Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 39-44 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

განათლების მნიშვნელობა კიბერუსაფრთხოების განვითარებაში

THE IMPORTANCE OF EDUCATION IN THE DEVELOPMENT OF CYBER SECURITY

ვლადიმერ სვანაძე საქართველოს ტექნიკური უნივერსიტეტის დოქტორანტი, საქართველოს ტექნოლოგიური ინოვაციების აკადემიის დირექტორი

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

რეზიუმე: ქვეყნის კრიტიკულ ინფრასტრუქტურაზე განხორციელებული წარმატებული კიბერშეტევების აღკვეთა დამოკიდებულია არსებულ კვალიფიციურ კადრებზე, და შესაბამისად განათლების სისტემაზე, რომელსაც შეუძლია შექმნას მსგავსი კვალიფიციური ადამიანური რესურსი. აქვე შეიძლება აღინიშნოს, რომ შესაძლებელია მოხდეს უცხოელი სპეციალისტების მოზიდვა, ან ბევრი კიბერთავდაცვითი ღონისძიებები გადაეცეს კერძო სექტორს, ანუ გატანილ იქნეს ე. წ. „აუთსორსინგად“. თუმცა ორივე ეს ფაქტორი წარმოშობს სხვა პრობლემებს, რაც უკავშირდება როგორც დიდ ფინანსურ საშუალებებს, ისე ნდობის საკითხს დაკავშირებულს კრიტიკული ინფრასტრუქტურის სუბიექტების კიბერთავდაცვით უზრუნველყოფაზე უცხო კომპანიებისთვის გადაცემასთან, რაც ეროვნული უსაფრთხოების თვალსაზრისით ყოვლად დაუშვებელია. ბევრი ექსპერტი ამახვილებს ყურადღებას მოცემულ ფაქტორზე და იძლევიან სტრატეგიულ რეკომენდაციებს კიბერუსაფრთხოების სფეროში ეროვნული საკადრო რესურსის აღზრდისა და განვითარების შესახებ, რაც ნებისმიერი ქვეყნისთვის ასე აუცილებელი და მნიშვნელოვანი ფაქტორია. ნაშრომში ჩატარებული კვლევა აჩვენებს 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.

საკვანძო სიტყვები: *კიბერშეტევა, კიბერთავდაცვა, კიბერუსაფრთოება, განვითარება*

ABSTRACT: The prevention of successful cyber-attacks on the critical infrastructure of the country depends on the available qualified personnel, and consequently on the education system, which can create a similarly qualified human resource. It can also be mentioned that it is possible to attract foreign specialists, or to transfer many cyber security measures to the private sector. However, both of these factors give rise to other problems related to both large financial resources and the issue of trust in the transfer of critical infrastructure entities cyber security to foreign companies, which is totally unacceptable from the point of view of national security. Many experts focus on this factor and make strategic recommendations on the development of national human resources in the field of cyber security, which is very necessary and important factor for any country.

The research conducted in the paper shows that in order to to develop and maintain cybersecurity in all its individual areas, it is necessary to have adequately educated and qualified personnel, which in turn provides increased critical infrastructure protection both globally and nationally.

KEYWORDS: *cyber-attacks, cyber security, cyber safety,development*

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 [1, 2].

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” [3].

ზოგადად ქვეყნის კრიტიკულ ინფრასტრუქტურაზე განხორციელებული წარმატებული კიბერშეტევების აღკვეთა დამოკიდებულია არსებულ კვალიფიციურ კადრებზე, და შესაბამისად განათლების სისტემაზე, რომელსაც შეუძლია შექმნას მსგავსი კვალიფიციური ადამიანური რესურსი. აქვე შეიძლება აღინიშნოს, რომ შესაძლებელია მოხდეს უცხოელი სპეციალისტების მოზიდვა, ან ბევრი კიბერთავდაცვითი ღონისძიებები გადაეცეს კერძო სექტორს, ანუ გატანილ იქნეს ე. წ. „აუთსორსინგად“. თუმცა ორივე ეს ფაქტორი წარმოშობს სხვა პრობლემებს, რაც უკავშირდება როგორც დიდ ფინანსურ საშუალებებს, ისე ნდობის საკითხს დაკავშირებულს კრიტიკული ინფრასტრუქტურის სუბიექტების კიბერთავდაცვით უზრუნველყოფაზე უცხო კომპანიებისთვის გადაცემასთან, რაც ეროვნული უსაფრთხოების თვალსაზრისით ყოვლად დაუშვებელია. ბევრი ექსპერტი ამახვილებს ყურადღებას მოცემულ ფაქტორზე და იძლევიან სტრატეგიულ რეკომენდაციებს კიბერუსაფრთხოების სფეროში ეროვნული საკადრო რესურსის აღზრდისა და განვითარების შესახებ, რაც ნებისმიერი ქვეყნისთვის ასე აუცილებელი და მნიშვნელოვანი ფაქტორია.

