UDC 321
SCOPUS CODE 3320
https://doi.org/10.36073/1512-0996-2022-2-167-177

კიბერსივრცე და ტერმინები: კიბერუშიშროება და კიბერუსაფრთხოება

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

რეცენზენტები:

ე. გვენეტაძე, სტუ-ის სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტის პროფესორი
E-mail: e.gvenetadze@mail.ru

ს. მიდელაშვილი, სტუ-ის სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტის ასოცირებული პროფესორი
E-mail: Sophiomidelashvili@gmail.com

ანოტაცია. ხშირად ტერმინებს „კიბერუსაფრთხოება“ და „კიბერუშიშროება“ იყენებენ შეუსაბამო კონტექსტში. ტერმინი „კიბერუშიშროება“ გამოიყენება, როდესაც მოსალოდნელი საფრთხის თავიდან არიდება მოითხოვს სოციალურ-პოლიტიკურ ღონისძიებათა დასახვასა და განხორციელებას (დოქტრინის, კანონების, სამართლებრივი აქტების შემუშავება და მიღება, კიბერუშიშროების და კიბერუსაფრთხოების უზრუნველყოფის მართვის პროცესის სრულყოფა), რადგან კიბერსივრცეში ეროვნული ინტერესების დაცულობის მდგომარეობა მიიღწევა კვალიფიციური კიბერპოლიტიკის შედეგად ეფექტური კიბერუსაფრთხოების სისტემის ჩამოყალიბებით, კიბერსივრცის მდგრადობით, არასასურველი შიგა და გარე ზემოქმედებისაგან დაცულობით. კიბერუშიშროების უზრუნველყოფაში ამოსავალი პოლიტიკური მიზანია, ხოლო შედეგი – მათი მიღწევა. კიბერუსაფრთხოება კი არის კიბერუშიშროების შემადგენელი კომპონენტი, განსხვავებული შინაარსისა და დატვირთვის მატარებელი. კიბერუსაფრთხოება არის კომპიუტერული და საინფორმაციო-სატელეკომუნიკაციო სფეროში შემავალი კომპონენტების (ქსელები, კომპიუტერები, პროგრამები, მონაცემები, მოწყობილობები) კიბერშეტევებისგან ტექნიკურად დაცვის ტექნოლოგიების, მეთოდიკისა და პროცესების ერთობლიობა. იგი უფრო „ტექნიკური“ საფრთხისგან დაცვასთან (მიღებულ იქნეს ორგანიზაციულ-ტექნიკური ზომები: განისაზღვროს კომპიუტერულ-საინფორმაციო-სატელეკომუნიკაციო სფეროს ექსპ-

ლუატაციის უსაფრთხოებაზე პასუხისმგებელი პირები და დაინერგოს შესაბამისი ტექნიკური ინფრასტრუქტურა და უსაფრთხოების სისტემა) ანუ მეტად „შრომის უსაფრთხოების დაცვასთან“ ასოცირდება ვიდრე სოციალურ-პოლიტიკური მიზნების დასახვა-განხორციელებასთან. კიბერუსაფრთხოების მიზანია მათი დაცვა, თვითონ მთლიანობაში ამ დაცულობის მიღწევა კი არის კიბერუშიშროების პოლიტიკური მიზნის მოთხოვნების შესაბამისი შედეგის მიღწევის უზრუნველყოფა.

საკვანძო სიტყვები: ეროვნული უშიშროება; ინფორმაციული ეპოქა; ინფორმაციული ტექნოლოგიები; კიბერსივრცე; კიბერუსაფრთხოება; კიბერუშიშროება; პოლიტიკა.

