Scientific and Practical Cyber Security Journal (SPCSJ) 5(3): 56-66 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

კიბერუსაფრთხოების საერთაშორისო ინდექსები და საქართველო

INTERNATIONAL INDEXES OF CYBERSECURITY AND GEORGIA

ვლადიმერ სვანაძე საქართველოს ტექნიკური უნივერსიტეტის დოქტორანტი, საქართველოსტექნოლოგიური ინოვაციების აკადემიის დირექტორი

Vladimer Svanadze, Georgian Technical University PhD Candidate. Director of Georgian Academy of Technological Innovations

რეზიუმე: კიბერუსაფრთხოებამ მიუხედავად თავისი განვითარების მოკლე პერიოდისა, შეიძლება ითქვას დაიკავა ერთერთი მთავარი ადგილი როგორც საერთაშორისო, ისე ეროვნულ უსაფრთხოებაში, გახდა ჩვენი ცხოვრების განუყოფელი ნაწილი, და მნიშვნელოვანი კომპონენტი. ფაქტიურად, ყოველივე ეს განაპირობა ინტერნეტისა და ინტერნეტ ტექნოლოგიების სწრაფმა განვითარებამ, პანდემიის ფონზე ელექტრონული სერვისების მიმართ გლობალურად მზარდმა მოთხოვნილებამ. ყოველივე ეს კი ითხოვს ინტერნეტის სტაბილურობისა და უსაფრთხოების დაცვის აუცილებლობას, რაშიც ჩართული არის როგორც ცალკეული ქვეყნები, ისე საერთაშორისო და რეგიონალური ორგანიზაციები. შეიძლება ითქვას, რომ ცალკეული ქვეყნების კიბერსივრცის უსაფრთხოება ისეთივე მნიშვნელოვანი გახდა, როგორც ქვეყნის სახმელეთო, საჰაერო, თუ საზღვაო ტერიტორიების დაცვა, და რაც თავის მხრივ ხდება საერთაშორისო და რეგიონალური უსაფრთხოების შემადგენელი ნაწილი. ფაქტიურად, რაც უფრო დამოკიდებულია საზოგადოება თანამედროვე ტექნოლოგიებზე, მით უფრო მოწყვლადია კიბერ თავდასხმების მიმართ.

მსოფლიო ეკონომიკური ფორუმის 2021 წლის გლობალური რისკების ანგარიშის მიხედვით, კიბერსივრცეში არსებული რისკები კვლავ შედიან გლობალური რისკების რიცხვში. პანდემიამ COVID – 19 დააჩქარა ტექნოლოგიების დანერგვის პროცესი, თუმცა, გამოავლინა კიბერ სისუსტეები და არამზაობა. ამვდროულად, გაამწვავა ტექნიკური უთანასწორობა როგორც საზოგადოებებს შორის გარედან, ისე მათ შიგნითაც.

იგივე ანგარიშის მიხედვით „მომავალ წელს ძალზედ მნიშვნელოვანია კიბერუსაფრთხოება განხილულ იქნეს, როგორც სტრატეგიული ბიზნეს - საკითხი და განვითარდეს მჭიდრო საპარტნიორო ურთიერთობები ინდუსტრიებს, ბიზნესის ლიდერებს, მარეგულირებელ ორგანოებსა და პოლიტიკოსებს შორის. ისევე, როგორც ნებისმიერი სხვა სტრატეგიული საზოგადოებრივი გამოწვევა, კიბერუსაფრთხოებაც ვერ მოგვარდება იზოლირებულად “.

საკვანძო სიტყვები: კიბერუსაფრთხოება, გლობალური ინდექსი, ეროვნული ინდექსი, განათლება, საერთაშორისო სატელეკომუნიკაციო კავშირი, ელექტრონული მმართველობის აკადემია, კიბერსივრცე

ABSTRACT: Despite its short period of development, cybersecurity has occupied one of the vital places in both international and national security; it has become an influential component and integral part of our lives. In fact, all these circumstances have been driven by the rapid evolvement of the Internet and Internet technologies, as well as the increasing global demand for e-services in the face of the pandemic. All above-mentioned determines the necessity for Internet stability and security with involvement of individual countries as well as international and regional organizations. It can be said that the cybersecurity of individual countries has become as important as the protection of the country land, air and sea and in turn it becomes an

integralTimes New Roman part of international and regional security. In fact, the more society relies on modern technology, the more vulnerable it is to cyber-attacks. According to the World Economic Forum 2021 Global Risks Report, cyber risks are still among the global risks. The COVID-19 pandemic has accelerated the implementation of technology, however, it revealed cyber vulnerabilities and unpreparedness. At the same time, it has exacerbated technical inequalities between societies both externally and internally. According to the same report, "next year, it is influential to consider cybersecurity as a strategic business issue and to develop close partnerships between industries, business leaders, regulators and politicians. Like any other strategic societal challenge, cybersecurity can't be solved separately in isolation." The paper offers the analysis of international indexes of cybersecurity and analyzes their correlation to Georgian ones.

