ბექა ლეჟავა •

საქართველოს კიბერუსაფრთხოების ინდექსის შედარებითი ანალიზი

აბსტრაქტი

ნაშრომის მიზანია საქართველოში არსებული კიბერ უსაფრთხოების ეკოსისტემის ანალიზი. დადგენა იმის, თუ რა გამოწვევების წინაშეა ქართული კიბერ სივრცე და როგორ გავლენას ახდენს იგი ქვეყნის კიბერ უსაფრთხოების გლობალურ ინდექსზე. საქართველოს გლობალური ინდექსის განსაზღვრისთვის, ნაშრომში გაანალიზებული და შედარებული იქნება ისეთი ორგანიზაციების კვლევები, როგორიცაა გაეროს საერთაშორისო საკომუნიკაციო გაერთიანება და ესტონეთის ელექტრონული მმართველობის აკადემია. ამასთან ერთად, მოხდება დარგის წამყვან ექსპერტებთან ექსპერტული ინტერვიუს ჩატარება და მიღებული შედეგების გაანალიზება, რის საფუძველზეც დადგინდება მიზეზები, რის გამოც ქვეყნის კიბერ უსაფრთოხების ინდექსი მკვეთრად შემცირდა 2018-2021 წლებში.

შესავალი

კიბერ ტექნოლოგიური განვითარების შეუქცევადმა პროცესმა და ჰაკერული თავდასხმების გახშირებულმა შემთხვევებმა საერთაშორისო საზოგადოებას ნათლად დაანახა ამ კუთხით უსაფრთხოების ზომების გაძლიერების აუცილებლობა.

• საქართველოს საზოგადოებრივ საქმეთა ინსტიტუტის“ (GIPA) დოქტორანტი. სამწუხაროდ, 2023 წლის მაისში ბექა ლეჟავა აგრესიული ფორმის ლიმფომის დიაგნოზით გარდაიცვალა. ბექას ხსოვნის პატივსაცემად, რომელიც გამორჩეული ადამიანი და მეცნიერი იყო, ჟურნალ „პოლიტიკის“ რედაქცია აქვეყნებს მის სადოქტორო სემინარს.

კიბერ დანაშაულს წარმოადგენს ნებისმიერი მართლსაწინააღმდეგო ქმედება, რომელიც ჩადენილია კომპიუტერული სისტემის გამოყენებით კიბერ სივრცეში. 21–ე საუკუნეში სწრაფი ტექნოლოგიური პროგრესის პარალელურად, კიბერ რისკების რაოდენობა მნიშვნელოვნად მატულობს. თანამედროვე პერიოდში კიბერდანაშაულის საკმაოდ გავრცელებული შემთხვევებია: ონლაინ თაღლითობა, კომპიუტერულ სისტემასთან უნებართვო წვდომა, ბავშვთა ონლაინ პორნოგრაფია, კომპიუტერული სისტემისა და მონაცემის უნებართვოდ გამოყენება და ა.შ.

ბევრ ქვეყანაში და ასევე საქართველოშიც კიბერ დანაშაულის მზარდი სტატისტიკა ძირითადად განპირობებულია კიბერ საკითხებზე საზოგადოების დაბალი ცნობიერებით. რაც უფრო დამოკიდებულია საზოგადოება თანამედროვე ტექნოლოგიებზე მით უფრო მოწყვლადია კიბერ თავდასხმების მიმართ. შესაბამისად, კიბერუსაფრთხოება **ძალიან აქტუალურია** როგორც საერთაშორისო ასევე რეგიონალურ დონეზე და ისეთივე **მნიშვნელობას** იძენს როგორიც ქვეყნის სახმელეთო, საჰაერო თუ საზღვაო ტერიტორიების დაცვაა.

კიბერ უსაფრთხოების საკითხის აქტუალობისა და მისი მნიშვნელობიდან გამომდინარე მრავალი საერთაშორისო თუ რეგიონალური ორგანიზაცია ატარებს ერთმანეთისგან დამოუკიდებელ კვლევებს, რითაც აფასებენ კიბერუსაფრთხოების სფეროს მისი ცალკეული კომპონენტის მიხედვით. თუმცა უნდა აღინიშნოს, რომ მათ შორის ყველაზე რეიტინგულად, სანდოდ და კომპეტენტურად აღიარებული არის ორი ორგანიზაციის მიერ წარმოდგენლი კვლევები, კერძოდ:

1)გაეროს ქვემდებარე სტრუქტურული ინსტიტუტის "საერთაშორისო სატელეკომუნიკაციო კავშირი/International Telecommunication Union (ITU)", რომელიც ყოველწლიურად ატარებს გლობალურ კვლევას კიბერუსაფრთხოების განვითარების შესახებ, რაც შემდეგ აისახება ნაშრომში "კიბერუსაფრთხოების გლობალური ინდექსი/Global Cybersecurity Index (GCI)". ITU თავის კვლევას აწარ-

მოებს უკვე თერთმეტი წელია და ყოველი წლის ივნისის თვეში აქვეყნებს წინა წლის კვლევის შედეგებს ;

2)ესტონური ორგანიზაცია "ელექტრონული მმართველობის აკადემია/e – Governance Academy (eGA)" ITU-ს მსგავსად eGA თავის კვლევას "ეროვნული კიბერუსაფრთხოების ინდექსი/National Cybersecurity Index (NCSI)" აწარმოებს კიბერუსაფრთხოების მიმართულებით, თუმცა არა გლობალურად არამედ ეროვნულ დონეზე ევროპის რეგიონის ქვეყნების მიხედვით და კვლევის შედეგებს აქვეყნებს ყოველი წლის სექტემბრის თვეში, ITU – „გლობალური კიბერ უსაფრთხოების ინდექსის" გამოქვეყნების შემდეგ .

მიუხედავად იმისა, რომ ITU-ს და eGA-ს მიერ კიბერ უსაფრთხოების გლობალური ინდექსის შესაფასებლად განსხვავებული მეთოდოლოგიები იყო გამოყენებული, კვლევის შედეგები ძალიან ახლოს არის ერთმანეთთან. ორივე ორგანიზაციის კვლევის ფოკუსი, მიმართულია სახელმწიფოს კიბერ უსაფრთხოების გაზომვად ასპექტებზე და კონცენტრირდება სახელმწიფოში არსებულ საკანონმდებლო ბაზაზე, სტრატეგიაზე, სამთავრობო უწყებებზე და ა.შ.

