საქართველოს კიბერუსაფრთხოების პოლიტიკა და მისი რეალიზაციის პერსპექტივები

თამთა კოდუა

კავკასიის საერთაშორისო უნივერსიტეტის დოქტორანტი

tamta.kodua@ciu.edu.ge

ORCID iD: https://orcid.org/0000-0002-4563-7131

DOI: 10.52340/splogos.2026.01.05

აბსტრაქტი

თანამედროვე მსოფლიოში კიბერსივრცე სახელმწიფოების უსაფრთხოების ერთ-ერთ უმნიშვნელოვანეს კომპონენტად იქცა. ინფორმაციული ტექნოლოგიების სწრაფი განვითარება, სახელმწიფო და კერძო სექტორის ციფრული ტრანსფორმაცია და კიბერშეტევების გახშირება ზრდის კიბერუსაფრთხოების ეფექტიანი პოლიტიკის აუცილებლობას. საქართველო, როგორც განვითარებადი დემოკრატიული სახელმწიფო და რეგიონული თანამშრომლობის აქტიური მონაწილე, განსაკუთრებულ ყურადღებას უთმობს კიბერუსაფრთხოების სისტემის გაძლიერებასა და საერთაშორისო სტანდარტებთან დაახლოებას.

საქართველოს კიბერუსაფრთხოების პოლიტიკა ეფუძნება ეროვნული უსაფრთხოების სტრატეგიასა და სპეციალურ საკანონმდებლო და ინსტიტუციურ ჩარჩოს, რომელიც მიზნად ისახავს კრიტიკული ინფრასტრუქტურის დაცვას, სახელმწიფო უწყებების ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფას და კიბერინციდენტებზე სწრაფ რეაგირებას. ამ მიმართულებით ქვეყანაში შექმნილია შესაბამისი უწყებები და მექანიზმები, რომლებიც უზრუნველყოფენ მონიტორინგს, პრევენციასა და თანამშრომლობას როგორც შიდა, ისე საერთაშორისო დონეზე.

პოლიტიკის რეალიზაციის პერსპექტივები მნიშვნელოვნად არის დამოკიდებული ტექნოლოგიური შესაძლებლობების განვითარებაზე, კვალიფიციური კადრების მომზადებაზე, საზოგადოების ცნობიერების ამაღლებასა და საერთაშორისო პარტნიორებთან თანამშრომლობის გაღრმავებაზე.

განსაკუთრებით მნიშვნელოვანია საჯარო და კერძო სექტორების კოორდინაცია, კიბერუსაფრთხოების კულტურის ჩამოყალიბება და თანამედროვე ტექნოლოგიების დანერგვა.

საბოლოოდ, საქართველოს კიბერუსაფრთხოების პოლიტიკის წარმატებული განხორციელება ხელს შეუწყობს ქვეყნის ეროვნული უსაფრთხოების განმტკიცებას, ეკონომიკური სტაბილურობის უზრუნველყოფას და ციფრული გარემოს სანდოობის ზრდას. მიუხედავად არსებული გამოწვევებისა, სწორი სტრატეგიული მიდგომებისა და საერთაშორისო გამოცდილების გაზიარების პირობებში, საქართველოს აქვს რეალური შესაძლებლობა განავითაროს მდგრადი და ეფექტიანი კიბერუსაფრთხოების სისტემა.

საკვანძო სიტყვები: კიბერუსაფრთხოება, სახელმწიფო უსაფრთხოება, კიბერპოლიტიკა, ინფორმაციული უსაფრთხოება, ციფრული ტრანსფორმაცია.

Georgia's Cybersecurity Policy and Prospects for its Implementation

Tamta Kodua

PhD Student,

Caucasus International University

tamta.kodua@ciu.edu.ge

ORCID iD: https://orcid.org/0000-0002-4563-7131

Abstract

In the modern world, cyberspace has become one of the most important components of state security. The rapid development of information technologies, the digital transformation of the state and private sectors, and the increase in cyber attacks increase the need for an effective cybersecurity policy. Georgia, as a developing democratic state and an active participant in regional cooperation, pays special attention to strengthening the cybersecurity system and bringing it closer to international standards.