KEYWORDS: *Cybersecurity, Global Index, National Index, Education, International Telecommunication Union, e – Governance Academy, Cyberspace*

კიბერუსაფრთხოების საკითხის აქტუალობისა და მისი მნიშვნელობიდან გამომდინარე უამრავი 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 აწარმოებს 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 კიბერუსაფრთხოების ინდექსის“ გამოქვეყნების შემდეგ.

მიუხედავად იმისა, რომ ITU - ს და eGA - ს მიერ კიბერუსაფრთხოების გლობალური ინდექსის შესაფასებლად განსხვავებული მეთოდოლოგიები იყო გამოყენებული, კვლევის შედეგები ძალიან ახლოს არის ერთმანეთთან. ორივე ორგანიზაციის კვლევის ფოკუსი, მიმართულია სახელმწიფოს კიბერუსაფრთხოების გაზომვად ასპექტებზე და კონცენტრირდება სახელმწიფოში არსებული საკანონმდებლო ბაზაზე, სტრატეგიაზე, სამთავრობო უწყებებზე და ა.შ. კვლევებში არ არის მოყვანილი ქვეყნებზე განხორციელებული და წარმატებით მოგერიებული კიბერ თავდასხმების მაგალითები, აქედან გამომდინარე, გარკვეულწილად კითხვის ნიშნის ქვეშ დგას სახელმწიფოს რეალური კიბერ თავდაცვითი პოტენციალი, თუმცა მოცემული ნაშრომის ფარგლებში, კიბერ უსაფრთხოების ასპექტების განხილვა ელექტრონული მმართველობის პერსპექტივიდან ხდება.

კიბერუსაფრთხოების გლობალური ინდექსი (GCI)

როგორც ზემოთ არის აღნიშნული „კიბერუსაფრთხოების გლობალური ინდექსი“ არის გაერო - ს ქვემდებარე სტრუქტურული ინსტიტუტის „საერთაშორიის სატელეკომუნიკაციო გაერთიანების (ITU)“, უფრო კონკრეტულად, ინფორმაციულ და კომუნიკაციების ტექნოლოგიების სპეციალიზირებული სააგენტოს ინიციატივა. მოცემული პროექტი პირველად გაეშვა 2015 წელს, და მისი მიზანი არის გლობალურად შეაფასოს კიბერუსაფრთხოების მდგომარეობა. ის აჩვენებს აგრეთვე თუ რა მდგომარეობაა კიბერუსაფრთხოების მიმართულებით ცალკეულ ქვეყანაში, კიბერუსაფრთხოების კომპონენტებში თუ სად არიან წარმოდგენილნი ძლიერად, სად უჭირთ, და სად შეიძლება მოხდეს კიბერშესაძლებლობების გაძლიერება. აგრეთვე, GCI - ით ხდება თითოეული ქვეყნის კიბერუსაფრთხოების მდგომარეობის ერთმანეთთან შედარება.

მიმდინარე წლის 29 ივნისს „საერთაშორისო სატელეკომუნიკაციო გაერთიანებამ (ITU)“ გამოაქვეყნა 2020 წლის „კიბერუსაფრთხოების გლობალური ინდექსი (GCI)“, რომელიც მოიცავს 194 სახელმწიფოს და კვლევა ტრადიციულად ხორციელდება ხუთი მიმართულებით, რაც მთლიანად აერთიანებს 20 კომპონენტს 82 კითხვით, კერძოდ:

1) **საკანონმდებლო ჩარჩოს მიმართულება** - კიბერკრიმინალის რეგულაცია; კიბერუსაფრთხოების რეგულაცია; ტრენინგები კიბერუსაფრთხოების სფეროში;
2) **ტექნიკური მიმართულება** - ეროვნული, სამთავრობო და სექტორული CERTები; სტანდარტები და სერტიფიკატები ორგანიზაციებისა და პროფესიონალებისთვის; ბავშვთა ონლაინ დაცულობა;
3) **ორგანიზაციული მიმართულება** - სტრატეგია; შესაბამისი სააგენტოები; კიბერუსაფრთხოების შეფასება;
4) **შესაძლებლობების განვითარება** - სტანდარტიზაციის ორგანოები; საუკეთესო პრაქტიკის კვლევის და განვითარების პროგრამები; საზოგადოების ცნობიერების ამაღლების კამპანიები; პროფესიონალთა ტრენინგ მოდულები; ეროვნული საგანმანათლებლო პროგრამები და აკადემიური სილაბუსები; წამახალისებელი მექანიზმები; კიბერუსაფრთხოების ადგილობრივი ინდუსტრია;
5) **თანამშრომლობის მიმართულება** - შიდა სახელმწიფოებრივი თანამშრომლობა; მრავალმხრივი შეთანხმებები; საერთაშორისო ხელშეკრულებებში მონაწილეობა; კერძო-საჯარო პარტნიორობა; უწყებათაშორისი თანამშრომლობა.

