Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 52 – 59 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

კიბერუსაფრთხოება და აკადემიური სექტორი

ვლადიმერ სვანაძე[1]

[1] საჯარო მმართველობის დოქტორი, ბიზნესისა და ტექნოლოგიების უნივერსიტეტის აფილირებული პროფესორი

რეზუმე: სულ უფრო მზარდია კიბერთავდასხმების სტატისტიკური მაჩვენებელი და ჰაკერების სულ უფრო დიდ ინტერესს წარმოადგენს აკადემიური სექტორი, სხვადასხვა სახის სამეცნიერო - კვლევითი ცენტრები, თუ ლაბორატორიები. აკადემიურ სექტორზე კიბერთავდასხმების მთავარ მიზანს წარმოადგენს სტუდენტებისა და თანამშრომლების ისეთი პერსონალური ინფორმაცია, როგორიცაა მათი მისამართები, ტელეფონის ნომრები, სოციალური უსაფრთხოების ნომრები, საბანკო ანგარიშები და ფინანსური დოკუმენტები. აკადემიურ სექტორში არის საკმაოდ დიდ მოცულობის მონაცემთა ბაზები, უზარმაზარი საჯარო ინფორმაცია, სადაც შედის არა მარტო პერსონალური მონაცემები, რაც შეიძლება ითქვას უფრო მეორეხარისხოვანია, არამედ იქ არის ინფორმაცია სხვადასხვა სახის კვლევების შესახებ, ამ კვლევების შედეგების შესახებ, კონკრეტული კვლევების პროცესისა და ტესტირების შესახებ. ამ ტიპის ინფორმაცია სასარგებლოა სხვადასხვა ქვეყნის მთავრობებისთვის, რომლებიც თავიანთი სადაზვერვო სამსახურების საშუალებით ხშირად მიმართავან კიბერჯაშუშობას, მათთვის საინტერესო ინფორმაციის მოპოვების მიზნით, რაც შეიძლება ეხებოდეს სხვადასხვა სახის ტექნოლოგიურ გადაწყვეტილებებს, მიღწევებსა თუ გამოგონებებს. აკადემიური სექტორი და მასში გაერთიანებული სამეცნიერო - კვლევითი ცენტრები და ლაბორატორიები არიან კიბერშეტევების სამიზნეები, რადგან იქ არსებული უზარმაზარი მოცულობის მონაცემები არის დაუცველი და ღირებული.

საკვანძო სიტყვები: კიბერუსაფრთხოება, კრიტიკული ინფრასტრუქტურა, კვლევითი ცენტრები და ლაბორატორიები, SQLI, ფიშინგი.

ABSTRACT: The statistical rate of cyber-attacks is increasing, and the academic sector and various scientific research centers are of increasing interest to hackers. The main objective of cyber-attacks in the academic sector is to obtain the personal information of students and employees, such as addresses, phone numbers, social security numbers, bank accounts, and financial documents. in the academic sector, there are quite large databases, and huge public information, which includes not only personal data, which can be said to be more secondary but also information about various types of research, the process, and testing of their results. This type of information is useful for governments of various countries, who often resort to cyber espionage to obtain interesting information that may relate to various technological solutions, achievements, or inventions. It can be noted that the academic sector, scientific research centers, and laboratories are the targets of cyber-attacks because of the huge amount of data that is vulnerable and valuable.

KEYWORDS: Cybersecurity, Critical Infrastructure, Research Centers and Laboratories, SQLI, Phishing.

1. შესავალი

კიბერუსაფრთხოებამ მიუხედავად თავისი განვითარების მოკლე პერიოდისა, შეიძლება ითქვას დაიკავა ერთ - ერთი 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, ინტერნეტის ერთიანობის შენარჩუნებას, 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, მისი განუყოფელი ნაწილი. ფაქტიურად, რაც უფრო დამოკიდებულია საზოგადოება თანამედროვე ტექნოლოგიებზე, მით უფრო მოწყვლადია კიბერ თავდასხმების მიმართ.