Georgia's cybersecurity policy is based on the National Security Strategy and a special legislative and institutional framework aimed at protecting critical infrastructure, ensuring the security of information systems of state agencies, and responding quickly to cyber incidents. In this direction, the country has created relevant agencies and mechanisms that ensure monitoring, prevention, and cooperation both domestically and internationally.

The prospects for policy implementation depend significantly on the development of technological capabilities, the training of qualified personnel, raising public awareness, and deepening cooperation with international partners. Coordination between the public and private sectors, the formation of a cybersecurity culture, and the introduction of modern technologies are especially important.

Ultimately, the successful implementation of Georgia's cybersecurity policy will contribute to strengthening the country's national security, ensuring economic stability, and increasing the trustworthiness of the digital environment. Despite the existing challenges, with the right strategic approaches and international experience sharing, Georgia has a real opportunity to develop a sustainable and effective cybersecurity system.

Keywords: Cybersecurity, State Security, Cyber Policy, Information Security, Digital Transformation

თემის აქტუალობა

თანამედროვე პერიოდში მსოფლიოში წარმოუდგენელია ნებისმიერი ურთიერთობები ციფრული ტექნოლოგიების გარეშე. აქედან გამომდინარე კიბერსაფრთხეები ახალი გამოწვევაა როგორც მსოფლიოსთვის, ასევე საქართველოსათვის და გავლენას ახდენს საერთაშორისო უსაფრთხოებაზე. შესაბამისად იზრდება კიბერსივრცისგან მომდინარე არაერთი რისკისა და საფრთხის განზომილება, რაც მეტად აქტუალურს ხდის საკითხს.

კვლევის თეორიული ჩარჩო

ნაშრომის პრაქტიკულ მნიშვნელობად მიმაჩნია ის, რომ ის შეიძლება დამხმარე მასალად იქნეს გამოყენებული კიბერუსაფრთხოების პროფილის

დისციპლინისათვის. ვფიქრობ, ამ მიმართულებით მომუშავე ადამიანებს გამოადგებათ.

სამეცნიერო სიახლე

თემის სიახლე იქნება, ის თუ რა გავლენას ახდენს კიბერუსაფრთხოება საქართველოს ეროვნულ უსაფრთხოებაზე. ასევე განვსაზღვრავთ რა გამოწვევების წინაშე შეიძლება აღმოჩნდეს ქვეყანა საერთაშორისო უსაფრთხოების სისტემაზე ცვალებადი მსოფლიო წესრიგის პირობებში.

შესავალი

კიბერუსაფრთხოების სფეროში საქართველოს კიბერაქტორების მიერ გასული ათწლეულის განმავლობაში გადადგმულმა ნაბიჯებმა განაპირობა ის, რომ საქართველო მოხვდა მსოფლიოს ტოპქვეყნების ათეულში გაეროს „ITU“ კიბერუსაფრთხოების ინდექსში, რომელიც ზომავს ქვეყნების მიერ აღებულ პასუხისმგებლობას კიბერუსაფრთხოების მიმართულებით გლობალურ დონეზე. ამ ინდექსის გამოსათვლელად კვლევა მოიცავს კიბერუსაფრთხოების ხუთ ძირითად მიმართულებას: საკანონმდებლო ბაზას; ტექნიკურ აღჭურვილობას; ორგანიზაციულ სტრუქტურას; შესაძლებლობების განვითარებას და თანამშრომლობას. ცხადია, ამ რეიტინგში წინსვლა ნიშნავს კიბერუსაფრთხოების ეროვნული სისტემის აღიარებას და შეიძლება აღინიშნოს, რომ საქართველო დსთ-ს ზონაში წამყვან ქვეყნად შეფასდა. მიუხედავად ამ წარმატებებისა, კიბერუსაფრთხოების სტრატეგიული და კონცეპტუალური დოკუმენტაცია, ისევე როგორც საკანონმდებლო ბაზა ფუნდამენტურ განახლებას მოითხოვს.