2020 წლის GCI - ში კვლევაში ჩართული იყო 169 მკვლევარი და ის მიმდინარეობდა, როგორც გლობალური გამოწვევების კუთხით, ისე რეგიონებისა და ქვეყნების მიხედვით. ITU - ს სტანდარტებით, რეგიონალური დაყოფა წარმოდგენილია შემდეგნაირად - აფრიკის რეგიონი, ამერიკის რეგიონი, არაბეთის სახელწიფოების რეგიონი, აზია - ოკეანეთის რეგიონი, ევროპა და დსთ - ს ქვეყნები.

ბოლო ინდექსის ფარგლებში ჩატარებული კვლევის შედეგების მიხედვით, კვლევაში მონაწილე პირველი 25 ქვეყნის ქულები და რეიტინგი მოცემული არის ქვემოთ მოყვანილ ცხრილში

ქვეყანა	ქულა	რეიტინგი
შეერთებული შტატები	**100**	**1**
დიდი ბრიტანეთი	**99.54**	**2**
საუდის არაბეთი	**99.54**	**2**
ესტონეთი	**99.48**	**3**
სამხრეთ კორეის რესპუბლიკა	**98.52**	**4**

სინგაპური	**98.52**	**4**
ესპანეთი	**98.52**	**4**
რუსეთის ფედერაცია	**98.06**	**5**
არაბეთის გაერთიანებული საემიროები	**98.06**	**5**
მალაზია	**98.06**	**5**
ლიეტვუა	**97.93**	**6**
იაპონია	**97.82**	**7**
კანადა	**97.67**	**8**
საფრანგეთი	**97.6**	**9**
ინდოეთი	**97.5**	**10**
თურქეთი	**97.49**	**11**
ავსტრალია	**97.47**	**12**
ლუქსემბურგი	**97.41**	**13**
გერმანია	**97.41**	**13**
პორტუგალია	**97.32**	**14**
ლატვია	**97.28**	**15**
ნიდერლანდები	**97.05**	**16**
ნორვეგია	**96.89**	**17**
მავრიკის რესპუბლიკა	**96.89**	**17**
ბრაზილია	**96.6**	**18**

წყარო: კიბერუსაფრთხოების გლობალური ინდექსი *GCI 2020*

კიბერუსაფრთხოების ეროვნული ინდექსი (NCSI)

როგორც აღინიშნა, კიბერუსაფრთხოების გლობალური კვლევის მეორე მნიშვნელოვან დოკუმენტსწარმოადგენს ესტონური ორგანიზაცია „ელექტრონული მმართველობის აკადემიის (eGA)“ მიერჩატარებული კვლევა „კიბერუსაფრთხოების ეროვნული ინდექსი“ (National CyberSecurity Index- NCSI), რომელიც ზომავს ქვეყნების მზაობას კიბერ საფრთხეების დაინციდენტების წინაშე. მოცემული კვლევა ფარავს შემდეგმიმართულებებს:

1) **კანონმდებლობა** - საკანონმდებლო აქტები; რეგულაციები; განკარგულებები;
2) **ორგანიზაციული** - არსებული სააგენტოები; ორგანიზაციები; CERT;
3) **თანამშრომლობა** - კომიტეტები; საბჭოები; სამუშაო ჯგუფები;
4) **შედეგები/პროდუქტები** - სამთავრობო პოლიტიკა; ტექნოლოგიები; ვებგვერდები; პროგრამები; აპლიკაციები.