მოცემული ნაშრომის ფარგლებში კიბერ უსაფრთხოების ასპექტების განხილვა ელექტრონული მმართველობის პერსპექტივიდან ხდება და სახელმწიფოს კიბერ უსაფრთხოების ისეთ ასპექტებს ზომავს რომლებსაც **დიდი პრაქტიკული მნიშვნელობა** ენიჭება. კერძოდ, კვლევა გვაჩვენებს თუ რა მდგომარეობაა კიბერ უსაფრთხოების მიმართულებით საქართველოში, კიბერუსაფრთხოების კომპონენტებში თუ სად არის იგი წარმოდგენილი ძლიერად, სად უჭირს და სად შეიძლება მოხდეს კიბერშესაძლებლობების გაძლიერება.

ნაშრომის **მეცნიერულ სიახლეს** წარმოადგენს ის, რომ დამტკიცდება ჰიპოთეზა 2020 წელს ქართული კიბერუსაფრთხოების ინდექსის რეიტინგში საქართველოს პოზიციების გაუარესება მოხდა პანდემიით გამოწვეული კრიზისის გამო ანუ კიბერუსაფრთხოების ინდექსთან მიმართებით საქართველოს რეგრესი 2018 წლიდან 2021 წლამდე მხოლოდ პანდემიამ გამოიწვია თუ არა მხოლოდ მან.

ასევე **მეცნიერული სიახლეა** ის, რომ კიბერუსაფრთხოების ინდექსთან მიმართებით საქართველოს რეგრესი/უკუსვლა და პანდემია არ არის ანდა ნაკლებად არის ნაკვლევი (ცნობილი არ არის ბევრი სხვა კვლევების შედეგები ამ კუთხით) და ეს მცირე კვლევა შეეცდება დადოს შესაბამისი შედეგი/შედეგები და სიახლე/ სიახლეები შემოგვთავაზოს.

გამოყენებული ლიტერატურის მიმოხილვა

იქიდან გამომდინარე, რომ კიბერუსაფრთხოების სფეროში მიმდინარე მოვლენები ფართო საზოგადოებისათვის არცთუ დიდი ხნის წინ გახდა აქტუალური, მოცემულ ნაშრომში უმეტესად გამოყენებული იქნება ყველაზე რეიტინგულად, სანდოდ და კომპეტენტურად აღიარებული ორი ორგანიზაციის მიერ წარმოდგენილი კვლევები (1.გაეროს ქვემდებარე სტრუქტურული ინსტიტუტის "საერთაშორისო სატელეკომუნიკაციო კავშირის" (International Telecommunication Union-ITU) ნაშრომი/კვლევა "კიბერუსაფრთხოების გლობალური ინდექსი / Global Cybersecurity Index-GCI" და 2. ესტონური ორგანიზაცია "ელექტრონული მმართველობის აკადემიის" (e – Governance Academy - eGA) კვლევა "ეროვნული კიბერუსაფრთხოების ინდექსი / National Cybersecurity Index - NCSI"), ისევე როგორც გავლენიანი ანალიტიკური გამოცემებისა თუ დამოუკიდებელი ექსპერტების სტატიები და კიბერუსაფრთხოების სპეციალისტთა კვლევები თუ მოსაზრებები აღნიშნულ თემასთან დაკავშირებით.

კვლევის საგანი, მიზანი და ამოცანები

კვლევის საგანს წარმოადგენს კიბერუსაფრთხოების კონტექსტში საქართველოს რეალობა უკანასკნელი 5 წლის განმავლობაში, ხოლო კვლევის ობიექტია ქართული კიბერუსაფრთხოების ინდექსი ამავე პერიოდში.

კვლევია მიზანია ქართული კიბერუსაფრთხოების უკანასკნელი 5 წლის დინამიკის შესწავლა, რისთვისაც შეიძლება გამოიყოს შემდეგი ამოცანები:

–კიბერ უსაფრთხოების კონტექსტში საქართველოს რეალობის გაანალიზება;

–საქართველოს ციფრულ ბაზარზე არსებული გარემოს შესწავლა ზოგადად და ბოლო 5 წლის მონაცემების, კერძოდ, ქართული კიბერუსაფრთხოების ინდექსის შედარებითი ანალიზი;

–საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU-ს) გლობალური კიბერუსაფრთხოების ინდექსის და ესტონეთის ელექტრონული მმართველობის აკადემიის National Cyber Security Index-ის ანგარიშების კვლევა/ანალიზი საქართველოსთან მიმართებაში და ამ ინდექსების ინდიკატორებში გამოვლენილი მიზეზების კვლევა;

-ქართული კიბერუსაფრთხოების ინდექსის მონაცემების გაანალიზება ახალი კორონავირუსის (COVID-19) პანდემიასთან მიმართებაში.

საკვლევი კითხვა და ჰიპოთეზა:

საკვლევი კითხვა შემდეგნაირად არის ჩამოყალიბებული: ქართული კიბერუსაფრთხოების ინდექსის გაუარესება პანდემიასთან დაკავშირებული კრიზისით იყო განპირობებული?

ჰიპოთეზა კი შემდეგია: ქართული კიბერუსაფრთხოების განვლილი დინამიკის შესწავლისას გამოვლინდა და გამოიკვეთა 2020 წელს კიბერუსაფრთხოების ინდექსის რეიტინგში საქართველოს პოზიციების გაუარესება. ეს ყოველივე მოხდა პანდემიით გამოწვეული კრიზისის გამო.

კვლევის ფარგლებში გამოყენებულია დღეისათვის მსოფლიოში აპრობირებული სოციალურ (ასევე პოლიტოლოგიურ და იურიდიულ) მეცნიერებაში დამკვიდრებული კვლევის ძირითადი მეთოდები. მათ შორის: **მეორადი მონაცემების ანალიზის მეთოდი** – ე. წ. „სამაგიდე (კაბინეტური) კვლევა“, ნორმატიული, შემეცნე-

ბითი, სინთეზური, ანალიზური, დედუქციური, ინდუქციური, თვისებრივი, დოკუმენტის ანალიზის, შემთხვევის შესწავლის (ე.წ. "Case Study") და შედარებითი ანალიზის მეთოდები. გამოყენებულია ასევე კვლევაში აღნიშნული პრობლემის ირგვლივ შემუშავებული თეორიები, ფუნდამენტური კვლევების შედეგები და დებულებები. კვლევის ძირითადი წყაროა: საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU-ს) გლობალური კიბერუსაფრთხოების ინდექსის და ესტონეთის ელექტრონული მმართველობის აკადემიის National Cyber Security Index-ის ანგარიშები და, საერთოდ, წერილობითი წყაროები.