შესავალი

თანამედროვე მსოფლიოში ინფორმაციული ტექნოლოგიების სწრაფმა განვითარებამ დიდი გავლენა მოახდინა განსაკუთრებული სოციალურ-პოლიტიკური სივრცის განზომილების ჩამოყალიბებაზე, რომელიც სულ უფრო მნიშვნელოვან როლს ასრულებს საშინაო და საგარეო პოლიტიკაში. ეს ახალი განზომილებაა ვირტუალური კიბერსივრცე (Cyberspace), რომელიც წარმოადგენს სოციალური ურთიერთქმედების გამორჩეულ სფეროს, განსაზღვრულია პროცესების ერთობლიობით, არსებობს მსოფლიოს კომპიუტერულ ქსელებში და გადაიქცა ადამიანის საქმიანობისა და არსებობის კიდევ ერთ განუყოფელ გარემოდ. დღეისათვის არ არსებობს მისი შეთანხმებული ოფიციალური განმარტება. მაგალითად, ოქსფორდის სასწავლო ლექსიკონის მიხედვით, იგი განიხილება როგორც წარმოსახვითი სივრცე ფიზიკური ადგილმდებარეობის გარეშე, რომელშიც ურთიერთობენ კომპიუტერული ქსელების მეშვეობით [1]. იგივე ოქსფორდის ინგლისური ენის ლექსიკონი განსხვავებულ განმარტებას იძლევა: კიბერსივრცე არის საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის ურთიერთკავშირის კომპლექსი, რომელიც მოიცავს ინტერნეტის გლობალურ ქსელს, კომპიუტერულ სისტემებს, ტელესაკომუნიკაციო ქსელებსა და პროცესორებს [2]. კემბრიჯის ლექსიკონი გვამცნობს, რომ ეს არის „ელექტრონული სისტემა, რომელიც შესაძლებლობას აძლევს კომპიუტერის მომხმარებლებს მთელ მსოფლიოში იურთიერთონ ერთმანეთთან და ნებისმიერი მიზნისთვის მიიღონ წვდომა ინფორმაციასთან“ [3]. აშშ-ის მთავრობის ოფიციალური საიტის, „კომპიუტერული უსაფრთხოების რესურსების ცენტრის“ (COMPUTER SECURITY RESOURCE CENTER – CSRC) ლექსიკონის [4] მიხედვით, კიბერსივრცე არის გლობალური ზონა საინფორმაციო გარემოში, რომელიც შედგება საინფორმაციო სისტემის ინფრასტრუქტურების ურთიერთდამოკიდებული ქსელისგან, მათ შორის ინტერნეტის, ტელეკომუნიკაციის ქსელების, კომპიუტერული სისტემებისა და ჩაშენებული პროცესორებისა და კონტროლერების ჩათვლით. კიბერსივრცის 30-ზე მეტი განმარტება შეიძლება მოიძებნოს როგორც სამეცნიერო ლიტერატურაში, ისე ოფიციალურ სამთავრობო წყაროებში, აზრიც არ აქვს ყველას ჩამოთვლას. ამიტომ ყველასათვის გასაგებად, შეიძლება უფრო მარტივად ითქვას – კიბერსივრცე არის პირობითი გარემო, რომელშიც კომუნიკაცია ხდება კომპიუტერული ქსელების მეშვეობით.

ძირითადი ნაწილი

ახალმა რეალობამ გააჩინა ახალი საფრთხეები და შექმნა უშიშროების უზრუნველყოფის თანამდევი პრობლემებიც. ახლად მოვლენილი კიბერუშიშროების პრობლემის აქტუალურობა განპირობებულია საინფორმაციო-საკომუნიკაციო და კიბერტექნოლოგიების წარმოუდგენლად არნახული განვითარების ფონზე კიბერთავდასხმების განუსაზღვრელი მასშტაბების შეუქცევადი პროცესებით, რომელიც მთელი მსოფლიოს წინაშე აყენებს უშიშროების უზრუნველყოფის ზომების გაძლიერების აუცილებლობას [5]. მე-20 საუკუნის მეორე ნახევარიდან დაწყებული სამხედრო კონფლიქტების კლასიკურ სახეებს თანდათან ენაცვლება სახელმწიფოთა დაპირისპირების ახალი ფორმები, მათ შორის, განსაკუთრებით გამოირჩა კიბერომი, რომლის საომარი მოქმედებისა და დაპირისპირების არეალია კიბერსივრცე. ომის ამ სახემ, 21-ე საუკუნეში ტექნოლოგიური უპირატესობის მოპოვების მცდელობები სულ უფრო სასტიკი გახადა, სადაც უკვე საერთოდ არ არსებობს საზღვრები და აკრძალვები. სახელმწიფოები ცდილობენ მოიპოვონ კონკურენტული უპირატესობა ციფრულ სამყაროში. წარმოშობისთანავე კიბერსივრცე გადაიქცა სხვადასხვა პოლიტიკური და სამხედრო ძალების ბრძოლის მეხუთე (ხმელეთის, ზღვის, ჰაერისა და კოსმოსის შემდეგ) ველად. მრავლისმეტყველია ის ფაქტი, რომ ჩრდილოატლანტიკური ალიანსის წევრი ქვეყნების თავდაცვის მინისტრების ბრიუსელის შეხვედრაზე გაკეთებულ განცხადებაში აღინიშნა, რომ კიბერსივრცე ნატოს გავლენის კიდევ ერთი სფერო ხდება, თანაბრად ზღვასთან, ჰაერთან და ხმელეთთან, შესაბამისად, საჭირო ხდება კოლექტიური თავდაცვის შესახებ ხელშეკრულების გამოყენებაც [6]. ხოლო, 2016 წლის 8 ივლისს, ნატოს სამიტმა ვარშავაში, კიბერსივრცე ოფიციალურად აღიარა თავდაცვის თანაბარუფლებიან სფეროდ. ნატოს გენერალურმა მდივანმა **იენს სტოლტენბერგმა** (Jens Stoltenberg) აღნიშნა: თანამედროვე გამოწვევები ითხოვს ვაღიაროთ, რომ კიბერშეტევები და მათგან დაცვა ისეთივე მნიშვნელოვანია, როგორც თავდაცვა ხმელეთზე, ზღვასა და ჰაერში [7].

როგორც აღინიშნა, კიბერსივრცე არ არსებობს რაიმე ფიზიკური ფორმით, იგი ურთულესი გარემოა, რომელიც წარმოიქმნება ადამიანებს, პროგრამულ უზრუნველყოფას, ინტერნეტმომსახურებას, ტექნოლოგიური მოწყობილობების, ქსელებსა და ქსელური კავშირების საშუალებებს შორის ურთიერთქმედების შედეგად.