საქართველო ერთ-ერთი პირველი ქვეყანაა მსოფლიოში, რომელმაც 2008 წელს დაინახა არა მხოლოდ სახმელეთო, საჰაერო და საზღვაო სივრცის დაცვის აუცილებლობა, არამედ კიბერსივრცის დავის აუცილებლობაც, რომელიც განმეორებითი და მიზანმიმართული კიბერთავდასხმებისგან, საკუთარ მიწაზე ფაქტობრივ სამხედრო ოპერაციებთან პარალელურად. მიუხედავად მიღწეული

პროგრესისა, მის საფუძველზე კიბერშეტევების წინააღმდეგ ბრძოლისა და მინიმიზაციის მცდელობისა, საქართველოს მაინც მოეთხოვება სიღრმისეული ძალისხმევა კიბერუსაფრთხოების განვითარების გაუმჯობესებულ, ეროვნულ-სტრატეგიულ დონეზე ასაყვანად. თუ წინა წლებში შეიქმნა კიბერუსაფრთხოების მდგრადი საფუძველი, მნიშვნელოვანია ამ დამხმარე ჩარჩოების მდგრადი განვითარების გაგრძელება, არსებული პროგრესის შენარჩუნება და ინსტიტუციური სტრუქტურის აგება, რომელიც გააძლიერებს კიბერუსაფრთხოების უზრუნველყოფის ეროვნულ შესაძლებლობებს და საქართველოს კიბერუსაფრთხოების პოლიტიკის სტრატეგიულ მიმართულებებს. საჯარო სექტორის ელექტრონული სერვისები იყენებენ ორფაქტორიან ავთენტიფიკაციას და ძლიერ კრიპტოგრაფიულ გადაწყვეტილებებს ეროვნულ ელექტრონულ ავთენტიფიკაციაში. კრიპტოგრაფიული გადაწყვეტა უნდა შეესაბამებოდეს „NIST“-ის 800-78-3 სპეციალურ გამოცემას, „ECRYPT II“ ყოველწლიურ მოხსენებას ალგორითმებისა და გასაღების ზომის შესახებ (2011-2012); „საქართველოს მოქალაქისა და საქართველოში მცხოვრები უცხოელისთვის საქართველოს მოქალაქის პირადობის (ბინადრობის) მოწმობისა და პასპორტის გაცემის წესის შესახებ“ კანონის მე-14 მუხლს, რომელიც განსაზღვრავს პირადობის მოწმობისა და მისი მოწმობის „ე“ მოთხოვნების მახასიათებლებს; „ციფრული ხელმოწერის სერტიფიკატების ტექნიკური რეგულირების და ციფრული ხელმოწერის სერტიფიკატების გამცემი მასერტიფიცირებელი ორგანოების დამტკიცების შესახებ“ მთავრობის №88 დადგენილებას; მე-3 მუხლს, რომელშიც ნათქვამია, რომ კვალიფიციური სერტიფიკატები უნდა შეესაბამებოდეს „ETSI TR“ 102 437 „TS“ 101 456 სახელმძღვანელოს“; და „PKI“ აპლეტს, რომელიც გამოიყენება „ID“ ბარათის კრიპტოგრაფიული ფუნქციებისთვის, რომელსაც აქვს ალგორითმი „RSA“-2048. ქვეყანაში არსებობს მონაცემთა გაცვლის უსაფრთხო ინტერორგანიზაციათაშორისი გარემო (უსაფრთხო ინტერნეტი), რაც საშუალებას აძლევს საჯარო სექტორის სუბიექტებს უზრუნველყონ უსაფრთხო ვებსერვისები მოქალაქეებისა და მეწარმეებისთვის. კერძო სექტორი და სხვა სუბიექტები

წარმოადგენენ ინტერფეისებს ამ გარემოში, თუ ისინი უზრუნველყოფენ ან მონაწილეობენ საჯარო სერვისების მიწოდებაში.[81]