საწყის ეტაპზე ჩემს მიერ მოხდა შესაბამისი საკანონმდებლო ჩარჩოს და საკვლევი პრობლემის ირგვლივ არსებული ინფორმაციის გაანალიზება, შესწავლა (კვლევის ნორმატიული მეთოდი) და მოხდა დინამიკაში სახელმწიფო პოლიტიკის კვლევა კონკრეტული დოკუმენტების (სახელმწიფო სტრატეგიის, სამოქმედო გეგმების და ა.შ.) ანალიზის საფუძველზე (ისტორიული მეთოდი) და ეროვნული კანონმდებლობის საერთაშორისო სტანდარტებთან შესაბამისობის შეფასება (შედარებით–სამართლებრივი მეთოდი).

საკვლევი პრობლემები განხილულია, როგორც შედარებითი და შემეცნებითი, ისე სისტემურ–სინთეზური თვალსაზრისით. შესაბამისად გამოყენებულია სინთეზური და ანალიზური მეთოდებიც (ანალიზი და სინთეზი). კვლევაში გამოყენებულია ზოგადი დებულებიდან კერძო დასკვნის გამოყვანის მსჯელობის ხერხი და ასევე კერძო ფაქტებიდან/ცალკეული დებულებებიდან ზოგადი დასკვნის გამოყვანის მეთოდი (დედუქციური და ინდუქციური მეთოდები ანუ დედუქცია/ინდუქცია).

კვლევის ჩატარებისას დავეყრდენი ზემოაღნიშნულ მკაფიოდ განსაზღვრულ პრინციპებს და კვლევის მიზნის/ქვემიზნების მისაღწევად გამოვიყენე სოციოლოგიური კვლევის თვისებრივი მეთოდები: 1.მონაცემების/ინფორმაციის მოპოვების მეთოდი; 2. მონაცემების/ინფორმაციის შეგროვება და დამუშავება; 3. მონაცემების/ინფორმაციის ანალიზი და შეფასება.

აღნიშნული კვლევის ფარგლებში გამოყენებულია მეორადი მონაცემების ანალიზის მეთოდი, ე.წ. „სამაგიდე (კაბინეტური) კვლევა“, რომელიც მოიცავს იმ კვლევებისა და დოკუმენტების ანალიზს, რომლებიც კვლევაში გაცხადებულ საკვლევ საკითხებს ეხება.

გარდა ამისა, თვისებრივი კვლევა, ნახევრად სტრუქტურირებული ექსპერტული ინტერვიუს მეთოდით ჩატარდა შერჩეულ ექსპერტებთან. აღნიშნული ინტერვიუები ჩატარდა საქართველოში ერთ-ერთ ყველაზე ძლიერ კიბერუსაფრთხოების ექსპერტებთან.

ქართული კიბერუსაფრთხოების ინდექსი – საქართველოს პროგრესი 2018 წლამდე

კიბერუსაფრთხოების მიმართულებით ზოგადად ქვეყნდება გარკვეული შედეგები ვინ რომელ ადგილზეა, ვის რა პრობლემები ანდა გამოწვევები აქვს, ვინ რა მიმართულებით უფრო ძლიერია და სხვა.

საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU-ს) გლობალური კიბერუსაფრთხოების ინდექსი ერთ-ერთ პრესტიჟულ, ავტორიტეტულ ინდექსად ითვლება, გამომდინარე იქიდან, რომ იგი არის ჟენევაში ბაზირებული გაეროს ქვემდებარე ინსტიტუტი. ასევე მეორე ინდექსიც: ესტონეთის ელექტრონული მმართველობის აკადემიის National Cyber Security Index-იც საკმაოდ აღიარებულია. ამ ინდექსით 2017 წელს ევროპის მასშტაბით საქართველოს საკმაოდ კარგი მაჩვენებელი ჰქონდა. ჩეხეთი იყო პირველი, ხოლო საქართველო მეორე ადგილზე გავიდა.[1] “ესტონეთის ელექტრონული მმართველობის აკადემია მხოლოდ საქართველოში არ მუშაობს,

[1]ესტონური ორგანიზაცია “ელექტრონული მმართველობის აკადემია /e– Governance Academy (eGA)“ კვლევა “ეროვნული კიბერუსაფრთხოების ინდექსი /National Cybersecurity Index (NCSI)“ https://ega.ee/?fbclid=IwAR2oULZoX7COmvs4KPFRsjx1aixFlG_1XQsTy8PluVogSDAbDsppJvGyIk8

ბევრგან მუშაობს. სხვათაშორის ეს პირველი ორგანიზაცია იყო, რომელმაც ერთ-ერთმა პირველმა დაიწყო ელექტრონული მმართველობის თემებზე საქართველოს მხარდაჭერა. ამჟამად ტარდება ტვინინგის პროგრამა (ევროკავშირის პროექტი) კიბერუსაფრთხოების მიმართულებით".[2] - აცხადებს კიბერუსაფრთხოების ექსპერტი ვლადიმერ სვანაძე.

2017 წელს რატომ იყო საქართველო წარმატებული კიბერუსაფრთხოების მიმართულებით?