სახელმწიფო საზღვრების არმქონე ეს ვირტუალური სივრცე გვევლინება პოლიტიკური, ეკონომიკური, ინფორმაციული და კულტურული კონკურენციის მნიშვნელოვან ასპარეზად. არსებითად, საინფორმაციო-სატელეკომუნიკაციო ტექნოლოგიების არნახული განვითარების ფონზე კონკურენციის ეს ველი წარმოადგენს ახალი (ვირტუალური) ტიპის პოლიტიკურ სივრცეს, რომელშიც ეჯახება სხვადასხვა პოლიტიკური სუბიექტის, სახელმწიფოებისა და პოლიტიკური ძალის ცენტრების ინტერესები. ინფორმაციული სივრცე პოლიტიკოსებისთვის, ფაქტობრივად, სამხედრო მოქმედებათა თეატრად იქცა, სადაც თითოეული მოწინააღმდეგე მხარე უპირატესობის მიღწევას ცდილობს. ინფორმაციული ტექნოლოგიების განვითარების დონე ინფორმაციულ ომში ქმნის უპრეცედენტო შესაძლებლობებს, მოწინააღმდეგის დასამარცხებლად, ტრადიციული ძალადობრივი შემმუსვრელი საშუალებების გამოყენების გარეშე.

კიბერომში ინფორმაციულ იარაღს ახასიათებს დანახარჯების მინიმალური დონე და გამოყენების მაღალი ეფექტურობა. იგი არ ანადგურებს მოწინააღმდეგის ცოცხალ ძალას, არ მოითხოვს რთული სტრუქტურების შექმნას და, ამასთანავე, არ არის აუცილებელი გადაიკვეთოს ოფიციალური სახელმწიფო საზღვარი. ინფორმაციულმა ერამ განსაკუთრებით გააქტიურა საბრძოლო მოქმედებათა ჩატარების წესი ორი მიმართულებით, შესაძლებელი გახდა:

- მოწინააღმდეგის ინფორმაციის პირდაპირი მანიპულირება, ინფორმაცია იქცა პოტენციურ იარაღად და სასარგებლო სამიზნედ;
- ინფორმაციული ტექნოლოგიების, როგორც საშუალებების გამოყენება საბრძოლო ოპერაციების წარმატებით ჩასატარებლად.

მტრულად განწყობილი სახელმწიფოების მიერ ინიცირებული კიბერთავდასხმა ხორციელდება როგორც სამთავრობო ქსელებზე, ისე ელექტრომომარაგების, სატრანსპორტო ან ფიჭური სატელეფონო კომპანიების კომპიუტერულ სისტემებზე, ფინანსურ ინსტიტუტებზე, ინდუსტრიული მართვის სისტემებზე თუნდაც იმ მიზნით, რომ წარმოქმნან ქაოსი, მოა-

ხდინონ მოსახლეობის დემორალიზაცია, ან თუნდაც კინეტიკური შეტევისთვის მოამზადონ ბრძოლის ველი, ან კიდევ კინეტიკური შეტევის პარალელურად კიბერთავდასხმები განახორციელონ.

დღეს, კიბერსივრცეში მიმდინარე კიბერომები სხვადასხვა ქვეყნის სადაზვერვო ორგანიზაციებს, მათ სამხედრო სტრუქტურებს შორის, აგრეთვე ეკონომიკური და ინფორმაციული ბრძოლები, ეკონომიკური შპიონაჟისა და ფინანსური დივერსიების ჩათვლით, განსაზღვრავს კიბერსივრცეში მიმდინარე პროცესების დიდ მნიშვნელობას თანამედროვე პოლიტიკური ანალიზისათვის, საერთაშორისო ურთიერთობების, პოლიტიკის მეცნიერებების თეორიისა და პრაქტიკისათვის.

განვითარების თანამედროვე რეალიებში მნიშვნელოვანი ასპექტი ხდება სუვერენიტეტის უზრუნველყოფა. ესაა მბრძანებლობისა და დაქვემდებარების ურთიერთობის სისტემის განვრცობა იმ სოციალურ სივრცეში, რომელსაც არ ახასიათებს ტერიტორიულობის ნიშანი. საუბარია კიბერსივრცესა და ქსელურ სივრცეებზე, როგორც სოციალური ურთიერთზემოქმედების სპეციფიკური ფორმის შესახებ. იძებნება ამ სფეროში სახელმწიფო სუვერენიტეტის ეფექტურად გავრცელების შესაბამისი გზები. საკანონმდებლო, აღმასრულებელი და სასამართლო ხელისუფლება, როდესაც იღებენ აქტებს, რომლებიც ეხება კიბერსივრცესა და ქსელურ სივრცეებში ურთიერთობებს, ფაქტობრივად ამ სფეროზე სახელმწიფო ხელისუფლების პროეცირებას ახდენენ. სამეცნიერო სივრცეში გაჩნდა სხვადასხვა ტერმინიც, მაგალითად, „ვირტუალური სუვერენიტეტი“, „ქსელური სუვერენიტეტი“ და სხვ.