მთლიანობაში, კვლევის ფარგლებში სახელმწიფოში არსებული კიბერთავდაცვითი პოტენციალი, 46 ინდიკატორის მიხედვით, 12 განზომილებაში იზომება და შედეგების მიხედვით დგინდება სახელმწიფოს კიბერუსაფრთხოების ინდექსი, კერძოდ:

- ელ - იდენტიფიკაცია და სერვისების;
- პერსონალურ მონაცემთა დაცვა;
- კიბერ ინციდენტებზე რეაგირება;
- კიბერ კრიზისების მართვა;
- კიბერ დანაშაულთან ბრძოლა;
- სამხედრო კიბერ ოპერაციები;

- კიბერუსაფრთხოების პოლიტიკის განვითარება;
- კიბერ საფრთხეების ანალიზი ;
- განათლება და პროფესიული განვითარება;
- წვლილი გლობალურ კიბერ უსაფრთხოებაში;
- ელ - სერვისების დაცვა;
- კრიტიკული ინფორმაციული ობიექტების დაცვა.

განათლება და კიბერუსაფრთხოება

აღსანიშნავია ის გარემოება, რომ კიბერუსაფრთხოების ორივე ინდექსში, გლობალურშიც და ეროვნულშიც, მოყვანილი კიბერშესაძლებლობების განვითარება თავის თავში მოიცავს ისეთ მნიშვნელოვან კომპონენტს როგორიც არის განათლება და პროფესიული განვითარება. ფაქტიურად, განათლება და პროფესიული განვითარება არის ის აუცილებელი მიმართულება, რომლის განვითარებაზეც ზრუნავს ყველა ქვეყანა. კერძოდ, კიბერუსაფრთხოების შესახებ განათლების ზრდის ხელშეწყობა და ცნობიერების გაზრდა ქვეყნებისთვის იმდენად პრიორიტეტულ და მნიშვნელოვან მიმართულებას წარმოადგენს, რომ ის შეყვანილი არის თითოეული ქვეყნის კიბერუსაფრთხოების ეროვნულ სტრატეგიებში. ამ მხრივ არც საქართველოს „კიბერუსაფრთხოების 2017 – 2018 წლების ეროვნული სტრატეგია და სამოქმედო გეგმა “ არის გამონაკლისი, სადაც მოცემული მიმართულება მოხსენიებულია როგორც ერთ - ერთი ძირითადი მიმართულება, კერძოდ:

1. კვლევა და ანალიზი;
2. სამართლებრივი ბაზის შემუშავება და სრულყოფა;
3. კიბერუსაფრთხოების სფეროში შესაძლებლობათა ამაღლება;
4. საზოგადოებრივი ცნობიერების ამაღლება და საგანმანათლებლო ბაზის შექმნა;
5. საერთაშორისო თანამშრომლობა.

უნდა ითქვას, რომ სტრატეგიებში განათლების სფეროს ასახვა ნათლად აჩვენებს ქვეყნების დიდ ინტერესს განავითაროონ თავიანთი კიბერუსაფრთხოებითი შესაძლებლობა, რაც პირდაპირ კავშირშია პროფესიული და კვალიფიციური ადამიანური რესურსის არსებობასთან. აქვე ცალკე აღსანიშნავია ის გარემოებაც, რომ სტრატეგიებში მოცემული კიბერუსაფრთხოების ძირითადი მიმართულებები, იქნება ეს კვლევა და ანალიზი, საერთაშორისო თანამშრომლობა, სამართლებრივ ბაზებზე მუშაობა და მისი განვითარება, თუ თავად კიბერუსაფრთხოების სფეროს შესაძლებლობების განვითარება და საზოგადოებრივი ცნობიერების ამაღლება, პირდაპირ კავშირშია სწორად დაგეგმილი და ძლიერი საგანმანათლებლო ბაზის განვითარებასთან, რადგან სტრატეგიის ყველა ჩამოთვლილი მიმართულება მოითხოვს კვალიფიციურ კადრს.

როცა ვსაუბრობთ კვალიფიციურ კადრზე იგულისხმება აკადემიური განათლების მქონე პირები, რომლებსაც მიღებული აქვთ სულ ცოტა ბაკალავრის აკადემიური ხარისხი. გარდა ამისა, არსებობს საერთაშორისო დონეზე აღიარებული სერტიფიცირებული კურსები, თუმცა მათი უმრავლესობა კონკრეტული მიმართულებით ითხოვს საბაზისო ცოდნას, რაც შესაბამისობაშია ბაკალავრის დონესთან. ასევე დამსაქმებელთა დიდი ნაწილი ვაკანტური ადგილის დასაკავებელი კონკურსის მოთხოვნების განათლების სექციაში პირდაპირ უთითებენ მინიმუმ ბაკალავრის დონეს. შესაძლებელია კიდევ ბევრი მაგალითის მოყვანა, თუმცა ეს ორი ერთმანეთისგან განსხვავებული მაგალითი პირდაპირ მიუთითებს კიბერუსაფრთხოების სფეროში აკადემიური განათლების მნიშვნელობაზე. აქვე თუ