2017 წლის იანვარში დამტკიცდა **საქართველოს კიბერუსაფრთხოების მეორე ეროვნული სტრატეგია** და ასევე **სამოქმედო გეგმა**.[3] ივნისის თვეში გამოქვეყნდა საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU-ს) ანგარიში და საქართველო **2017** წელს **ევროპაში მე-2** ადგილზე, ხოლო **გლობალურად მე-8** ადგილზე გავიდა.[4]

2017 წელს კვლევის დროს დსთ-ს სივრცეში განგვიხილეს და ამ მასშტაბშიც/დსთ-ს ქვეყნებში 2017 წელს საქართველომ პირველი ადგილი დაიკავა. ITU ადრე საქართველოს დსთ-ს ქვეყნებში მოიაზრებდა, ხოლო 2018 წლიდან ამ კუთხით საქართველო უკვე გადავიდა ევროპულ ნაწილში/რეგიონში. "შემდეგ 2017 წლის აგვისტოში ჩატარდა ოლიმპიადა (სწავლებები და ოლიმპიადები ტარდება ყოველწლიურად ესტონეთში) და საქართველოს წარმომადგენელმა- ამჟამად თი ბი სი ბანკის კომპიუტერული უსაფრთხოების სპეცი-

[2] ნახევრად სტრუქტურირებული ექსპერტული ინტერვიუს რესპონდენტი: ვლადიმერ სვანაძე - ა(ა)იპ "ინტერნეტის განვითარების ინიციატივა", პრეზიდენტი, კიბერუსაფრთხოების ექსპერტი

[3] საქართველოს მთავრობის დადგენილება №14 საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ; 2017 წლის 13 იანვარი, ქ. თბილისი

[4] გაეროს ქვემდებარე სტრუქტურული ინსტიტუტის "საერთაშორისო სატელეკომუნიკაციო კავშირის" (International Telecommunication Union-ITU) ნაშრომი/კვლევა "კიბერუსაფრთხოების გლობალური ინდექსი/Global Cybersecurity Index-GCI" 2017, გვ. 59

ალისტმა ზვიად კიკვიძემ პირველი ადგილი აიღო იქ. ძლიერი სპეციალისტია ამ მიმართულებით და ეს იყო საკმაოდ კარგი მიღწევა ქვეყნისთვის".[5]- აცხადებს კიბერუსაფრთხოების ექსპერტი ვლადიმერ სვანაძე.

2017 წელი იყო საკმაოდ წარმატებული. რა უძღოდა ამას წინ?

• **2008** წლის აგვისტოს ომის შემდეგ შეიქმნა საჯარო სამართლის იურიდიული პირი – მონაცემთა გაცვლის სააგენტო (ამჟამად ციფრული მმართველობის სააგენტო);

• **2012** წელს მიღებულ იქნა **საქართველოს კანონი "ინფორმაციული უსაფრთხოების შესახებ"**[6];

• **2012** წელსვე ამავე კანონით განისაზღვრა კრიტიკული ინფრასტრუქტურის სუბიექტები და იქ შევიდა მხოლოდ სამთავრობო/საჯარო სექტორის წარმომადგენლები. კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხა თავიდან მოიცავდა 36 სუბიექტს (მიღების თარიღი: 11/03/2013), შემდეგ ამ სუბიექტთა რაოდენობა გახდა 39 (მიღების თარიღი: 29/04/2014), შემდეგ 15/08/2016 წელს გახდა 40 (დაემატა საქართველოს სახელმწიფო უსაფრთხოების სამსახური), ხოლო 31/12/2021 წელს გახდა 61 საჯარო/სამთავრობო სუბიექტი (პირველი კატეგორია) და შემდეგ კატეგორიებად დაემატა კერძო (მეორე და მესამე კატეგორია);

• **2012** წელსვე საქართველო შეუერთდა **ბუდაპეშტის კონვენციას "კომპიუტერული დანაშაულის შესახებ"**[7] რის შედეგადაც 2012 წლის ოქტომბრის ბოლოს საქართველოს შინაგან საქმეთა სამინისტროს კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო;

[5]ნახევრად სტრუქტურირებული ექსპერტული ინტერვიუს რესპონდენტი: ანდრო გოცირიძე - კიბერუსაფრთხოების საგანმანათლებლო კვლევითი ცენტრის დამფუძნებელი; იხ. ვლადიმერ სვანაძე (სქოლიო 2)

[6] საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ", საკანონმდებლო მაცნე, 05/06/2012

[7]კონვენცია კომპიუტერული დანაშაულის შესახებ, ბუდაპეშტი, საკანონმდებლო მაცნე, 23.XI.2001

• **2013** წელს დაიწერა **საქართველოს კიბერუსაფრთხოების პირველი ეროვნული სტრატეგია და სამოქმედო გეგმა** (2013-2015 წლების)[8];

• **2013** წელსვე საქართველოში შეიქმნა პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი (ამჟამად პერსონალურ მონაცემთა დაცვის სამსახური) და შესაბამისად დაიწერა სტრატეგია ამ მიმართულებით;

• **2014** წელს საქართველოს თავდაცვის სამინისტროში შეიქმნა კიბერუსაფრთხოების ბიურო. მანამდე არსებობდა კრიტიკული ინფრასტრუქტურის სუბიექტები, სადაც ასევე მოიაზრებოდა თავდაცვის სამინისტროც. 2014 წელს კი მოხდა გამიჯვნა თავდაცვის სფეროსი და სამოქალაქო სფეროსი. თავდაცვის სფეროზე პასუხისმგებელი გახდა: კიბერუსაფრთხოების ბიურო. "საქართველოს თავდაცვის სამინისტროში კიბერუსაფრთხოების ბიუროს შექმნა Capacity Building-ისთვის ძალიან მნიშვნელოვანი იყო. ჩატარდა რამდენიმე მნიშვნელოვანი კიბერ სავარჯიშო ამავე სამინისტროში ამერიკელებთან, პოლონელებთან, ესტონელებთან ერთად და ა.შ. და ეს ყველაფერი ამ ანგარიშებში აისახა შესაბამისად 2017 წელს".[9]- **აცხადებს კიბერუსაფრთხოების ექსპერტი ანდრო გოცირიძე.**

როდესაც კვლევა ჩატარდა 2012 წლიდან 2016 წლამდე გამოვლინდა, რომ საქართველომ საკმაოდ მოკლე დროში გააკეთა ეს ყველაფერი. "საერთაშორისო ურთიერთობებში ჩრდილოატლანტიკურ ალიანსთან (ნატოსთან) დამყარდა მჭიდრო ურთიერთობა და ჩატარდა პირველი ერთობლივი წვრთნები, რაც Inter Agency და International Cooperation-ში ანუ ამ ორი ინდიკატორისათვის მნიშვნელოვანია".[10] - **აცხადებს კიბერუსაფრთხოების ექსპერტი ან-**

[8] საქართველოს პრეზიდენტის ბრძანებულება №321 საქართველოს კიბერუსაფრთხოების სტრატეგიისა დასაქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013–2015 წწ. სამოქმედო გეგმის დამტკიცების შესახებ; 2013 წლის 17 მაისი, ქ. თბილისი

[9] იხ. ანდრო გოცირიძე (სქოლიო 5)

[10] იხ. ანდრო გოცირიძე (სქოლიო 5)

დრო გოცირიძე. შემდეგ საქართველო შეუერთდა ევროპულ სწავლებებს. ესტონეთშიც დადიოდნენ, ისინიც ჩამოდიოდნენ და საქართველომ ამ ყველაფერს, რომ მიაღწია სწორედ ამ ყველაფერმა ასახვა ჰპოვა საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU-ს) და ესტონური ორგანიზაცია "ელექტრონული მმართველობის აკადემიის" (eGA-ს) ანგარიშში. ეს კი იყო მნიშვნელოვანი წარმატება.