სახელმწიფო ხელისუფლების გავლენა ვირტუალურ გაერთიანებაზე შეზღუდულია. მიუხედავად მთლიანობაში სახელისუფლებო უფლებამოსილებების ერთობლიობისა, დღეისათვის სახელმწიფო კიბერსივრცეში წარმოდგენილია, როგორც ვირტუალური აქტორი, რომელსაც აქვს უფრო მეტად განვითარებული ინფორმაციული რესურსები და შესაძლებლობა შეზღუდოს სხვა აქტორების დაშვება კიბერსივრცეში (მთლიანად ან მის ცალკეულ სექტორში). სახელმწიფოს სუვერენიტეტის გავრცელებას ვირტუალურ გაერთიანებაზე აძნელებს ქსელური პრინციპით ორგანიზებული კიბერსივრცე. ვირტუალურ გაერთიანებაზე სუვერენიტეტის შეზღუდვაში განსაკუთრებულ როლს ასრულებს კიბერსივრცის პარამეტრები (ეფემერულობა, ინტერაქტიურობა, პარამეტრების პირობითობა, აქტორების ანონიმურობა, ვირტუალური იდენტურობის ფორმირება და სხვ.).

21-ე საუკუნის დასაწყისიდანვე საქართველო ჩაბმულია კიბერსივრცის ჩამოყალიბების პროცესში, რაც ბუნებრივად გულისხმობს სათანადო კიბერპოლიტიკის (კონცეფციის) შემუშავებას, კიბერსივრცის დაცვისა და გამოყენების უზრუნველყოფის საიმედო სისტემის შექმნას, კიბერსივრცეში ქვეყნის ეროვნული ინტერესების ეფექტურ დაცვას, ასევე, სახელმწიფო საინფორმაციო რესურსების, ქვეყნის საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურის, სატელეკომუნიკაციო და საკომუნიკაციო სისტემებისა და ობიექტების უსაფრთხოების გარანტიებს, რამაც საბოლოოდ უნდა უზრუნველყოს საქართველოს კიბერუშიშროება და მთლიანობაში ინფორმაციული უშიშროება. ამ თვალსაზრისით მისასალმებელია ის ფაქტი, რომ საქართველოს მთავრობის მიერ მიღებულ იქნა საკმაოდ სოლიდური და საჭირო დადგენილება „საქართველოს კიბერუსაფრთხოების 2021 –

2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ“. დოკუმენტში გათვალისწინებულია ოქსფორდის უნივერსიტეტის კიბერუშიშროების გლობალური ცენტრის (The Global Cyber Security Capacity Centre) მიერ მომზადებული შეფასების დოკუმენტი, რომელშიაც საუბარია საქართველოში არსებული კიბერუშიშროების გარემოზე და ასახულია კონკრეტული რეკომენდაციები და ინიციატივები მისი განვითარების მიზნით. სტრატეგიაში გაერთიანებულია როგორც კიბერ- და ინფორმაციული უშიშროების გარემოს გაუმჯობესების, ისე კიბერდანაშაულთან ბრძოლისა და კიბერთავდაცვითი შესაძლებლობების გაძლიერებისკენ მიმართული კონკრეტული კომპონენტები. სტრატეგია მიზნად ისახავს კიბერუშიშროების, კიბერთავდაცვისა და კიბერდანაშაულის სფეროებში კიბერკულტურისა და კიბერგანათლების განვითარებას, მმართველობითი სისტემის მდგრადობის უზრუნველყოფას, საჯარო-კერძო თანამშრომლობის გაძლიერებას, ძლიერი ადამიანური რესურსების შექმნასა და საერთაშორისო ასპარეზზე საქართველოს, როგორც უსაფრთხო და დაცული ქვეყნის როლის გაძლიერებას.

შინაარსობრივად კვალიფიციურად შედგენილ ამ საჭირო დოკუმენტში, სამწუხაროდ, ტერმინის აღრევასთან გვაქვს საქმე. სათაურში ნაცვლად „კიბერუშიშროებისა“ გამოყენებულია ტერმინი „კიბერუსაფრთხოება“. მთლიანად დოკუმენტშიც ტერმინი „კიბერუშიშროება“ საერთოდ არ გვხვდება, რაც შეეხება ტერმინს „კიბერუსაფრთხოება“, ზოგ ადგილას შინაარსობრივად სწორად არის ნახმარი, ზოგან – არა). სათაურში (და დოკუმენტის შესაბამის ადგილებში) უნდა იყოს გამოყენებული ტერმინი **კიბერუშიშროება, რადგანაც 15-საუკუნოვანი ქართული ტრადიციიდან გამომდინარე, ტერმინი „უშიშროება“ გამოიყენება იმ შემთხვევაში, თუ მოსალოდნელი საფრთხის (საშიშროების) თავიდან არიდება (გაუვნებელყოფა) მოითხოვს სოციალურ-პოლიტიკურ საქმიანობას, სოციალურ-პოლიტიკური ხასიათის ღონისძიებათა დასახვასა და განხორციელებას** (პოლიტიკის შემუშავება, კონცეფცია, დაგეგმვა და სხვ.) ანუ დაკავშირებულია **ადამიანის, საზოგადოებისა და სახელმწიფოს სოციალურ-პოლიტიკურ საქმიანობასთან.**