საქართველოს მთავრობამ მონაცემთა გაცვლის სააგენტოს მიანიჭა ავტორიზაცია, შექმნას და შეინარჩუნოს საქართველოს სამთავრობო „გეითვეი“ – უსაფრთხოების პლატფორმა მთავრობასა და კერძო სუბიექტებს შორის მონაცემთა გაცვლისთვის. „G3“ – საქართველოს სამთავრობო „გეითვეის“ მონაცემთა გაცვლის ინფრასტრუქტურის დონე, რომელიც „e-ID“ მართვის (რეგისტრაცია, ავთენტიფიკაცია და ავტორიზაცია), უსაფრთხოების, აპლიკაციების თავსებადობისა და ელექტრონული სერვისების ინტეგრაციის საშუალებას იძლევა, „ვებ“-ზე დაფუძნებული სამუშაო ნაკადის გამოყენებით „back“-ოფისის სისტემების ურთიერთდაკავშირებისათვის, რაც უზრუნველყოფს ერთიან და ინტეგრირებულ მთავრობის ხედვას, ტრანზაქციებისა და დოკუმენტების წარდგენის პროცესის სტანდარტიზაციით და ერთიანი რეგისტრაციისა და ხელმოწერის გამოცდილების უზრუნველყოფით. საქართველოს კიბერუსაფრთხოების მიღწევები არ შემოიფარგლება მხოლოდ ტექნიკური ასპექტებით, არამედ მოიცავს ორგანიზაციულ და სამართლებრივ შესაძლებლობებს. საქართველომ მართლაც აამოქმედა ელექტრონული მეგობრული კიბერუსაფრთხოებისა და მონაცემთა დაცვის სამართლებრივი სისტემა. საქართველო არის პირველი აღმოსავლეთ პარტნიორობა 5-ის („EaP“) ქვეყანა, რომელიც უმეტეს შემთხვევაში შეესაბამება ევროკავშირის კანონს „eGOV“ და „ICT1“-ს. 2017 წელს საქართველომ მოახდინა „eIDAS“-ის სრული ინტეგრაცია – ევროპარლამენტისა და საბჭოს 2014 წლის 23 ივლისის რეგულაცია („EU“) No 910/2014 შიდაბაზარზე ელექტრონული ტრანზაქციების ელექტრონული იდენტიფიკაციისა და ნდობის სერვისების შესახებ – და გააუქმა დირექტივა 1999/93/ „EC“ თავის ახალ კანონში ელექტრონული დოკუმენტაციისა და ელექტრონული ნდობის სერვისების შესახებ, რითაც დაადგინა გამოყენების წესები და პირობები კვალიფიციური ელექტრონული

[81] საქართველოს კიბერუსაფრთხოების ფორუმი, 2024.

ხელმოწერის, უსაფრთხო ციფრული ავთენტიფიკაციისა და ევროკავშირის მოთხოვნების მსგავსი სხვა კვალიფიციური ნდობის სერვისებისთვის.[82]

კიბერდანაშაული საქართველოში

კიბერსივრცე არის ნაყოფიერი ნიადაგი დანაშაულებრივი ქმედებების ჩასადენად. ტექნოლოგიური ინოვაციების წყალობით, დისტანციურად და ფარულად დანაშაულის ჩადენის შესაძლებლობა, მტკიცებულებების ცვალებადობა, კრიმინალების იდენტიფიცირების სირთულეები და იურისდიქციასთან დაკავშირებული პრობლემები, ინტერნეტის არასანქცირებულ გამოყენებას ხელსაყრელ სივრცედ აქცევს კიბერდანაშაულებისთვის. „კიბერ“ ელემენტი ხდება თითქმის ნებისმიერი ტიპის დანაშაულის განუყოფელი ნაწილი.