მსოფლიო ეკონომიკური ფორუმის 2022 წლის გლობალური რისკების ანგარიშის მიხედვით, კიბერსივრცეში არსებული რისკები კვლავ შედის 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 სტრატეგიულად მნიშვნელოვანი საზოგადოებრივი გამოწვევა, კიბერუსაფრთხოებაც ვერ მოგვარდება იზოლირებულად “.

სულ უფრო მზარდია კიბერთავდასხმების სტატისტიკური მაჩვენებელი და ჰაკერების სულ უფრო დიდ ინტერესს წარმოადგენს აკადემიური სექტორი, სხვა და სხვა სახის სამეცნიერო - კვლევითი ცენტრები თუ ლაბორატორიები. აკადემიურ სექტორზე კიბერთავდასხმების მთავარ მიზანს წარმოადგენს სტუდენტებისა და თანამშრომლების ისეთი პერსონალური ინფორმაციის მოპოვება, როგორიცაა მისამართები, ტელეფონის ნომრები, სოციალური უსაფრთხოების ნომრები, საბანკო ანგარიშები და ფინანსური დოკუმენტები, სადაზღვევო პოლისები. ხშირ შემთხვევაში, ეს მონაცემები შემდეგ თავსდება „Dark Net“ - ზე, სადაც მისი გამოყენება შესაძლებელია სხავადასხვა სახის კიბერკრიმინალური ქმედებებისთვის.

მაგრამ ისმის კითხვა რატომ გახდა აკადემიური სექტორი კიბერკრიმინალების სამიზნე?

მთავარ მიზეზს ალბათ წარმოადგენს ის ფაქტი, რომ აკადემიურ სექტორში არის საკმაოდ დიდ მოცულობის მონაცემთა ბაზები, უზარმაზარი საჯარო ინფორმაცია, სადაც შედის არა მარტო პერსონალური მონაცემები, რაც შეიძლება ითქვას უფრო მეორეხარისხოვანია, არამედ იქ არის ინფორმაცია სხვადასხვა სახის კვლევების შესახებ, ამ კვლევების შედეგების შესახებ, თითოეული კვლევის პროცესისა და ტესტირების შესახებ.

ამ ტიპის ინფორმაცია სასარგებლოა სხვადასხვა ქვეყნის მთავრობებისთვის, რომლებიც ხშირად მიმართავან კიბერჯაშუშობას, მათთვის საინტერესო ინფორმაციის მოპოვების მიზნით, რაც შეიძლება ეხებოდეს სხვადასხვა სახის ტექნოლოგიურ გადაწყვეტილებებს, მიღწევებსა თუ გამოგონებებს. გარდა ამისა, მსგავსი ინფორმაცია არის ასევე ეკონომიკურად ღირებული.

როცა ვსაუბრობთ კიბერუსაფრთხოებსა და აკადემიური სექტორის ურთიერთდამოკიდებულებაზე, ასევე განათლების როლზე მოცემული დარგის განვითარებაზე, შეიძლება გამოიყოს ორი ძირითადი მიმართულება, კერძოდ;

1. კიბერუსაფრთხოების მნიშვნელობა და როლი სასწავლო - კვლევითი ცენტრებისა და ლაბორატორიების ინფრასტრუქტურის სრულ დაცვაში;

2. განათლების მნიშვნელობა და როლი კიბერუსაფრთხოების განვითარებისთვის.

2. სასწავლო - კვლევითი ცენტრებისა და ლაბორატორიების კიბერუსაფრთხოება

აკადემიური სექტორი და მასში გაერთიანებული სამეცნიერო - კვლევითი ცენტრები და ლაბორატორიები არიან კიბერშეტევების სამიზნეები, რადგან იქ არსებული უზარმაზარი მოცულობის მონაცემები არის ნაკლებად დაცული და ღირებული.