დავამატებთ იმ ფაქტს, რომ გლობალურად კიბერუსაფრთხოების სპეციალისტთა აშკარა დეფიციტია, ხოლო მათზე მოთხოვნილება სულ უფრო იზრდება, მაშინ შეიძლება ითქვას, რომ ეს იქნება უახლესი მომავლის ერთ - ერთი მოთხოვნადი სპეციალობა. აგრეთვე, თუ გავითვალისწინებთ ასეთ მზარდ მოთხოვნილებას, თავისუფლად შეიძლება ითქვას, რომ მოცემული მიმართულების სპეციალისტების შრომითი ანაზღაურება არის საკმაოდ მაღალი. კერძოდ, მაგალითისთვის, https://www.payscale.com/ - ის მიხედვით, უსაფრთხოების ოპერაციების ცენტრის (Security Operations Center SOC) დამწყები ანალიტიკოსის წლიური ხელფასი 81,351 აშშ დოლარს შეადგენს. იგივე წყაროს ინფორმციით, საკმაოდ მაღალანაზღაურებადი არის ისეთი სპეციალობები როგორებიც არის:

- Penetration Tester;
- Information Security Analyst;
- Security Analyst;
- Ethical Hacker.

ჩამოთვლილი სპეციალობების საშუალო წლიური ანაზღაურება დაახლოებით 83,968 აშშ დოლარს შეადგენს. ალბათ ყველაზე უფრო გასათვალისწინებელი ფაქტი არის ის, რომ მოცემული სპეციალობების ხალხის დასაქმება სირთულეს არ წარმოადგენს და საერთაშორისო და ადგილობრივ ბაზარზე ძნელად თუ მოიძებნება მოცემული სპეციალობების კარგი და კვალიფიციური კადრები. ამიტომ, შეიძლება ითქვას, რომ კიბერუსაფრთხოების მიმართულებით მაღალი დონის განათლების მიღებაში ფინანსური საშუალებების „დაბანდება“ საკმაოდ წარმატებულ ინვესტირებას უნდა წარმოადგენდეს.

განვითარებად ქვეყნებში კიბერუსაფრთხოების მიმართულებით განათლების განვითარების პროცესი არათანმიმდევრულად და რთულად მიმდინარეობს, ხოლო ხშირ შემთხვევაში ეს პროცესი საერთოდ არ არსებობს, ან თუ არსებობს საერთოდ არის მოწყვეტილი დარგის განვითარებისა და მისი მდგრადობის შენარჩუნებასთან. გამონაკლისს არ წარმოადგენს არც საქართველო. შეიძლება თამამად ითქვას, რომ საქართველოში კიბერუსაფრთხოების მიმართულებით აკადემიურ დონეზე განათლება საერთოდ არ არსებობს, არის მხოლოდ სხვადასხვა უნივერსიტეტებში არსებული ცალკეული მოდულები. ქვეყანაში არ არის საბაკალავრო და სამაგისტრო პროგრამები, როცა საქართველოს კიბერსივრცე, კრიტიკული ინფრასტრუქტურა დგას გლობალურად არსებული სულ უფრო ახალი გამოწვევების წინაშე.

ფაქტიურად, შეიძლება ითქვას, რომ კიბერუსაფრთხოების განვითარებისა და მდგრადობის შენარჩუნებისთვის მის ყველა ცალკეულ მიმართულებაზე, აუცილებელი არის შესაბამისი განათლებული და კვალიფიციური კადრების არსებობა, რაც თავის მხრივ უზრუნველყოფს კრიტიკული ინფრასტრუქტურის დაცულობის გაზრდას როგორც გლობალურ, ისე ეროვნულ დონეზე.

საქართველო და კიბერუსაფრთხოების საერთაშორისო ინდექსები

ზემოთ წარმოდგენილი ორგანიზაციების მიერ ყოველწლიურად ხდება საქართველოს კიბერშესაძლებლობების შეფასება. შეიძლება ითქვას, რომ საქართველოსთვის კიბერუსაფრთხოების სფეროში ყველაზე წარმატებული იყო 2017 წელი, როცა ITU - ს „გლობალური კიბერუსაფრთხოების ინდექსის (GCI)“ მიხედვით, ქვეყანამ გლობალურ რეიტინგში დაიკავა მე - 8 ადგილი, ევროპის რეგიონში ასევე მე - 8 ადგილი, ხოლო დსთ - ს ქვეყნებს შორის პირველი ადგილი. ქვემოთ ცხრილში მოცემულია საქართველოს შეფასებები კვლევითი კომპონენტების მიხედვით -

სამართლებრივი, ტექნიკური, ორგანიზაციული, შესაძლებლობებისა და თანამშრომლობის განვითარება.