ქართული კიბერუსაფრთხოების ინდექსი – საქართველოს რეგრესი 2018 წლიდან 2021წლამდე

2018 წელს საქართველო **გლობალურად მე-18-ეა** (საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU-ს) გლობალური კიბერუსაფრთხოების ინდექსი)[11], ხოლო **ევროპაში მე-9-ეა** (ესტონეთის ელექტრონული მმართველობის აკადემიის ინდექსი National Cyber Security Index)[12], ხოლო **2019 წელს** შესაბამისი ინდექსების ანგარიშები არ გამოუციათ.

2020 წელს საქართველო **გლობალურად 55-ეა** (საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU-ს) გლობალური კიბერუსაფრთხოების ინდექსი)[13], ხოლო **ევროპაში 30-ეა** (ესტონეთის ელექტრო-

[11] გაეროს ქვემდებარე სტრუქტურული ინსტიტუტის "საერთაშორისო სატელეკომუნიკაციო კავშირის" (International Telecommunication Union-ITU) ნაშრომი/კვლევა "კიბერუსაფრთხოების გლობალური ინდექსი /Global Cybersecurity Index-GCI" 2018, გვ. 62-64

[12] იხ. ესტონური ორგანიზაცია "ელექტრონული მმართველობის აკადემია/e– Governance Academy (eGA)" კვლევა "ეროვნული კიბერუსაფრთხოების ინდექსი/National Cybersecurity Index (NCSI)" (Footnote 1)

[13] გაეროს ქვემდებარე სტრუქტურული ინსტიტუტის "საერთაშორისო სატელეკომუნიკაციო კავშირის" (International Telecommunication Union-ITU) ნაშრომი/კვლევა "კიბერუსაფრთხოების გლობალური ინდექსი/Global Cybersecurity Index-GCI" 2020, გვ. 26-30

ნული მმართველობის აკადემიის ინდექსი National Cyber Security Index)[14].

რატომ? 2020 წლისთვის შედეგების გაუარესება ბუნებრივია. საქართველოში 2018/2019 წლებიდან გარკვეული სტაგნაცია შეინიშნება კიბერუსაფრთხოების განვითარების კუთხით, თუმცა ეს არ არის საგანგაშო საკითხი. ამას თავისი მიზეზები და ახსნა აქვს. საქართველომ ასე უცებ ნაბიჯები, რომ გადადგა პარალელურად შემდეგ წლებში უკვე სხვებმაც განავითარეს ეს ყველაფერი და საქართველოს რეიტინგმა შესაბამისად უკან გადმოიწია.

საქართველოს 2020 წლის რეიტინგში გაუარესება მხოლოდ პანდემიის ბრალი არ იყო. გაუარესდა ინდექსი იმიტომ, რომ ობიექტურად 2018, 2019, 2020 წლებში საქართველოში სტაგნაცია იყო კიბერუსაფრთხოების თვალსაზრისით.

"პანდემია მოგეხსენებათ, რომ იყო სრულიად ახალი ხილი მხოლოდ კიბერუსაფრთხოებისთვის კი არა, ზოგადად ყველა სექტორისთვის, სფეროსთვის, ჯანდაცვის სფეროსთვისაც მათ შორის განსაკუთრებით. პანდემიამ ძალიან შეუშალა ხელი კიბერუსაფრთხოების განვითარებას და 2020 წლის ინდექსების შედეგებზეც აისახა. პანდემიის დროს პრიორიტეტი სამთავრობო დონეზე გახდა პანდემია და მასთან ბრძოლა, ხოლო კიბერუსაფრთხოებამ გადაინაცვლა შემდეგ პლანზე. პრიორიტეტებიდან არ ამოვარდნილა, მაგრამ უკან ჩამოიწია. მთელი აქცენტი პანდემიის პერიოდში გადატანილი იყო რა თქმა უნდა პანდემიაზე"[15] - აცხადებს კიბერუსაფრთხოების ექსპერტი ვლადიმერ სვანაძე.

2020 წელი იყო საკმაოდ წარუმატებელი კიბერუსაფრთხოების მიმართულებით. **რა უძღოდა ამას წინ?**

[14] იხ. ესტონური ორგანიზაცია "ელექტრონული მმართველობის აკადემია/e–Governance Academy (eGA)" კვლევა "ეროვნული კიბერუსაფრთხოების ინდექსი/National Cybersecurity Index (NCSI)" (Footnote 1)

[15] იხ. ვლადიმერ სვანაძე (სქოლიო 2)

• **კიბერუსაფრთხოების მეორე ეროვნული სტრატეგია** მოიცავდა 2017-2018 წლებს. ამ კიბერუსაფრთხოების ეროვნულ სტრატეგიას 2018 წელს გაუვიდა ვადა და უნდა დაწერილიყო მესამე სტრატეგია, რომლის უკიდურესი ვადა უნდა ყოფილიყო 2019 წლის მაისი. 2019 და 2020 წლები ისე გავიდა, რომ არ იქნა მიღებული სტრატეგია და ამან ასახვა ჰპოვა ანგარიშებში. მაშასადამე, არ გვქონდა რამდენიმე წელი კიბერუსაფრთხოების ახალი ეროვნული სტრატეგია, რომელსაც ისინი საკმაოდ დიდ მინუსად გვითვლიან. **კიბერუსაფრთხოების მესამე ეროვნული სტრატეგია**[16] მიღებულ იქნა გვიან ანუ 2021 წლის სექტემბერში.