აქვე ისევ გავმეორდები, რომ არა მხოლოდ სტუდენტებისა და თანამშრომლების პერსონალურ მონაცემებზეა საუბარი, არამედ საუბარია კვლევის უახლოეს შედეგებზე, რაც შეიძლება გახდეს საერთაშორისო დონის კიბერჯაშუშობის სამიზნე. სწორედ ამიტომ, აკადემიური სექტორისთვის სასიცოცხლოდ მნიშვნელოვანია უზრუნველყოფილ იქნას კიბერუსაფრთხოებითი ღონისძიებები და დაიცვას თავისი კრიტიკული ინფრასტრუქტურა პოტენციური თავდასხმებისგან.

როგორც ზემოთ იყო აღნიშნული, იმის გამო, რომ სამეცნიერო - კვლევითი ცენტრები და ლაბორატორიები ინახავენ ინფორმაციის ისეთ უზარმაზარ რაოდენობას, რომ ისინი ხშირად ხდებიან ჰაკერების და სხვა კიბერ კრიმინალების სამიზნე, რაზეც მეტყველებს ასევე მოცემული მიმართულებით კიბერშეტევების მზარდი სტატისტიკა. ფაქტია, რომ 2018 – 2022 წლებში სასწავლო - კვლევით დაწესებულებებში მოხდა 2500 - ზე მეტი კიბერინციდენტი, რამაც გამოიწვია მონაცემთა დარღვევა. გარდა ამისა, აღსანიშნავია ის გარემოებაც, რომ ბევრ უნივერსიტეტს და იქ არსებულ სასწავლო - კვლევით ცენტრებსა და ლაბორატორიებს აქვთ მოძველებული ან ცუდად აშენებული კიბერუსაფრთხოებისა და ინფორმაციული ტექნოლოგიების სისტემები, რაც კიდევ უფრო დაუცველს და მოწყვლადს ხდის მათ ინფრასტრუქტურას [1].

აქვე მოყვანილია კიბერსივრციდან მომდინარე ის ხუთი კიბერსაფრთხე, რასაც ხშირად აწყდებიან სასწავლო - კვლევითი ცენტრები და ლაბორატორიები, კერძოდ:

1. **ფიშინგი (Phishing)**[1] - ეს არის ყველაზე უფრო გავრცელებული პრობლემა მოცემული სექტორისთვის, სასწავლო - კვლევითი დაწესებულებებისთვის;
2. **რანსომვეარი (Ransomware)**[2] - ეს არის კიდევ ერთი მთავარი გამოწვევა, რომლის წინაშეც დგას სასწავლო - კვლევითი ცენტრები და ლაბორატორიები დღეს;
3. ბევრი ჰაკერი იყენებს **SQL[3] ინექციებს** კვლევით ინსტიტუტებზე თავდასხმისას;
4. არსებობს მრავალი სხვა ტიპის მონაცემთა დარღვევა, რომელთა წინაშეც ხშირ შემთხვევაში დაუცველია უნივერსიტეტების ინფრასტრუქტურა. მაგალითად, არსებობს მრავალი სხვადასხვა ტიპის **მავნე პროგრამა[4],** რომელსაც ჰაკერები იყენებენ წლების განმავლობაში;

[1] ფიშინგი ინტერნეტთაღლითობის ფორმაა, რომელიც მომხმარებელს მოტყუების გზით აიძულებს, გაამჟღავნოს თავისი სენსიტიური და პერსონალური ინფორმაცია თაღლითების მიერ შექმნილ ყალბ ვებგვერდზე შეყვანის გზით

[2] მავნე პროგრამა რომელსაც „მძევლად“ აყავს ჩვენი სისტემა, მისი გამოწერის და დაყენების შემდეგ, ის ახდენს სისტემის შიფრაციას კრიპტოგრაფიული მეთოდების გამოყენებით. ამის შემდეგ პროგრამა გვთხოვს ფულს თუ გვინდა რომ კრიპტოგრაფიული გასაღები მივიღოთ და გავშიფროთ ჩვენი სისტემა;

