლიტიკურ ამოცანად გადაწყვეტაზე გადასვლის შემდეგ, კიბერსივრცეში გაზრდილი საშიშროების თავიდან ასარიდებლად შინა-არსობრივად ახალი სოციალურ-პოლიტიკური საქმიანობის გამოსახატად გამოყენებული უნდა იქნეს ძირძველი ქართული სოციალურ-პოლიტიკური გაგების ტერმინი „უშიშროება“, ანუ სამეცნიერო კვლევებში გამოყენებული უნდა იქნეს სოციალური, ჰუმანიტარული მეცნიერებების თემატიკის შესაბამის კონტექსტში - ტერმინები „კიბერუშიშროება“, „საინფორმაციო უშიშროება“.

ლიტერატურა

1. Dunn-Cavelty, M., Eriksen, Ch., Scharte, B. (2023). Making cyber security more resilient: adding social considerations to technological fixes. *Journal of Risk Research*, 26 (7), 801-814.;
2. Dewar, R. (2022). *Cyberspace is a Consensual Hallucination*. Retrieved from: https://www.researchgate.net/publication/325216608_Cyberspace_is_a_Consensual_Hallucination;
3. Egloff, F.J. (2019). Contested Public Attributions of Cyber Incidents and the Role of Academia. *Contemporary Security Policy*, 41(1), 55–81;
4. Eggenschwiler, J. (2022). *Big Tech's Push for Norms to Tackle Uncertainty in Cyberspace*.;
5. Wilson, T. L., & Hershey, D. A. (1996). The research methods script. *Teaching of Psychology*, 23(2), 97-99.;
6. Dunn-Cavelty, M., & Wenger, A. (Eds). (2022). *Cyber security politics: socio-technological transformations and political fragmentation*. New York,; Routledge.;

7. Dunn-Cavelty, M., Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41.;
8. Jiadze, N. (2023). *Georgia's cyber security policy and international challenges*. [Doctoral dissertation, Georgian Technical University].
9. Kuprashvili, H. (2022). Cyberspace and Terms: “kiberushishroeba” (Cyber Security) and “kiberusaprtkhoeba” (Computer Security). *Works of GTU*, 2(524), 167-177.;
10. Abuladze, I. (1973). *Dictionary of the old Georgian language*. Tbilisi: “Metsniereba”.;
11. Sarjveladze, Z. (1995). *Dictionary of the old Georgian language*. Georgia, Tbilisi: Tbilisi State University.;
12. Chubinashvili, N. (1961). *Georgian dictionary with Russian translation*. Tbilisi: Soviet Georgia.;
13. Chubinashvili, D. (1984). *Georgian-Russian dictionary*. Tbilisi: Soviet Georgia.;
14. *Russian-Georgian Technical Dictionary. Compiled by the Terminology Section of the Technical Society of Georgia, with the addition of Gymnastics Terminology*. (1920).
15. *Georgian-English Dictionary*. (1950).
16. *Georgian-Russian and Russian-Georgian technical dictionary. Compiled by the Terminology Section of the Technical Society of Georgia. corrected and supplemented*. (1921).
17. *Russian-Georgian Road technical dictionary*. (1925).
18. Kuprashvili, H. (2022). *The National Security of Georgia*. Tbilisi: Universali. (In Georgian);
19. Kuprashvili, H. (2014). *Terms „ushishroeba“ (Security) or „usaprtkhoeba“ (Safety)?!* Tbilisi: Universali. (In Georgian).

UDC 004; 3; 351.746

SCOPUS CODE 1700; 3300; 3320

<https://doi.org/10.36073/1512-0996-2024-1-108-120>

Expanding the Scope and Area of Academic Scientific Research in the Information Age

Henri Kuprashvili Department of Politics and International Relations, Georgian Technical University, Georgia, 0160, Tbilisi, 77, M. Kostava str.
E-mail: kuprashvilihenri07@gtu.ge

Reviewers:

- O. Shonia**, Doctor of Technical Sciences, Professor, Faculty of Informatics and Control Systems, GTU
E-mail: o.shonia@gtu.ge
- D. Khupenia**, DIR, Assistant Professor, Faculty of Law and International Relations, GTU
E-mail: khupenia.d@gtu.ge

Abstract. The topic refers to the analysis of the current process of expanding the scope and area of scientific research. Internet technologies have changed the political, economic and social reality. Today, security mechanisms became a combined target. The data indicate that the challenges related to unpredictable dangers led to the need to make serious socio-political decisions at all levels, including the need to implement political, legal, economic,

military-defense and social measures, to develop new normative regulation systems. Accordingly, cyberspace problems emphasized the role of researchers in various fields of science and expanded the scope and area of academic scientific research. It has become urgent to increase the involvement of Georgian researchers in the ongoing scientific-research processes in this direction.

At the same time, there was a need to clarify the use of terms by Georgian researchers in the study of cyberspace problems in the socio-political context. In particular, after the transformation of cyber security as a technical problem into its socio-political task, into cyber security, i.e. when the content of activities changes in order to avoid increased dangers, it is necessary to use the terms in the context of the field of social sciences, as the changes refer not only to activities related to security techniques, but also to human, socio-political activities of society and the state, planning and implementing socio-political events (policy development, concept, planning, etc.). Separation of this problem for research suits the needs of the current situation in social sciences. Accordingly, a specific contribution has been made to the research of strategic assessments of possible trends.

Keywords: cyberspace; cyber safety; cyber security; scientific knowledge system; scientific research; standard classification of education; term.

განხილვის თარიღი 15.11.2023

შემოსვლის თარიღი 28.11.2023

ხელმოწერილია დასაბეჭდად 22.03..2024