„ასევე მნიშვნელოვანია, რომ 2018 წლის ბოლოს შევიკრიბეთ და დავიწყეთ კიბერუსაფრთხოების უკვე მესამე ეროვნულ სტრატეგიაზე მუშაობა იმიტომ, რომ 2019 წლის მაისში მიღებული უნდა ყოფილიყო იგი. შემდეგ 2019 წლის იანვარში ჩვენ კიდევ შევიკრიბეთ, ამაში ჩართული იყო დიდი ბრიტანეთის ოქსფორდის კიბერუსაფრთხოების ცენტრი, რომელიც გვეხმარებოდა ამ სტრატეგიის დაწერაში და საბოლოოდ მათ დაწერეს იგი ჩვენი რეკომენდაცია/წინადადებებით და მათზე დაყრდნობით. 2019 წლის ივნისამდე ვიყავით ჩართული ექსპერტები კერძო სექტორიდან, თუმცა შემდეგ უკვე თავის თავზე ამის დაწერა აიღო საჯარო/სახელმწიფო სექტორმა იმიტომ, რომ გადადიოდნენ უკვე სამოქმედო გეგმაზე სადაც უკვე სახელმწიფო სტრუქტურები იყო განსაზღვრული. პასუხისმგებელი სუბიექტები იყვნენ მხოლოდ სახელმწიფო სტრუქტურები და შესაბამისად ჩვენ უკვე ჩამოვშორდით ამ პროცესს”[17] - აღნიშნავს კიბერუსაფრთხოების ექსპერტი ვლადიმერ სვანაძე.

[16] საქართველოს მთავრობის დადგენილება №482 საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ; 2021 წლის 30 სექტემბერი, ქ. თბილისი

[17] იხ. ვლადიმერ სვანაძე (სქოლიო 2)

• ძალიან მოძველებული იყო **საქართველოს კანონი "ინფორმაციული უსაფრთხოების შესახებ"**, იმიტომ რომ გლობალურად გაჩნდა ახალი რეალობები (ყველა დადგა ამ რეალობების წინაშე) და შესაბამისად ამ ყველაფერმა ასახვა არ ჰპოვა კანონში, რომელიც ასევე გამომდინარე უნდა ყოფილიყო **კომპიუტერული დანაშაულის შესახებ ბუდაპეშტის კონვენციისა** რომელზეც მუდმივად მიდის მუშაობა და მუდმივად ვითარდება. ახალი რეალობა დგება, ახალი დანაშაულები ჩნდება და ა.შ. და ამ ყველაფრის ასახვა კანონში არ მოხდა. ასევე კანონში კრიტიკული ინფრასტრუქტურის სია არ მოიცავდა: კერძო სექტორს. კერძო სექტორი კრიტიკულ ინფრასტრუქტურაში შევიდა გვიან ანუ 2021 წლის დეკემბრიდან. მაშასადამე, აღნიშნულ რეალობას საქართველო ჩამორჩა და ნორმატიული აქტების კუთხით ბოლო წლებში ამ სფეროში საქართველომ მოიკოჭლა.

„როდესაც ვეუბნებით, რომ საკანონმდებლო ბაზა გვაქვს კი ბატონო ერთხელ ჩაგვითვალეს კარგ შედეგად, მაგრამ როდესაც სიღრმეებში ჩავიდნენ ნახეს, რომ საკანონმდებლო ბაზა ამბობდა, რომ კრიტიკული ინფრასტრუქტურა არ არის: ბიზნესი და თუ იგი არ არის კრიტიკული ინფრასტრუქტურა ეს სერიოზული პრობლემაა და ასევე იყო "ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონთან დაკავშირებით გარკვეული პრობლემები და ესეც ჩაგვითვალეს გაუარესებად და ამაზე დაყრდნობით დაეცა რეიტინგი. ის კანონი, რომელიც მანამდე მოქმედებდა იყო 2012 წელს მიღებული და იყო ძალიან მოძველებული. მაგალითად: არ არსებობდა აღსრულების მექანიზმები თუკი რომელიმე კრიტიკული ინფრასტრუქტურის სუბიექტი არ აკმაყოფილებდა პირობებს" [18] - აღნიშნავს კიბერუსაფრთხოების ექსპერტი ანდრო გოცირიძე.

• ამ პერიოდში ტექნიკური მიმართულებით საქართველომ ვერ მოახერხა ტექნიკური განვითარება. ერთადერთი თუ არ ჩავთვლით იმას, რომ კიბერუსაფრთხოების ბიუროში სპეციალური

[18] იხ. ანდრო გოცირიძე (სქოლიო 5)

სერვერები დაიდგა, ბატალიონებში ბრიგადების დონეზე დაიდგა სპეციალური საგანგაშო მოწყობილობები, მაგრამ გლობალურად საქართველოს მასშტაბით ამის ასახვა არ მოხდა.

• 2019-2020 წლების პერიოდში შიდა ინსტიტუციური ურთიერთობა მოირღვა, 95% ონლაინ მუშაობდა ამ პერიოდში და როცა საგანგებო სიტუაციებზე რეაგირების ოპერატიულ ჯგუფზე (CERT - Computer Emergency Response Team) ანუ დაცულობაზეა საუბარი - ონლაინ მუშაობა რთულია. ამ რთულ პროცესში კიბერუსაფრთხოების გლობალური ინდექსის ხუთივე მიმართულება (1. საკანონმდებლო ჩარჩოს, 2. ტექნიკური, 3. ორგანიზაციული, 4. შესაძლებლობების განვითარების და 5. თანამშრომლობის მიმართულება) მოირღვა, რამაც ასახვა ჰპოვა საქართველოს უკან დახევაზე.

„ამ ინდექსის გაუარესება მხოლოდ პანდემიასთან დაკავშირებული კრიზისით არ იყო განპირობებული. მან უბრალოდ ხელი შეუშალა გარკვეულ ტექნიკურ სამუშაო პროცესს. ტექნიკურად შეხვედრების ორგანიზება, ექსპერტების ჩამოყვანა და ა.შ. გარკვეულ სირთულეებთან იყო დაკავშირებული. შესაბამისად ამან თავისი უარყოფითი ზეგავლენა იქონია და ამ ყველაფერმა ასახვა ჰპოვა 2020 წლის ინდექსშიც”[19] - ამბობს კიბერუსაფრთხოების ექსპერტი ვლადიმერ სვანაძე.

• კიბერუსაფრთხოების საკითხის და მისი მნიშვნელოვანობის შესახებ ცნობიერება არ იყო შესაბამის საფეხურზე ამაღლებული. ისეთი ყურადღება არ ეთმობოდა ამ საკითხებს როგორიც საჭიროა და რაც უნდა დათმობოდა მას.