ქვეყანა	GCI ქულა	სამართლებრივი	ტექნიკური	ორგანიზაციული	შესაძლებლობების განვითარება	თანამშრომლობა
სინგაპური	0.92	0.95	0.96	0.88	0.97	0.87
შეერთებული შტატები	0.91	1	0.96	0.92	1	0.73
მალაზია	0.89	0.87	0.96	0.77	1	0.87
ომანი	0.87	0.98	0.82	0.85	0.95	0.75
ესტონეთი	0.84	0.99	0.82	0.85	0.94	0.64
მავრიკის რესპუბლიკა	0.82	0.85	0.96	0.74	0.91	0.70
ავსტრალია	0.82	0.94	0.96	0.86	0.94	0.44
საქართველო	0.81	0.91	0.77	0.82	0.90	0.70
საფრანგეთი	0.81	0.94	0.96	0.60	1	0.61
კანადა	0.81	0.94	0.93	0.71	0.82	0.70

წყარო: კიბერუსაფრთხოების გლობალური ინდექსი *GCI 2017*

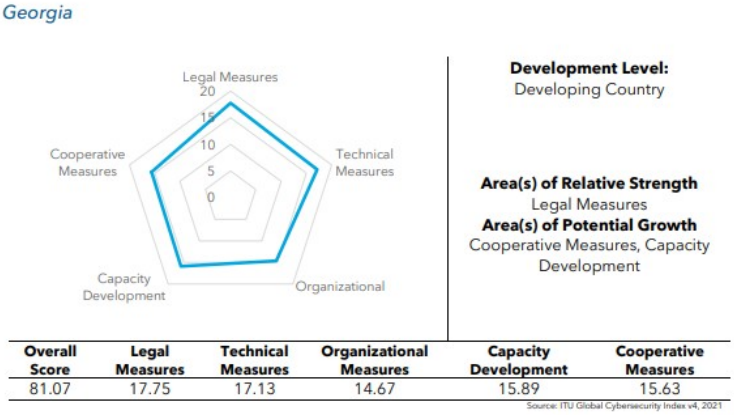
იმავე წელს eGA - ს მიერ გამოქვეყნებული კვლევის შედეგების მიხედვით საქართველომ ევროპის რეგიონში დაიკავა მეორე ადგილი, რაც ქვეყნისთვის საკმაოდ დიდი მიღწევა იყო (იხ. ქვემოთ მოყვანილი ცხრილი).

ქვეყანა	ქულა	რეიტინგი
ჩეხეთის რესპუბლიკა	72.73	1
საქართველო	65.66	2
ლიეტვუა	65.15	3

ბელორუსია	59.09	4
უკრაინა	56.06	5
მოლდოვა	42.42	6
ლატვია	41.92	7

წყარო: კიბერუსაფრთხოების ეროვნული ინდექსი *NCSI 2017*

აღსანიშნავია, რომ 2019 წელს ITU - მ გამოაქვეყნა კიბერ უსაფრთხოებისგანახლებული კვლევა, რომლის მიხედვითაც ადგილობრივი ექსპერტები, 153კითხვის ნაცვლად, 50 ასპექტის მიხედვით აფასებდნენ ქვეყანაში არსებულ კიბერუსაფრთხოების გარემოს. აღნიშნული დოკუმენტის მიხედვით, 0.85 ქულით,საქართველომ ევროპაში მეცხრე, ხოლო მსოფლიოში 18 - ადგილი დაიკავა. თავის მხრივ, 2018 წელს eGA - ს მიერ ჩატარებული კვლევის შედეგების მიხედვით თანახმად, საქართველომ 64.9 ქულით, სიაში 19 - ე ადგილი დაიკავა. 2020 წლის GCI - ის მიხედვით, საქართველოს კიბერშესაძლებლობები კიდევ უფრო გაუარესდა, კერძოდ, ქვეყანამ 81.06 ქულით გლობალურ რეიტინგში დაიკავა 55 - ე ადგილი, ხოლო 81.07 ქულით ევროპის რეგიონის რეიტინგში 30 - ე ადგილი. ქვემოთ ნახატზე მოცემულია GCI – ის მიერ შეფასებული საქართველოს კიბერშესაძლებლობა 2020 წლისთვის თავისი ყველა ხუთი მიმართულებითა და შემადგენელი კომპონენტებით.