კიბერუსაფრთხოების სფეროში კვალიფიციური ადამიანური რესურსის ყოლა არის საკმაოდ დეფიციტური არა მარტო განვითარებადი, არამედ განვითარებული ქვეყნებისთვისაც. მოცემული პროფესიის ადამიანებზე მოთხოვნა გაიზარდა განსაკუთრებით მას შემდეგ, რაც ინტერნეტისა და ინტერნეტ ტექნოლოგიების სწრაფმა განვითარებამ და გლობალურად არსებულმა ვითარებამ, განსაკუთრებით კი პანდემიამ, დააჩქარა ციფრული ტრანსფორმაციის დანერგვაზე მოთხოვნილების გაზრდა. ციფრული ტრანსფორმაციის დანერგვის პროცესში იქნება ეს კერძო თუ საჯარო სექტორში, აუცილებელია მოხდეს ბალანსის შენარჩუნება ტექნოლოგიურ ინოვაციებსა და კიბერუსაფრთხოებას შორის, რაც

კომპლექსური პროცესია და მოითხოვს ორგანიზაციის ყველა სტრუქტურული ერთეულის ჩართულობას. ეს კი თავის მხრივ ხელს უწყობს ციფრული ტრანსფორმაციის ფარგლებში კიბერუსაფრთხოების სტრატეგიისა და პოლიტიკის სწორი მიმართულებით შემუშავებას, პროცესის სწორ დაგეგმვას. ყოველივე ეს მოითხოვს კიბერუსაფრთხოების მიმართულებით კვალიფიციურ და გამოცდილ ადამიანურ რესურსს, რაც თავის მხრივ პირდაპირ კავშირშია განათლების სისტემასთან.

კიბერუსაფრთხოების შესახებ განათლების ზრდის ხელშეწყობა და ცნობიერების გაზრდა ქვეყნებისთვის იმდენად პრიორიტეტულ და მნიშვნელოვან მიმართულებას წარმოადგენს, რომ ის შეყვანილი არის თითოეული ქვეყნის კიბერუსაფრთხოების ეროვნულ სტრატეგიებში [4]. ამ მხრივ არც საქართველოს „კიბერუსაფრთხოების 2017 – 2018 წლების ეროვნული სტრატეგია და სამოქმედო გეგმა“ [5] 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 განავითარონ 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 [6, 7]:

- 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.

საქართველოს კიბერსივრცეზე, დაწყებული 2008 წლის „აგვისტოს ომის“ დროიდან მოყოლებული დღემდე, განხორციელდა არა ერთი სერიოზული კიბერთავდასხმა, რომლის დროსაც დარღვეული იყო კიბერსივრცის მდგრადობა. თითქმის ყველა კიბერთავდასხმის თავიდან აღკვეთის, ან საგამოძიებო პროცესში ჩართული იყვნენ ქვეყნის სტრატეგიული პარტნიორები და მათი დახმარებით ხდებოდა ქვეყნის კრიტიკული ინფრასტრუქტურის ერთიანობის შენარჩუნება. ქვეყნის წინაშე მდგარი საფრთხეების, კვალიფიციური კადრების აშკარა ნაკლებობის ფონზე და ასევე მიუხედავად, ორივე სტრატეგიაში განათლების განვითარების მიმართულების მნიშვნელობის აღნიშვნისა, ქვეყანაში მაინც ვერ მოხერხდა კიბერუსაფრთხოების საგანმანათლებლო აკადემიური პროგრამების დანერგვა და განვითარება. ეს პროცესი დაკავშირებულია რიგ საკითხებთან. კერძოდ, ქვეყნის წამყვანი უნივერსიტეტები არის კერძო სექტორის წარმომადგენლები, რომლებისთვისაც ყოველი ახალი პროგრამის დანერგვა დაკავშირებულია გარკვეულ ფინანსურ დანახარჯებთან და,

რომლებიც ყველა ამ პროცესს უყურებს მოგების მიღების გადასახედიდან, ანუ ორიენტირებულნი არიან მოგებაზე და ბიზნესის განვითარებაზე, და ეს ბუნებრივიც არის. ეს კი იძლევა იმის ვარაუდს, რომ კერძო უმაღლეს სასწავლებლებს ამ ეტაპზე არ უღირთ კიბერუსაფრთხოების მიმართულებით საბაკალავრო და სამაგისტრო პროგრამების დანერგვა, თუ მათ არ დაინახეს იქიდან წამოსული მოგება. მეორე მხარეა, სახელმწიფო, რომლის ინტერესებშიც შედის იყოლიოს მაღალი კვალიფიკაციის კადრები, რათა დააკომპლექტოს ის საჯარო სამსახურები, რომლებიც პასუხისმგებელნი არიან ქვეყნის კრიტიკული ინფრასტრუქტურის დაცვაზე და ასევე დააკომპლექტოს კრიტიკული ინფრასტრუქტურის სუბიექტები, რასაც ავალდებულებს კანონი „ინფორმაციული უსაფრთხოების შესახებ“.