„აქ ძირეული პრობლემა ის არის, რომ კიბერუსაფრთხოების აღქმა როგორც მნიშვნელოვანი საკითხისა და სტრატეგიის აღქმა (არა აქვს მნიშვნელობა კიბერი იქნება თუ სხვა) როგორც მნიშვნელოვანი დოკუმენტისა არ იყო”[20] - აღნიშნავს კიბერუსაფრთხოების ექსპერტი ანდრო გოცირიძე.

[19] იხ. ვლადიმერ სვანაძე (სქოლიო 2)

[20] იხ. ანდრო გოცირიძე (სქოლიო 5)

კვლევის შედეგების შეჯამება

პროგრესის შეჯამება

2008 წლის აგვისტოს ომის შემდგომი პროგრესული ნაბიჯები კიბერუსაფრთხოების მიმართულებით საქართველოში 2017 წელს დაგვირგვინდა ამ მიმართულებით საქართველოს მაღალი რეიტინგების სახით გლობალური და რეგიონალური მასშტაბით.

ქართული კიბერუსაფრთხოების ინდექსის კუთხით 2018 წლამდე საქართველოს პროგრესის ანუ წარმატებების მიზეზებად/ფაქტორებად შეიძლება დასახელდეს შემდეგი:

- **2008** წლის აგვისტოს ომის შემდეგ საჯარო სამართლის იურიდიული პირი – მონაცემთა გაცვლის სააგენტოს (ამჟამად ციფრული მმართველობის სააგენტოს) შექმნა;
- **2012** წელს **"ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის** მიღება;
- **2012** წლიდან კრიტიკული ინფრასტრუქტურის საჯარო/სამთავრობო და კერძო სუბიექტების რაოდენობის ეტაპობრივი გაზრდა და მათი განსაზღვრა კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხაში;
- **2012** წელს საქართველოს მიერთება **"კომპიუტერული დანაშაულის შესახებ" ბუდაპეშტის კონვენციაზე**;
- **2012** წელს საქართველოს შინაგან საქმეთა სამინისტროს კრიმინალური პოლიციის დეპარტამენტში კიბერდანაშაულთან ბრძოლის სამმართველოს შექმნა;
- **2013** წელს პირველი ეროვნული სტრატეგიის (2013-2015 წლების) დაწერა/მიღება;
- **2013** წელს საქართველოში პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის (ამჟამად პერსონალურ მონაცემთა დაცვის სამსახურის) შექმნა და ამ მიმართულებით სტრატეგიის დაწერა/მიღება;

• **2014** წელს საქართველოს თავდაცვის სამინისტროში კიბერუსაფრთხოების ბიუროს შექმნა;

• **2017** წელს საქართველოს კიბერუსაფრთხოების მეორე სტრატეგიისა და სამოქმედო გეგმის დამტკიცება და ბევრი სხვა მიზეზები/ფაქტორები.

რეგრესის შეჯამება

ამრიგად 2017 წლის წარმატებების შემდეგ 2018 წლიდან საქართველოს რეიტინგის დაცემა დაიწყო კიბერუსაფრთხოების მიმართულებით. 2018, 2019 და 2020 წლებში საქართველოში სტაგნაცია იყო კიბერუსაფრთხოების თვალსაზრისით, რაც შედეგად საქართველოს 2020 წლის რეიტინგში მკვეთრი გაუარესებით გამოვლინდა.

საქართველოს 2020 წლის რეიტინგის ასეთი სახით გაუარესება მხოლოდ პანდემიის ბრალი არ იყო. უბრალოდ პანდემიის დროს პრიორიტეტი შეიცვალა და კიბერუსაფრთხოებამ გადაინაცვლა შემდეგ საფეხურებზე.

ქართული კიბერუსაფრთხოების ინდექსის კუთხით 2018 წლიდან 2021 წლამდე საქართველოს რეგრესის ანუ წარუმატებლობების მიზეზებად/ფაქტორებად შეიძლება დასახელდეს შემდეგი:

• კანონში ცვლილებების დროულად არ შეტანა. მათ შორის ყველაზე მნიშვნელოვანი ცვლილების არ განხორციელება 2021 წლამდე პერიოდში. კერძოდ, კრიტიკული ინფრასტრუქტურის სუბიექტებად საჯარო სექტორის გარდა ინტერნეტ პროვაიდერების ანუ სატელეკომუნიკაციო კომპანიების და კერძო სექტორის დროულად არ განსაზღვრა, მათი არ დამატება ახალ სიაში და მათი რაოდენობის დროულად არ გაზრდა (იგულისხმება **საქართველოს კანონი "ინფორმაციული უსაფრთხოების შესახებ"**);

• კიბერუსაფრთხოების მესამე ეროვნული სტრატეგიის და სამოქმედო გეგმის დროულად არ მიღება;

• საქართველოს თავდაცვის სამინისტროს მიერ თავისი სტრატეგიის დროულად არ მიღება;

• კანონით კერძო სექტორის არ დავალდებულება და ქვეყანაში კერძო CERT-ების/ საგანგებო სიტუაციებზე რეაგირების ოპერატიული ჯგუფების (CERT - Computer Emergency Response Team) და კერძო SOC-ების / უსაფრთხოების ოპერაციების ცენტრების (Security Operation Center-ს) დროულად არ ჩამოყალიბება (იგულისხმება მათი ჩამოყალიბება, შეღწევადობის ტესტზე ლიცენზიის მიღება, შეღწევაზე ტესტების ჩატარება ანუ შეღწევადობის ტესტების/დაცულობის წარმოება, აუდიტის ჩატარება, ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლების მიცემა კერძო სექტორის წარმომადგენლებისთვის და ა.შ. ასევე ამ ყოველივეს ეროვნულ სტრატეგიაში შეტანა);

• კანონით კერძო სექტორის დროულად არ დავალდებულება მოეწესრიგებინათ თავიანთი კრიტიკული ინფრასტრუქტურა, აეყვანათ თავისი კიბერუსაფრთხოების სპეციალისტები, კიბერუსაფრთხოების მენეჯერები, შემოეღოთ პერსონალური მონაცემების დაცვის მიმართულებით ოფიცრის ახალი შტატი (პერსონალური მონაცემების დაცვის ოფიცრის ან/და ინფორმაციული უსაფრთხოების მენეჯერების კატეგორია/პოზიცია ყველა ორგანიზაციაში) და შეექმნათ დასაქმების ახალი საშუალებები ქვეყანაში;