ამ დროს, განსხვავებული შინაარსისა და დატვირთვის მატარებელია ტერმინი „კიბერუსაფრთხოება“. ცნობილია, რომ **კიბერუსაფრთხოება** არის **კომპიუტერული და საინფორმაციო-სატელეკომუნიკაციო სფეროში შემავალი კომპონენტების** (ქსელები, კომპიუტერები, პროგრამები, მონაცემები, მოწყობილობები) **კიბერშეტევებისგან** (ციფრული თავდასხმები, დაზიანება, არაავტორიზებული წვდომა და სხვ.) **დაცვის ტექნოლოგიების, მეთოდიკისა და პროცესების ერთობლიობა**. ე.ი. მისი მიზანია მათი დაცვა, ხოლო თვითონ მთლიანობაში ამ დაცულობის მიღწევა კი არის **კიბერუშიშროების პოლიტიკური მიზნის** მოთხოვნების შესაბამისი შედეგის მიღწევის უზრუნველყოფა. ნათელია, რომ კიბერუსაფრთხოების უზრუნველყოფა უფრო „ტექნიკის“ საქმეა, უფრო „ტექნიკური“ საფრთხისგან დაცვაა. მაგალითად, იგი უფრო ცნობილი „შრომის უსაფრთხოების დაცვასთან“ ასოცირდება და არა სოციალურ-პოლიტიკური მიზნების დასახვასთან. ე. ი. მოცემულ ობიექტზე კიბერუსაფრთხოების უზრუნველსაყოფად მიღებული უნდა იქნეს შესაბამისი ორგანიზაციულ-ტექნიკური ზომები: განისაზღვროს **კომპიუტერული და საინფორმაციო-სატელეკომუნიკაციო სფე-**

როს (ქსელები, კომპიუტერები, მოწყობილობები, პროგრამები, მონაცემთა ბაზები) **ექსპლუატაციის უსაფრთხოებაზე პასუხისმგებელი პირი და დაინერგოს შესაბამისი ტექნიკური ინფრასტრუქტურა და უსაფრთხოების სისტემა**.[1]

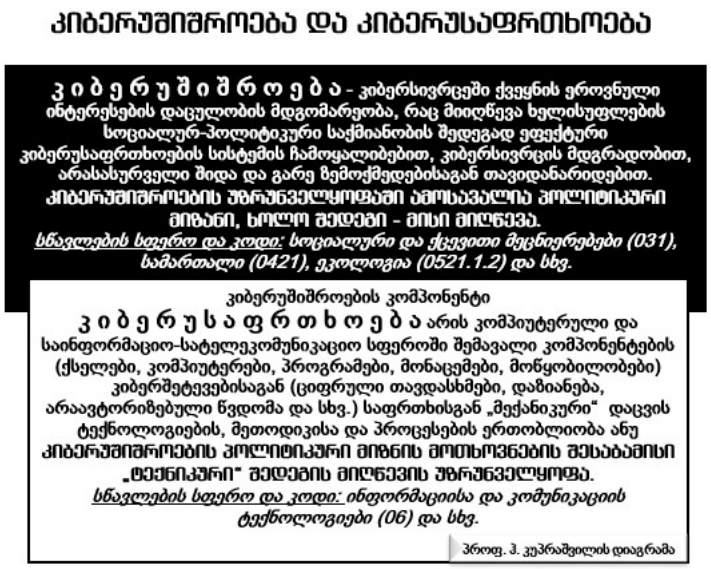
სულ სხვა შინაარსს მოიცავს საქმიანობა, როდესაც კიბერუსაფრთხოების ტექნიკური უზრუნველყოფის მისაღწევად ხელისუფლებამ უნდა შეიმუშაოს სოციალურ-პოლიტიკური ხასიათის ღონისძიებები (კანონების, სამართლებრივი აქტების შემუშავება და მიღება, მათ შორის, ეროვნული ინტერესების დაცვა, მართვის პროცესის სრულყოფა, სახელმწიფო უწყებებს შორის ფუნქცია-მოვალეობების გამიჯვნა, კოორდინაციის, ურთიერთთანამშრომლობისა და ინფორმაციის მიმოცვლის მექანიზმების დახვეწა, კრიტიკული ინფრასტრუქტურის ჩამონათვალის დადგენა და სხვ.). ეს საქმიანობა სრულიად განსხვავებული და ფართოა ვიდრე ტექნიკური ხასიათის ზომების გატარება. დოკუმენტის სათაურიდან ნათლად ჩანს და თვითონ მასშიც ხაზგასმით არის აღნიშნული, რომ „სტრატეგია, როგორც კიბერუსაფრთხოების სფეროში **სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი,** წარმოადგენს სტრატეგიული მიზნებისა და ამოცანების ერთობლიობას და მათ შესასრულებლად ითვალისწინებს კონკრეტულ აქტივობებს, რესურსებსა და პასუხისმგებელ უწყებებს“ [8] ანუ ეს არის პოლიტიკური დოკუმენტი, რომელშიაც განსაზღვრულია საქართველოს კიბერუშიშროების ეროვნული სტრატეგია, კიბერუშიშროების ეროვნული სტრატეგიის მიზნები და ამოცანები, განვითარების პრიორიტეტული ასპექტები, სტრატეგიის შემუშავებისა და განხორციელების პრინციპები და სხვ. ე.ი. თვითონ დოკუმენტის ეს ხაზგასმის შინაარსი მიუთითებს, რომ ამ დოკუმენტში ტერმინი „კიბერუსაფრთხოება“ არასათანადოდ არის გამოყენებული.