აღსანიშნავია ის გარემოებაც, რომ კანონში „ინფორმაციული უსაფრთხოების შესახებ“ შედის ცვლილებები, რომლის მიხედვითაც არსებული კრიტიკული ინფრასტრუქტურის სუბიექტების ნუსხას ემატება ასევე ორი კატეგორია კერძო სექტორიდან - სატელეკომუნიკაციო კომპანიები და საბანკო სექტორი, რომლებსაც ექნებათ ასევე ვალდებულება თავისთან იყოლიონ როგორც ინფორმაციული უსაფრთხოების მენეჯერები, ისე კიბერუსაფრთხოების სპეციალისტები [8, 9]. გარდა ამისა, ყოველივეს ემატება ის გარემოებაც, რომ მოცემულ კანონში შეტანილი ცვლილებებით გარკვეული ვალდებულების ქვეშ იქნებიან ასევე კერძო სექტორის სხვა ინდუსტრიული სეგმენტებიც. ფაქტიურად, შეიძლება ითქვას, რომ ქვეყანაში სულ უფრო იზრდება მოთხოვნილება კიბერუსაფრთხოების და მათ შორის ასევე, ინფორმაციული უსაფრთხოების მაღალი კვალიფიკაციის კადრების მიმართ. თუმცა სახელმწიფოს მხრიდან ამ მიმართულებით სამწუხაროდ არაფერი არ კეთდება, ვერ მოხერხდა ვერც ერთ სახელმწიფო უმაღლეს სასწავლებელში შესაბამისი პროგრამების ჩამოყალიბება და განვითარება. სტუდენტები და კურსდამთავრებულები თავად ცდილობენ აიმაღლონ კვალიფიკაცია სხვადასხვა სერტიფიცირებული კურსების გავლით როგორც საერთაშორისო, ისე ლოკალურ დონეზე. თუმცა აქაც გარკვეულ პრობლემებს აწყდებიან, რადგან საერთაშორისო სერტიფიცირებული კურსები, რომლებიც ფაქტიურად სპეციალობას იძლევა, არის საკმაოდ ძვირადღირებული, ხოლო ლოკალურ დონეზე არსებული კურსები არ იძლევა იმ დონის კვალიფიკაციას, რომ შესაძლებელი იყოს კარგად დასაქმება. სამწუხაროდ, არც სახელმწიფო არ სთავაზობს რაიმე სახის კვალიფიკაციის ასამაღლებელ კურსებს.

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.

მსგავსი თანამშრომლობა იქნებოდა ე. წ. „სტეიქჰოლდერიზმის“ კარგი მაგალითი, რაც ასე აპრობირებულია დასავლეთში. ეს არის აუცილებელი როგორც დარგის აკადემიურ დონეზე განვითარებისთვის, ისე ზოგადად, ქვეყნის კრიტიკული ინფრასტრუქტურის დაცულობის მაქსიმალურად გაზრდისთვის.

დასკვნის სახით 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.

გამოყენებული ლიტერატურა

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;
2. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019
3. 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;
4. Cybersecurity education in a developing nation: the Ecuadorian environment, Frankie E. Catota1,2,*, M. Granger Morgan1 and Douglas C. Sicker, Journal of Cybersecurity, 2019, 1–19
5. საქართველოს კიბერუსაფრთხოების 2017 – 2018 წლების სტრატეგია და სამოქმედო გეგმა, საქართველოს მთავრობა, 13 იანვარი, 2017;
6. Cybercrime in Georgia: Current Challenges and Possible Developments, Nata Goderdzishvili, Shalva Khutsishvili, PMCG Research Center, 2021;
7. კანონი „ინფორმაციული უსაფრთხოების შესახებ“, საქართველოს საკანონმდებლო მაცნე, 2012;
8. კიბერ თავდაცვა. კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები (ნაშრომების და სტატიების კრებული), ვლადიმერ სვანაძე, ანდრია გოცირიძე, 2015.
9. Sergiy Gnatyuk , Maksim Iavich , Giorgi Iashvili , Andriy Fesenko ENSURING EUROPEAN CIVIL AVIATION CYBERSECURITY, Scientific and practical cyber security journal, 2019