[3] Structured Query Language - სტრუქტურიზებული მოთხოვნების ენა, რომლის დახმარებითაც შესაძლებელია მონაცემთა ბაზებთან წვდომა და იქ შენახული ინფორმაციით მანიპულირება. SQL არის ANSI-სტანდარტი (American National Standards Institute);

[4] მავნე პროგრამა, საზიანო პროგრამა (ინგლ. malware) — ყველა იმ პროგრამის სახელწოდება, რომელიც ცდილობს მოიპოვოს უკანონი და არა სანქცირებული გზების საშუალებით წვდომა მსხვერპლის კომპიუტერზე ან პროგრამა, რომელიც მიზანმიმართულად არის შექმნილი იმისათვის, რომ ავნოს

5. **მოძველებული ტექნოლოგია** – ბევრი უნივერსიტეტი, სასწავლო - კვლევითი ცენტრი და ლაბორატორია იყენებს მოძველებულ ტექნოლოგიას, რაც კიბერშეტევების მიმართ მათ კიდევ უფრო დაუცველს და მოწყვლადს ხდის. პროგრამული უზრუნველყოფის თუნდაც ერთი განახლების გამოტოვებამ შეიძლება ორგანიზაცია კიდევ უფრო დაუცველი გახადოს.

როგორც იყო აღნიშნული სხვადასხვა ქვეყნის მთავრობები ცდილობენ კვლევების ჩატარებისა და შედეგების შესახებ ინფორმაციის მოპოვებას და ამ მიზნით, აქტიურად იყენებენ ჰაკერების მომსახურებას, ახორციელებენ კიბერშეტევებს. ეს პროცესი განსაკუთრებით თვალშისაცემი იყო პანდემიის პერიოდში, როცა კვლევითი ცენტრები და ლაბორატორიები აქტიურად მუშაობდნენ კორონის საწინააღმდეგო წამლისა და ვაქცინის შემუშავებაზე.

ამ კუთხით, ძალიან აქტიურობდნენ ჰაკერული ჯგუფები რუსეთის ფედერაციიდან, რომლებმაც განახორციელეს რამოდენიმე კიბერშეტევა დიდი ბრიტანეთის, შეერთებული შტატებისა და კანადის COVID – 19 კვლევით ცენტრებზე. სამივე ქვეყნის ოფიციალური პირები თავიანთ განცხადებაში დეტალურად აღწერენ რუსული ჰაკერული ჯგუფის აქტივობას, სახელწოდებით APT 29, რომელიც ასევე მოიხსენიება სახელწოდებით “the Dukes” ან “Cozy Bear.” გაერთიანებული სამეფოს კიბერუსაფრთხოების ეროვნული ცენტრის (NCSC) მიერ გამოქვეყნებული ინფორმაცია დეტალურად აღწერს რუსული ჰაკერული ჯგუფის საქმიანობას და ცალსახად ასახელებს კონკრეტულ კიბერინციდენტებსა და მცდელობებს შეერთებული შტატების, გაერთიანებული სამეფოსა და კანადის ვაქცინების კვლევისა და განვითარების ორგანიზაციების მიმართ.

პანდემიის პერიოდში, 2020 წლის სექტემბერში მოხდა ჰაკერული თავდასხმა საქართველოს ჯანდაცვის სისტემაზე[5]. საქართველოს შინაგან საქმეთა სამინისტროს ინფორმაციით, საქართველოს ჯანდაცვის, შრომისა და სოციალური დაცვის სამინისტროზე უცხო ქვეყნიდან განხორციელდა კიბერშეტევა. კიბერთავდასხმის მთავარი მიზანი იყო სამინისტროს ცენტრალური აპარატისა და მისი სტრუქტურული ერთეულების, მათ შორის დაავადებათა კონტროლისა და საზოგადოებრივი ჯანმრთელობის ეროვნული ცენტრისა და რიჩარდ ლუგარის კვლევითი ცენტრის დოკუმენტებისა და პანდემიის მართვაზე იქ არსებული მნიშვნელოვანი ინფორმაციის უკანონო გზით მოპოვება და გამოყენება [2].