კიბერუშიშროება გულისხმობს კიბერსივრცეში ქვეყნის ეროვნული ინტერესების დაცულობის მდგომარეობას, რაც მიიღწევა კვალიფიციური კიბერპოლიტიკის შედეგად ეფექტური კიბერუსაფრთხოების სისტემის ჩამოყალიბებით, კიბერსივრცის მდგრადობით, არასასურველი შიგა და გარე ზემოქმედებისაგან დაცულობით.

კიბერუშიშროება ეროვნული უშიშროების (სისტემის) შემადგენელი მნიშვნელოვანი კომპონენტია (ქვესისტემაა), კიბერუსაფრთხოება კი კიბერუშიშროების შემადგენელი კომპონენტია (ანუ ქვესისტემის ქვესისტემაა).

კიბერუშიშროება, როგორც აღინიშნა, კიბერუსაფრთხოებასაც მოიცავს და ისინი ერთმანეთს შეეფარდება როგორც სისტემა და ქვესისტემა. **კიბერუშიშროების უზრუნველყოფაში ამოსავალი, პოლიტიკური მიზანია, ხოლო შედეგი – მათი მიღწევა.**

[1] სხვათა შორის, ასევე, მკაფიო განსხვავება არსებობს ინფორმაციულ უსაფრთხოებასა და კიბერუსაფრთხოებას შორის. ინფორმაციის უსაფრთხოება გულისხმობს ფიზიკური და ციფრული მონაცემების დაცვას არაავტორიზებული გამოყენების, წვდომისა და მოდიფიკაციისგან. კიბერუსაფრთხოება კი გულისხმობს ციფრული მონაცემების დაცვას არაავტორიზებული გამოყენების, წვდომისა და მოდიფიკაციისგან. სხვა სიტყვებით რომ ვთქვათ, ინფორმაციული უსაფრთხოება იცავს ფიზიკურ და ციფრულ მონაცემებს ნებისმიერი ტიპის უკანონო წვდომისგან, ხოლო კიბერუსაფრთხოება იცავს ციფრულ მონაცემებს უკანონო ციფრული წვდომისგან.



ამავე დროს, კიბერუშიშროება და კიბერუსაფრთხოება ერთმანეთსაც განაპირობებენ. კიბერუსაფრთხოება აუცილებელია, რადგან მისი განხორციელება აუცილებლია კიბერუშიშროების პოლიტიკის წარმატებისათვის. ამასთანავე, კიბერუშიშროების პოლიტიკის მიერ დასახული და განხორციელებული ამოცანების გარეშე, კიბერუსაფრთხოება ქვეყნის ეროვნული ინტერესების დაცვაში ვერ იქნება შესაბამისი როლის შემსრულებელი.

ცხადია, აქ გასათვალისწინებელია კონკრეტულად საქართველოში ტერმინ ,,უშიშროების“ გამოყენების ისტორიული და ენათმეცნიერების მიერ დადგენილი ტრადიციაც. რადგანაც მისი არასწორი ფორმულირება გარკვეული გაუგებრობის წყარო ხდება. მაგალითად, 2004-2006 წლებიდან ხელისუფლებაში აღზევებულმა მედროვე პოლიტიკოსების, არაკვალიფიციური და საქმეში ჩაუხედავი პირების მიკერძოებულმა და ვოლუნტარისტულმა ქმედებებმა სათავე დაუდო სავალალო ტენდენციას, რის შედეგადაც ძირძველი ქართული სიტყვა „უშიშროება" **თვითნებურად** გამოაცხადეს არასასურველ ტერმინად და ამოიღეს ხმარებიდან, ხოლო მის ნაცვლად დაიწყეს მასმედიაში დამკვიდრება სრულიად განსხვავებული შინაარსის მატარებელი სიტყვის „უსაფრთხოება“ ანუ ორი განსხვავებული შინაარსის მქონე მოვლენის აღსანიშნავად დაამკვიდრეს ერთი ტერმინი "უსაფრთხოება", ისევე, როგორც ეს არის რუსულ ენაში, რომელშიაც, მაგალითად, ინგლისური (Security, Safty) და ქართული (უშიშროება, უსაფრთხოება) ენებისაგან განსხვავებით აქვთ მხოლოდ ერთი ტერმინი „Безопасность“). მაგალითად, „ეროვნული უშიშროება“ შეცვალეს ტერმინით „ეროვნული უსაფრთხოება“ და შეუსაბამო კონტექსტი დაამკვიდრეს არა მარტო მასმედიაში, არამედ საკანონმდებლო დონეზეც კი მოახდინეს ცვლილებები.