წყარო: კიბერუსაფრთხოების გლობალური ინდექსი *GCI 2020*

მოცემულ ნახატზე ნათლად ჩანს, რომ საქართველოს კიბერუსაფრთხოების კომპონენტები და ქულები ხუთივე მიმართულებით შემცირებულია, კერძოდ:

1. იურიდიულ - სამართლებრივი - 17.75
2. ტექნიკური შესაძლებლობები - 17.13
3. ორგანიზაციული განვითარება - 14.67
4. შესაძლებლობების განვითარება - 15.89
5. თანამშრომლობის განვითარება - 15.63

ფაქტიურად, საქართველოს კიბერუსაფრთხოება 2017 წლიდან ნაცვლად გაუმჯობესებისა, წავიდა გაუარესებისკენ, რისი მიზეზიც არის ამჟამად დარგის ყველა მიმართულებით არსებული სტაგნაციური მდგომარეობა. ქვეყნის წარმატების

მიზეზად, რამაც 2017 წელს ასახვა ჰპოვა საერთაშორისო კიბერუსაფრთხოების ინდექსებში, შეიძლება მოვიყვანოთ ის ფაქტები, რომ საქართველომ მოკლე დროში შეძლო:

1. იურიდიულ - სამართლებრივი და ნორმატიული ბაზის მოწყობა, კერძოდ:
   - მიიღეს „კანონი ინფორმაციული უსაფრთხოების შესახებ“ (2012);
   - დაიწერა კიბერუსაფრთხოების ორი სტრატეგია და სამოქმედო გეგმა (2013 – 2015 და 2017 - 2018);
   - განისაზღვრა კრიტიკული ინფრასტრუქტურის სუბიექტები (2013);
   - მიიღეს კანონი „პერსონალური მონაცემების შესახებ“ (2013);
2. ქვეყანა შეუერთდა ბუდაპეშტის კიბერდანაშაულის კონვენციას (2012);
3. შსს - შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო (2012);
4. შეიქმნა პერსონალური მონაცემების დაცვის ინსპექტორის ოფისი (2013);
5. თავდაცვის სფერო საერთოდ გამოეყო სამოქალაქო სფეროს და თავდაცვის სამინისტროში შეიქმნა „სსიპ - კიბერუსაფრთხოების ბიურო“ (2014), რაც იყო დიდი წარმატება და აუცილებელი მოვლენა ქვეყნის კიბერუსაფრთხოების მიმართულებით.

დასკვნა

ბოლოში დასკვნის სახით შეიძლება ითქვას, რომ სახელმწიფოებში და ზოგადად გლობალურად კიბერუსაფრთხოების მდგომარეობის შეფასება ხდება ისეთი ორგანიზაციების მიერ, რომელთა სანდოობა და რეპუტაცია არის მაღალი. ჩვენს შემთხვევაში საუბარია მაღალი დონის ისეთ სანდო და რეპუტაციულ ორგანიზაციებზე, როგორებიცაა:

1) გაეროსქვემდებარესტრუქტურულიინსტიტუტის „საერთაშორისოსატელეკომუნიკაციოკავშირი/International Telecommunication Union (ITU)“, რომელიცყოველწლიურადატარებსგლობალურკვლევასკიბერუსაფრთხოებისგანვითარებისშესახებ, რაცშემდეგგაისახებანაშრომში „კიბერუსაფრთხოებისგლობალურიინდექსი/Global Cybersecurity Index (GCI)“. ITU თავისკვლევასაწარმოებსუკვეთერთმეტიწელიადაყოველიწლისივნისის თვეშიაქვეყნებსწინაწლისკვლევისშედეგებს;
2) ესტონურიორგანიზაცია „ელექტრონულიმმართველობისაკადემია/e – Governance Academy (eGA)“ ITU - სმსგავსად eGA თავისკვლევას „ეროვნულიკიბერუსაფრთხოებისინდექსი/National Cybersecurity Index (NCSI)“ აწარმოებსკიბერუსაფრთხოებისმიმართულებით, თუმცაარაგლობალურადარამედეროვნულდონეზეევროპისრეგიონისქვეყნებისმიხედვითდაკვლევისშედეგებსაქვეყნებსყოველიწლისსექტემბრის თვეში, ITU – „გლობალურიკიბერუსაფრთხოებისინდექსის“ გამოქვეყნებისშემდეგ.