საქართველომ განსაზღვრა კიბერდანაშაული და დაადგინა იგი „კიბერდანაშაულის შესახებ ევროპის საბჭოს კონვენციის“ შესაბამისი კანონმდებლობით; „კიბერდანაშაულის შესახებ საქართველოს სამართლებრივი ჩარჩო“ მოიცავს ყველა დანაშაულს, როგორც ამას მოითხოვს კიბერდანაშაულის შესახებ კონვენცია. საქართველოს კიბერდანაშაულის კანონმდებლობა შეესაბამება ევროპულ პრინციპებსა და წესებს, როგორც არსებითი, ასევე პროცედურული ასპექტებით, კერძოდ, ეროვნული კანონმდებლობა, დამნაშავეთა უკანონო წვდომა, უკანონო მოსმენა, მონაცემთა ჩარევა, სისტემაში ჩარევა, მოწყობილობების ბოროტად გამოყენება, კომპიუტერთან დაკავშირებული გაყალბება, ბავშვთა პორნოგრაფიასთან დაკავშირებული დანაშაულები და საავტორო და მასთან დაკავშირებული უფლებების დარღვევასთან დაკავშირებული დანაშაულები.

ბოლო ხუთი წლის განმავლობაში დაფიქსირდა, რომ კიბერდამნაშავეებმა გაზარდეს თავდასხმები სახელმწიფოს საკუთრებაში არსებულ კრიტიკულ სექტორებსა და სხვა კომერციული სექტორის სერვისებზე და მიზნად ისახავდნენ

[82] საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ.

მინიმუმ რეპუტაციის დაკარგვას და სათანადო პირობებში კი, აღნიშნული სექტორების სრული დახურვის მიღწევას. ასეთი შემთხვევის კარგი მაგალითია 2016 წელს განხორციელებული „DdoS„ შეტევა საბანკო სექტორისა და სახელმწიფო ფინანსური ელექტრონული სერვისების წინააღმდეგ. შედეგად, ონლაინ საბანკო სერვისებისა და სახელმწიფო საგადასახადო სისტემების ფუნქციონირება, მინიმუმ მცირე დროით შეჩერდა. ყველაზე გავრცელებული თავდასხმები კრიტიკულ ინფრასტრუქტურებზე, რომლებიც ბოლო წლებში მოხდა, არის: „ფიშინგი“, გამოსასყიდი პროგრამები, „დეფეისი“, „DdoS“ და ელფოსტის გაყალბება.

ეროვნული კანონები და სტრატეგია კიბერუსაფრთხოების შესახებ

ძირითადი კანონი, რომელიც საფუძველს უქმნის საინფორმაციო და კიბერუსაფრთხოების ჩარჩოებს, არის საქართველოს ინფორმაციული უსაფრთხოების აქტი. კანონს ავსებს რიგი ქვენორმატიული აქტები, რომლებიც განსაზღვრავს და შემდგომ ავითარებს პრაქტიკული განხორციელების საკანონმდებლო დებულებებს. მიუხედავად არსებული საკანონმდებლო ბაზისა, კიბერუსაფრთხოების კანონმდებლობას აქვს რამდენიმე ხარვეზი, რომელიც მოითხოვს შესაბამის განხილვას შესაბამისი ორგანოების მხრიდან.

კერძოდ, გადაუდებელი აუცილებლობაა შემუშავდეს ინკლუზიური ჩარჩო კრიტიკული ინფორმაციული ინფრასტრუქტურის აქტივების კლასიფიკაციისთვის, რომელიც მოიცავს კერძო სექტორსაც. აღნიშნული კრიტიკული ინფორმაციული ინფრასტრუქტურის იდენტიფიცირების მეთოდოლოგია და პრინციპები უნდა განხორციელდეს ქსელისა და საინფორმაციო სისტემების უსაფრთხოების შესახებ დირექტივის („NIS“ დირექტივა) და ევროკავშირში არსებული საუკეთესო პრაქტიკის შესაბამისად. ბევრი ნაბიჯია გადასადგმელი ძლიერი აღსრულების მექანიზმების შემუშავებისთვის, რათა უზრუნველყოს კრიტიკული ინფორმაციის სისტემის სუბიექტების („CISS“) შესაბამისობა კიბერუსაფრთხოების ახალ სამართლებრივ რეჟიმთან. „CISS“-ისთვის კიბერუსაფრთხოების გარანტიების ნაკლებობა წარმოადგენს გამოწვევას კრიტიკული ინფორმაციული სისტემებისა და სერვისების ხელმისაწვდომობის,