შსს - ს ცნობით, კიბერთავდასხმის შედეგად მოპოვებული ავთენტური დოკუმენტების ნაწილი ატვირთულია ერთ - ერთ უცხოურ ვებგვერდზე და ხელმისაწვდომია საზოგადოებისთვის. ამასთანავე, ამავე ვებგვერდზე იტვირთება მიზანმიმართულად გაყალბებული დოკუმენტები, რომლებიც საზოგადოების დაშინების, დაბნეულობისა და უნდობლობის გაღვივებას ისახავს მიზნად. მიუხედავად იმისა, რომ შსს არ აკონკრეტებს ქვეყანას, საიდანაც განხორციელდა კიბერშეტევა, პროცესები და დეზინფორმაციული კამპანია, რომელიც წინ უძღოდა მოცემულ კიბერშეტევას, დიდი ალბათობით მიუთითებს რუსულ კვალზე.

როცა ვსაუბრობთ კონკრეტულ ფაქტებზე, რაც უკავშირდება კვლევით ცენტრებზე კიბერთავდასხმებს, აუცილებლად უნდა გავიხსენოთ რუსული ჰაკერული ჯგუფი, რომელიც ცნობილია „Cold River“ - ის სახელით, რომელმაც 2022 წლის ზაფხულის პერიოდში განახორციელა რამოდენიმე კიბერშეტევა აშშ - ს სამ ბირთვულ კვლევით ლაბორატორიაზე.

და მაინც ჩნდება კითხვა თუ სასწავლო - კვლევითი ცენტრები და ლაბორატორიები ჰაკერების დიდი ინტერესის ქვეშ არიან, თანაც სხვადასხვა ქვეყნების მთავრობები არიან დაინტერესებული

მომხმარებლის კომპიუტერს ან მასში არსებულ ინფორმაციას, მოხმარებლისგან მალულად, ასეთ პროგრამებს ხშირად ვირუსებს ეძახიან, ისინი იყოფიან რამდენიმე კლასებად და სახეობებად.

[5] https://ge.usembassy.gov/u-s-embassy-statement-on-september-1-2020-cyberattack-against-georgian-ministry-of-health/

მიმდინარე კვლევებით, ტესტებითა და შედეგებით, მაშინ როგორ შეიძლება დაცული იყოს კვლევითი ცენტრების კრიტიკული ინფრასტრუქტურა? რა შეიძლება ვურჩიოთ მათ?
ყოველივეს გათვალისწინებით, როცა ვსაუბრობთ კვლევითი ცენტრების კრიტიკული ინფრასტრუქტურის დაცვაზე, პირველ რიგში აუცილებელია სამთავრობო დონეზე ჩართულობა, საჯარო, კერძო და აკადემიურ სექტორებს შორის თანამშრომლობის გაძლიერება, რაც მოიცავს კრიტიკული ინფრასტრუქტურის მოწესრიგებას, კიბერუსაფრთხოებითი და ინფორმაციული უსაფრთხოებით გათვალისწინებული ღონისძიებების განხორციელებას, თანამშრომელთა ცნობიერების ამაღლებას, რაც ზოგადად კიბერუსაფრთხოების ერთ - ერთი შემადგენელი ნაწილია, და ასევე სხვა მნიშვნელოვან ღონისძიებებს.