უნდა ითქვას, რომ ორივე ინდექსი ასახავს კიბერუსაფრთხოების მიმართულებით არსებულ მაქსიმალურად რეალურ სურათს, რომლის შეფასება მოიცავს დარგის ყველა მიმართულებასა და მის შემადგენელ კომპონენტებს, კერძოდ:

1. **საკანონმდებლოჩარჩოსმიმართულება** - კიბერკრიმინალისრეგულაცია; კიბერუსაფრთხოებისრეგულაცია; ტრენინგებიკიბერუსაფრთხოებისსფეროში;

2. **ტექნიკურიმიმართულება** - ეროვნული, სამთავრობოდასექტორული CERTები;
   სტანდარტებიდასერტიფიკატებიორგანიზაციებისადაპროფესიონალების თვის; ბავშვთაონლაინდაცულობა;
3. **ორგანიზაციულიმიმართულება** - სტრატეგია; შესაბამისისააგენტოები; კიბერუსაფრთხოებისშეფასება;
4. **შესაძლებლობებისგანვითარება** - სტანდარტიზაციისორგანოები; საუკეთესოპრაქტიკისკვლევისდაგანვითარებისპროგრამები;
   საზოგადოებისცნობიერებისამაღლებისკამპანიები;
   პროფესიონალთატრენინგმოდულები;
   ეროვნულისაგანმანათლებლოპროგრამებიდააკადემიურისილაბუსები;
   წამახალისებელიმექანიზმები;
   კიბერუსაფრთხოებისადგილობრივიინდუსტრია;
5. **თანამშრომლობისმიმართულება** - შიდასახელმწიფოებრივითანამშრომლობა;
   მრავალმხრივიშეთანხმებები;
   საერთაშორისოხელშეკრულებებშიმონაწილეობა; კერძო-საჯაროპარტნიორობა; უწყებათაშორისითანამშრომლობა.

წინამდებარე ნაშრომში ცალკე არის გამოყოფილი განათლების მნიშვნელობა კიბერუსაფრთხოების სფეროში, რადგან ეს არის ის შემადგენელი კომპონენტი, რომლის მიხედვითაც ახდენს შეფასებას ორივე გლობალური და ეროვნული ინდექსი. ამის მთავარი მიზეზი არის ის გარემოება, რომ კიბერუასფრთხოების დარგი მოითხოვს მაღალკვალიფიციურ აკადემიური დონის კადრებს და ამიტომაც ხდება მოცემული მიმართულებით საგანმანათლებლო პროგრამების განვითარება საბაკალავრო და სამაგისტრო დონეებზე. გარდა ამისა, ხდება აკადემიური კვლევების კომპონენტების განვითარება. ამ კუთხით სავალალო მდგომარეობაა საქართველოში, სადაც არ არსებობს არც ბაკალავრიატი და არც მაგისტრატურა, არ ტარდება კვლევები და ფაქტიურად, მოცემული მიმართულებით დარღვეული არის კავშირი საჯარო სექტორსა და აკადემიურ წრეებს შორის, როცა ამ უკანასკნელისთვის შეიძლება თავად სახლემწიფო ყოფილიყო დამკვეთი მისთვის აუცილებელი კადრების მომზადებასა და გადამზადებაში. არ შეიძლება არ აღინიშნოს ასევე თანამშრომლობის აუცილებლობა სამეცნიერო კვლევების ჩატარების მიმართულებითაც, რაც დღეს ფაქტიურად საერთოდ მოშლილია და არ ტარდება აკადემიური დონის სამეცნიერო კვლევითი საქმიანობა.

ბიბლიოგრაფია

1. The Global Risks Report 2021, 16th Edition of the World Economic Forum, In partnership with Marsh McLennan, SK Group and Zurich Insurance Group, 19 January, 2021 https://www.weforum.org/reports/the-global-risks-report-2021;
2. ვლადიმერ ნაფეტვარიძე, ელექტრონული მმართველობის დანერგვა საქართველოში: პრობლემები და პერსპექტივები, 2020;
3. ვლადიმერ სვანაძე „განათლების მნიშვნელობა კიბერუსაფრთხოების განვითარებაში“, 2021;
4. e – Governance Academy https://ega.ee/projects/?programme=cyber-security;
5. ვლადიმერ სვანაძე, ანდრია გოცირიძე "კიბერ თავდაცვა: კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები (ნაშრომების და სტატიების კრებული)", 2016;

6. GUIDE TO GOOD GOVERNANCE IN CYBERSECURITY, DCAF Business and Security Division, Directorate for Security Cooperation and Defence (DCSD) of the French Ministry of Europe and Foreign Affairs, 19 January, 2021 https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021_0.pdf;
7. https://www.cybrary.it/.
8. M. Iavich, S. Gnatyuk, G. Iashvili, A. Fesenko. Cyber security European standards in business. Scientific and Practical Cyber Security Journal (SPCSJ), 3(2):36-39, 2019