მთლიანობისა და კონფიდენციალურობის თვალსაზრისით. გარდა ამისა, არსებული საკანონმდებლო ბაზა არ ითვალისწინებს ინციდენტების შეტყობინებისა და დაუცველობის გამჟღავნების წესებსა და პროცედურებს. ასევე არ არის ინციდენტების ტაქსონომიის წესები და რეაგირების სქემები; არ არსებობს ეროვნული დონის კიბერუსაფრთხოების ინციდენტების ცენტრალური რეესტრი. კანონი განსაზღვრავს მონაცემთა გაცვლის სააგენტოს და თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს, როგორც ქვეყნის კიბერუსაფრთხოებაზე პასუხისმგებელ სამთავრობო უწყებებს.

საქართველოს სისხლის სამართლის კოდექსით, კომპიუტერულ ინფორმაციაზე უნებართვო წვდომა; მავნე პროგრამის შექმნა, გამოყენება ან გავრცელება და ქსელური სისტემების ექსპლუატაცია ითვლება დანაშაულად, ისევე როგორც კიბერტერორიზმი. საერთაშორისო დონეზე საქართველომ 2012 წელს გაატარა ევროპის საბჭოს მიერ შემუშავებული კიბერდანაშაულის შესახებ კონვენციის რატიფიცირება. საქართველო ახლა იზიარებს კონვენციის წევრი ქვეყნების მართვის საერთო პრინციპებს და მიზნად ისახავს შექმნას ყოვლისმომცველი სამართლებრივი საფუძველი ეროვნულ დონეზე და ამავე დროს გააძლიეროს საერთაშორისო თანამშრომლობა.

საჯარო ადმინისტრაციის რეფორმის სამოქმედო გეგმა 2019-2020 წლებში, 2019 წლის 10 ივნისის მიღებული მთავრობის N 274 დადგენილებით, პირდაპირ ხაზს უსვამს მთავრობის ძალისხმევას კრიტიკული ინფორმაციის ქსელებისა და ინფრასტრუქტურის კიბერდაცვას: „მართვის მაღალი სტანდარტის უზრუნველსაყოფად, ასევე ძალიან მნიშვნელოვანია კრიტიკული ინფორმაციული ინფრასტრუქტურისა და საინფორმაციო სისტემების უსაფრთხოებისა და დაცულობის მაღალი დონე. ახალი სამოქმედო გეგმა განსაზღვრავს აქტივობებს, რომლებიც უზრუნველყოფენ ასეთი სისტემების უსაფრთხოებასა და დაცულობას და ზოგადად, კიბერ და ინფორმაციული უსაფრთხოების შესახებ ცნობიერების ამაღლებას“ (თავი 4, საჯარო მმართველობის რეფორმის სამოქმედო გეგმა 2019-2020 წწ.). კერძოდ, ის მოიცავს შემდეგ აქტივობებს: კრიტიკული ინფორმაციული სისტემის სუბიექტების განსაზღვრის მეთოდოლოგიის შემუშავებას, საჯარო

სექტორში შეჭრის აღმოჩენის სისტემის დანერგვას, სკოლებში კიბერჰიგიენის სასწავლო გეგმების შექმნას და შესაბამისი განახლებული სასწავლო მასალების შექმნას ელექტრონული სწავლების პლატფორმისთვის.[83]

დასკვნა

დღეისათვის საქართველოს აქვს ერთ-ერთი ყველაზე ძლიერი მხარდაჭერა კიბერუსაფრთხოების სფეროში. შემდეგი პერიოდისთვის იგეგმება ახალი პოლიტიკისა და სტრატეგიების შემოღება, ასევე საინფორმაციო მხარდაჭერა და წვრთნა კიბერუსაფრთხოების სპეციალისტებისთვის, ხოლო მესამე უსაფრთხოების სტრატეგია მუშავდება, რომელიც მოიცავს წინა ვერსიებში გამოტოვებულ სფეროებს, რათა არსებული ვერსია იყოს ჰარმონიზებული ევროპულ კანონმდებლობასა და სფეროს უსაფრთხოების სტანდარტებთან.