• სტრატეგიით კიბერუსაფრთხოების მიმართულებით საგანმანათლებლო სფეროს საკითხების დროულად არ გააქტიურება (საქართველოში აკადემიურ დონეზე (ბაკალავრიატი, მაგისტრატურა, დოქტორანტურა) არ ისწავლებოდა ეს სფერო);

• ასევე შესაბამის დოკუმენტებში ცნობიერების ამაღლების მიმართულების არ განსაზღვრა და კერძო/საჯარო სექტორს შორის თანამშრომლობის არ გააქტიურება იმ დონეზე რა დონეზეც საჭირო იყო (მაგალითად, სტრატეგიაში არ იქნა გათვალისწინებული/განსაზღვრული საკითხები ე.წ. Stakeholder-ების ანუ დაინტერესებული მხარეების მიმართულებით, Supply Chain-ის საკითხი ანუ მომწოდებელი კომპანიების კიბერუსაფრთხოების დაცულობა (ანუ სა-

იდან შემოდის პროდუქცია; რუსეთი, რომ საფრთხეა მაგალითად და იქ წარმოებული პროდუქცია/სერვისი, რომ არ უნდა მივიღოთ და სხვა) და ა.შ.

დასკვნა

ამრიგად, ქართული კიბერუსაფრთხოების განვლილი დინამიკის შესწავლისას გამოვლინდა და გამოიკვეთა 2020 წელს კიბერუსაფრთხოების ინდექსის რეიტინგში საქართველოს პოზიციების გაუარესება. მოხდა ეს მხოლოდ პანდემიით გამოწვეული კრიზისის გამო თუ სხვა მიზეზებიც გამოვლინდა ზემოაღნიშნული ინდექსის ინდიკატორებში? დიახ. ქართული კიბერუსაფრთხოების ინდექსის გაუარესება მხოლოდ პანდემიასთან დაკავშირებული კრიზისით არ იყო განპირობებული.

ნაწილობრივ გამართლდა და ნაწილობრივ დამტკიცდა კვლევის ჰიპოთეზა, რადგან პანდემიამ ირიბი გავლენა მოახდინა და შეაფერხა კიბერუსაფრთხოების გლობალური ინდექსის ხუთივე მიმართულება (1.საკანონმდებლო ჩარჩოს, 2.ტექნიკური, 3.ორგანიზაციული, 4.შესაძლებლობების განვითარების და 5.თანამშრომლობის მიმართულება), თუმცა კიბერუსაფრთხოების საკითხის და მისი მნიშვნელოვანობის შესახებ ცნობიერებაც არ იყო შესაბამის საფეხურზე ამაღლებული. ისეთი ყურადღება არ ეთმობოდა ამ საკითხებს როგორიც საჭიროა და მთელი აქცენტი პანდემიის პერიოდში გადატანილი იყო პანდემიაზე.

გამოყენებული ლიტერატურა

1. ესტონური ორგანიზაცია “ელექტრონული მმართველობის აკადემია/e– Governance Academy (eGA)“ კვლევა “ეროვნული კიბერუსაფრთხოების ინდექსი/National Cybersecurity Index (NCSI)“ https://ega.ee/?fbclid=IwAR2oULZoX7COmvs4KPFRsjx1aixFlG_1XQsTy8PluVogSDAbDsppJvGyIk8
2. ნახევრად სტრუქტურირებული ექსპერტული ინტერვიუს რესპონდენტი: ვლადიმერ სვანაძე - ა(ა)იპ "ინტერნეტის განვითარების ინიციატივა", პრეზიდენტი, კიბერუსაფრთხოების ექსპერტი
3. საქართველოს მთავრობის დადგენილება №14 საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ; 2017 წლის 13 იანვარი, ქ. თბილისი
4. გაეროს ქვემდებარე სტრუქტურული ინსტიტუტის “საერთაშორისო სატელეკომუნიკაციო კავშირის” (International Telecommunication Union-ITU) ნაშრომი/კვლევა “კიბერუსაფრთხოების გლობალური ინდექსი/Global Cybersecurity Index-GCI“ 2017
5. ნახევრად სტრუქტურირებული ექსპერტული ინტერვიუს რესპონდენტი: ანდრო გოცირიძე - კიბერუსაფრთხოების საგანმანათლებლო კვლევითი ცენტრის დამფუძნებელი
6. საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“, საკანონმდებლო მაცნე, 05/06/2012
7. კონვენცია კომპიუტერული დანაშაულის შესახებ, ბუდაპეშტი, საკანონმდებლო მაცნე, 23.XI.2001
8. საქართველოს პრეზიდენტის ბრძანებულება №321 საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013–2015 წწ. სამოქმედო გეგმის დამტკიცების შესახებ; 2013 წლის 17 მაისი, ქ. თბილისი

9. გაეროს ქვემდებარე სტრუქტურული ინსტიტუტის “საერთაშორისო სატელეკომუნიკაციო კავშირის” (International Telecommunication Union-ITU) ნაშრომი/კვლევა “კიბერუსაფრთხოების გლობალური ინდექსი/Global Cybersecurity Index-GCI“ 2018
10. გაეროს ქვემდებარე სტრუქტურული ინსტიტუტის “საერთაშორისო სატელეკომუნიკაციო კავშირის” (International Telecommunication Union-ITU) ნაშრომი/კვლევა “კიბერუსაფრთხოების გლობალური ინდექსი/Global Cybersecurity Index-GCI“ 2020
11. საქართველოს მთავრობის დადგენილება №482 საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ; 2021 წლის 30 სექტემბერი, ქ. თბილისი

Bekha Lezhava

A Comparative Study of Cybersecurity Index of Georgia

Abstract

The aim of the paper is to analyze the existing cyber security ecosystem in Georgia. Determining what challenges the Georgian cyberspace is facing and how it affects the country's global cyber security index.

In order to determine the global index of Georgia, the paper will analyze and compare the studies of such organizations as the United Nations International Communication Union and the Estonian e-Government Academy. Along with this, an expert interview will be conducted with leading experts in the field and the results will be analyzed, based on which the reasons why the country's cyber security index has decreased sharply in 2018-2021 will be determined.