არადა ქართველების მეტყველებასა და წერილობით სიტყვაკაზმულობაში კარგა ხანია ნათლადაა გარკვეული და განსაზღვრული ორივე ტერმინის შინაარსი, მნიშვნელობა და გამოყენების წესი. მაგალითად, ტერმინის „უშიშროება“ **სოციალურ-პოლი-**

ტიკურ კონტექსტში გამოყენების წესს ადასტურებს ჩვენამდე მოღწეული წერილობითი წყაროებით დადასტურებული თხუთმეტსაუკუნოვანი ისტორიული ტრადიცია. მე-20 საუკუნეში კი ეს კიდევ უფრო განამტკიცა ქართულმა ავტორიტეტულმა ენათმეცნიერებამ, როდესაც მეცნიერულადაც დაადგინა ამ ტერმინის გამოყენების შინაარსობრივი კონტექსტი და გამოყენების არეალი. ქართველები, როგორც ამას მე-5 საუკუნიდან დაწყებული წერილობითი წყაროები (საისტორიო, სასულიერო-ჰაგიოგრაფიული, მხატვრული ლიტერატურა და სხვ.) მოწმობს, ტერმინს „უშიშროება“ (უშიშოებაჲ) ტრადიციულად, როგორც აღინიშნა, იყენებდნენ მხოლოდ **სოციალურ-პოლიტიკურ კონტექსტში** (უშიშროება სახელმწიფოსი, ქვეყნის, საზოგადოების, ხელისუფლების, ადამიანის და სხვ.). ამ ტერმინს ხმარობდნენ ქართველთა სახელოვანი ჰაგიოგრაფები, მწერლები, მემატიანენი, მეცნიერები, პოლიტიკური, სამხედრო და საზოგადო მოღვაწენი. მოკლედ, 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 ჟორდანია** თუ **ქაქუცა ჩოლოყაშვილი, ივანე ჯავახიშვილი** თუ **ამბროსი ხელაია**, **კონსტანტინე გამსახურდია** თუ **ოთარ ჭილაძე**, **არნოლდ ჩიქობავა** თუ **ილია მეორე, ზვიად გამსახურდია** თუ **ედუარდ შევარდნაძე** თუ ჩვეულებრივი მოქალაქე, ამ ტერმინს იყენებდა მხოლოდ სოციალურ-პოლიტიკურ კონტექსტში. რაც შეეხება ტერმინ „უსაფრთხოებას“, იგი მე-20 საუკუნის 50-იან წლებამდე ქართულ წერილობით წყაროებში საერთოდ არც გვხვდება [9].

ამ ტერმინების ანალიზის დროს, ასევე არ იქნება ურიგო თუ გათვალისწინებული იქნება საფრთხეების წარმოშობის წყაროებიც, რომელთაც აქვთ ბუნებრივი, ტექნოგენური, საწარმოო და სოციალურ-პოლიტიკური ხასიათი:

1. **ბუნებრივი** ხასიათის საფრთხეებს (საშიშროებას) მიეკუთვნება, პირველ ყოვლისა, ბუნებრივი კატაკლიზმების (მიწისძვრები, ზვავები, მეწყრები, წყალდიდობები, გვალვები და სხვ.) შედეგებით მიყენებული ზიანის შესაძლებლობა;

2. **ტექნოგენური** ხასიათის საფრთხეები (საშიშროება) დაკავშირებულია ტექნიკური ობიექტების: ატომური და ჰიდროელექტროსადგურები, ქიმიური, ნავთობისა და გაზის საწარმოები და მრეწველობის სხვა დარგები – ფუნქციონირების პროცესში წარმოშობილ გარკვეულ საფრთხეებთან (საშიშროებასთან);

3. **საწარმოო** ხასიათის საფრთხეები (საშიშროება) არის საწარმოო გარემოსა და სამუშაო პროცესის (მანქანა-დანადგარები, მასალები, ნივთიერებები, სამუშაო მეთოდები, გარემო პირობები, ტექნიკური საშუალებები, შრომის ორგანიზება და სხვ.) ფიზიკური, ქიმიური, ბიოლოგიური ან ფიზიოლოგიური ფაქტორებით გამოწვეული, რომლებითაც საფრთხე (საშიშროება) ექმნება ადამიანს, საზოგადოებას;

4. **სოციალურ-პოლიტიკური** ხასიათის საფრთხეები (საშიშროება) უშუალოდ დაკავშირებულია ადამიანის, საზოგადოებისა და სახელმწიფოს საქმიანობასთან. მათგან, როგორც საკუთარი თავისთვის, ისე გარემოსთვისაც, წარმოიშობა მუქარების უდიდესი რაოდენობა, რომელთა წყაროა სხვადასხვა სოციალური ძალის საქმიანობა [10].

დასკვნა

არსებითად კიბერსივრცის დაცულობაზე, მასში მიმდინარე კიბერომების შედეგებზე უკვე მნიშვნელოვნადაა დამოკიდებული საქართველოს პოლიტიკური და ეკონომიკური სუვერენიტეტი, ეროვნული ინტერესების დაცვისა და ეროვნული უშიშროების უზრუნველყოფის დონე. გარდა იმისა, რომ ინფორმაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად პირდაპირპროპორციულად იზრდება მათზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულება და ურთიერთკავშირი, კიბერუშიშროების უზრუნველყოფა უკვე იქცა საგარეო პოლიტიკის განუყოფელ შემადგენელ ნაწილად და სულ უფრო აქტიურ როლს ასრულებს საერთაშორისო ურთიერთობების საკითხშიც.