საქართველო არის იმ მცირერიცხოვან ქვეყნებს შორის, სადაც კიბერუსაფრთხოების განვითარება წინ უსწრებს მის „ICT“ განვითარებას. კიბერუსაფრთხოების თვალსაზრისით, მდგომარეობა ძალიან კარგია.

სხვა განვითარებადი ქვეყნების გაანალიზებით, რომლებიც ახორციელებენ ევროკავშირის მსგავს პროექტებს რეგიონში, როგორებიცაა მოლდოვა, სომხეთი, აზერბაიჯანი და უკრაინა, ცხადია, რომ საქართველოს აქვს ყველაზე მოწინავე და მხარდაჭერილი ჩარჩო კიბერუსაფრთხოების სფეროში და რეგიონის სხვა სახელმწიფოებს სთავაზობს გამოცდილებისა და კარგი პრაქტიკის გაზიარებას, რათა კიბერსფეროში უზრუნველყონ ციფრული გარემო უკეთესი მომავლისთვის.

საქართველოს მმართველობითი მიდგომებიდან მიღებული ზოგადი გაკვეთილები:

[83] საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ.

• ლიდერები მნიშვნელოვანია. მრავალი სამთავრობო, საჯარო და კერძო ორგანიზაციის ლიდერები კიბერუსაფრთხოებას და კიბერუსაფრთხოების მართვას პრიორიტეტად აქცევენ.

• ლიდერები არ არის ყველაფერი. კანონები, პოლიტიკა, სტრუქტურები და პროცესები ინიცირებას ახდენენ და შეუსაბამებენ კიბერუსაფრთხოების მმართველობას კიბერუსაფრთხოების პრიორიტეტებთან ისე, რომ პიროვნებების ცვლილებამ არ გამოიწვიოს ფოკუსის შეცვლა.

• მმართველობა კვეთს ორგანიზაციულ საზღვრებს. კიბერუსაფრთხოების განაწილებული ბუნება მოითხოვს არაერთ მართვის მექანიზმს, რომლებიც აკავშირებს მრავალ ორგანიზაციასა და სექტორს.

გამოყენებული ლიტერატურა

1. “Global Commission on Internet Governance,” Centre for International Governance Innovation, accessed November 19, 2019, https://www.cigionline.org/activity/global-commission-internet-governance.
2. “Global Commission on Internet Governance,” Centre for International Governance Innovation, accessed November 19, 2019, https://www.cigionline.org/activity/global-commission-internet-governance.
3. 5. Association Agenda between THE EUROPEAN UNION and GEORGIA 2017-2020 https://www.eeas.europa.eu/sites/default/files/annex_ii_-_eu-georgia_association_agenda_text.pdf.
4. Association Agenda between THE EUROPEAN UNION and GEORGIA 2017-2020 https://www.eeas.europa.eu/sites/default/files/annex_ii_-_eu-georgia_association_agenda_text.pdf.
5. Georgian Cybersecurity Forum, 2024, https://nsc.gov.ge/en/NEWS/georgia-cybersecurity-forum.html;

6. Martin Libicki, “The Coming of Cyber Espionage Norms,” in Defending the Core, ed. H. Rõigas R. Jakschis, L. Lindström and T. Minárik (Tallinn: NATO CCD COE Publications, 2017), 7–23.
7. Martin Libicki, “The Coming of Cyber Espionage Norms,” in Defending the Core, ed. H. Rõigas, R. Jakschis, L. Lindström and T. Minárik (Tallinn: NATO CCD COE Publications, 2017), 7–23.
8. On the approval of the National Cybersecurity Strategy of Georgia for 2021 – 2024 and its Action Plan, https://www.matsne.gov.ge/ka/document/view/5263611?publication=0.
9. საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ. https://www.matsne.gov.ge/ka/document/view/5263611?publication=0.
10. საქართველოს კიბერუსაფრთხოების ფორუმი, 2024. https://nsc.gov.ge/en/NEWS/georgia-cybersecurity-forum.html.