აქედან გამომდინარე, ინფორმაციული ეპოქის განვითარების ტენდენციების გათვალისწინებით, კიბერუშიშროების უზრუნველსაყოფად საქართველოს სახელმწიფოს ამოცანაა პრიორიტეტული გახადოს **სოციალურ-პოლიტიკური საქმიანობა** (დოქტრინის, კანონების, სამართლებრივი აქტების შემუშავება და მიღება, კიბერუშიშროების უზრუნველყოფისა და კიბერუსაფრთხოების დაცვის მართვის პროცესის სრულყოფა და სხვ.). წარმართოს კიბერუშიშროების უზრუნველყოფის პოლიტიკა ისე, რომ არა მხოლოდ მოიგერიოს მტრის შემოტევები კიბერსივრცეში, არამედ შექმნას საკუთარი კიბერსივრცე, სხვა შემთხვევაში იქნება მუდამ სხვა სახელმწიფოთა მანიპულირების ობიექტი. ასევე, ტერმინების გამოყენებისას გაითვალისწინოს ენათმეცნიერების მიერ მეცნიერულად დადგენილი ნორმები და გამოიყენოს ისინი შესაბამის კონტექსტში.

ლიტერატურა

1. Oxford Learner's Dictionaries. (n.d.). https://www.oxfordlearnersdictionaries.com/definition/english/digital_2 ;
2. Oxford English Dictionary. (n.d). https://www.oed.com/start?showLogin=false ;
3. Cambridge Dictionary. (n.d.). https://dictionary.cambridge.org/dictionary/english/cyberspace ;
4. Computer Security Resource Center – CSRC. Information Technology Laboratory. (n.d.) Meaning of Cyberspace. https://csrc.nist.gov/glossary/term/cyberspace ;
5. Kuprashvili, H. (2022). Functional Anatomy of the Staff of the National Security Council of Georgia. San Francisco: *Academia Letters*. https://doi.org/10.20935/AL4502 (In Georgian);
6. Hardy, H. (2016, June 15). *Cyberspace is officially a war zone – NATO.* Euronews. https://www.euronews.com/2016/06/15/cyberspace-is-officially-a-war-zone-nato ;
7. *NATO braces for cyber war.* (2016, September 8). Euronews. https://www.euronews.com/2016/09/08/nato-braces-for-cyber-war ;
8. Government of Georgia. (2021). The national-level conceptual document *Georgia's National Cybersecurity Strategy* for 2021-2024 and its Action Plan. (Document number: 482). https://www.matsne.gov.ge/ka/document/view/5263611?publication=0 (In Georgian);
9. Kuprashvili, H. (2014). Terms „ushishroeba“ (Security) or „usaprtkhoeba“ (Safety)?! Tbilisi: Universali. https://gtu.ge/Library/Pdf/El_wignebi/erovnuli_us.pdf (In Georgian);
10. Kuprashvili, H. (2021) *National Security and National Interests.* Tbilisi: Meridiani. https://www.researchgate.net/publication/358243831_erovnuli_ushishroeba_da_erovnuli_interesebi (In Georgian).

UDC 321
SCOPUS CODE 3320
https://doi.org/10.36073/1512-0996-2022-2-167-177

Cyberspace and Terms: "kiberushishroeba" (Cyber Security) and "kiberusaprtkhoeba" (Computer Security)

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

Reviewers:
E. Gvenetadze, Professor, Faculty of Law and International Relations, GTU
E-mail: e.gvenetadze@mail.ru
S. Midelashvili, Associate Professor, Faculty of Law and International Relations, GTU
E-mail: Sophiomidelashvili@gmail.com

Abstract. The terms "kiberushishroeba" (cyber security) and "kiberusaprtkhoeba" (computer security) are often used in inappropriate contexts. The term "kiberushishroeba" is used when the avoidance of an imminent threat requires the formulation and implementation of socio-political measures (development and adoption of doctrines, laws, legal acts, improvement of the "kiberushishroeba" and "kiberusaprtkhoeba" assurance management process), because the state of protection of national interests in cyberspace is achieved through the establishment of an effective Computer Security system, cyberspace sustainability, protection from unwanted internal and external influences – as a result of qualified cyber policy. The starting-point in "kiberushishroeba" providing is political aim and the result – to achieve them. "Kiberusaprtkhoeba" is an integral component of "kiberushishroeba", a carrier of different content and weight. "Kiberusaprtkhoeba" is a combination of technologies, methods and processes of technical protection against cyberattacks of components (networks, computers, programs, data, devices) within the field of computer and information-telecommunication. It is more associated with protection from "technical" threats (to be taken organizational-technical measures: to identify those responsible for the operation safety of the computer-information-telecommunication field and to introduce appropriate technical infrastructure and security system) or rather to "protection of labor safety" than formulation and implementation of socio-political goals. The goal of "kiberusaprtkhoeba" is to protect them, and to achieve this protection as a whole is ensuring of the result that meets the requirements of the political goal of "kiberushishroeba".

Keywords: computer security; cybersecurity; cyberspace; information age; information security; national security; politics.

განხილვის თარიღი 22.01.2022
შემოსვლის თარიღი 24.02.2022
ხელმოწერილია დასაბეჭდად 06.06.2022