3. განათლების მნიშვნელობა კიბერუსაფრთხოების განვითარებაში

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. „აუთსორსინგულ“ მომსახურებაზე. 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 [3-4].
კიბერუსაფრთხოების სფეროში კვალიფიციური ადამიანური რესურსის ყოლა არის საკმაოდ დეფიციტური არა მარტო განვითარებადი, არამედ განვითარებული ქვეყნებისთვისაც. მოცემული პროფესიის ადამიანებზე მოთხოვნა გაიზარდა განსაკუთრებით მას შემდეგ, რაც ციფრული ტრანსფორმაციის ფარგლებში გაიზარდა მოთხოვნილება კიბერუსაფრთხოების სტრატეგიისა და პოლიტიკის სწორი მიმართულებით შემუშავებასა და პროცესის სწორ დაგეგმვაზე. 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[6]. ამ მხრივ არც საქართველოს „კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგია და სამოქმედო გეგმა“ არის გამონაკლისი, სადაც მოცემული მიმართულება სხვა მიმართულებებთან ერთად მოხსენიებულია როგორც ერთ - ერთი ძირითადი მიმართულება, კერძოდ:

1. კვლევა და ანალიზი;
2. სამართლებრივი ბაზის შემუშავება და სრულყოფა;
3. კიბერუსაფრთხოების სფეროში შესაძლებლობათა განვითარება;

[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

4. **საზოგადოებრივი ცნობიერების ამაღლება და საგანმანათლებლო ბაზის შექმნა;**
5. საერთაშორისო თანამშრომლობა.

უნდა აღინიშნოს, რომ სტრატეგიებში განათლების სფეროს ასახვა ნათლად აჩვენებს ქვეყნების დიდ ინტერსს 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 [5-6].
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 სფეროსთვის აკადემიური განათლების მნიშვნელობაზე. აქვე თუ დავამატებთ იმ ფაქტს, რომ გლობალურად კიბერუსაფრთხოების სპეციალისტთა აშკარა დეფიციტია, ხოლო მათზე მოთხოვნილება სულ უფრო იზრდება, მაშინ შეიძლება ითქვას, რომ უახლოეს მომავალში ეს იქნება ერთ - ერთი მოთხოვნადი სპეციალობა. აგრეთვე, თუ გავითვალისწინებთ ასეთ მზარდ მოთხოვნილებას, თავისუფლად შეიძლება ითქვას, რომ მოცემული მიმართულების სპეციალისტების შრომითი ანაზღაურება არის საკმაოდ მაღალი. კერძოდ, არსებული სტატისტიკის მიხედვით, უსაფრთხოების ოპერაციების ცენტრის[7] დამწყები ანალიტიკოსის წლიური ხელფასი აჭარბებს 80 ათას აშშ დოლარს. ასეთ მაღალანაზღაურებად სპეციალობებად მოიაზრება[8]:

- შეღწევადობის ტესტერი (Penetration Tester);
- ინფორმაციული უსაფრთხოების ანალიტიკოსი (Information Security Analyst);
- უსაფრთხოების ანალიტიკოსი (Security Analyst);
- ეთიკური ჰაკერი (Ethical Hacker).

ალბათ ყველაზე უფრო გასათვალისწინებელი ფაქტი არის ის, რომ მოცემული სპეციალობების ხალხის დასაქმება სირთულეს არ წარმოადგენს როგორც საერთაშორისო, ისე ადგილობრივ ბაზარზე. 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 შენარჩუნებისგან.

[7] Security Operations Center SOC
[8] https://www.cybrary.it/

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, სამ სტრატეგიაში განათლების განვითარების მიმართულების მნიშვნელობის აღნიშვნისა, ქვეყანაში მაინც ვერ მოხერხდა კიბერუსაფრთხოების საგანმანათლებლო აკადემიური პროგრამების უფრო ფართოდ დანერგვა და განვითარება, თუ არ ჩავთვლით კავკასიის უნივერსიტეტის საბაკალავრო და ანდრია პირველწოდებულის სახლობის უნივერსიტეტის სამაგისტრო პროგრამებს [7].

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“ შესული ცვლილებების მიხედვით, არსებული კრიტიკული ინფრასტრუქტურის სუბიექტების ნუსხას დაემატა ასევე ორი კატეგორია კერძო სექტორიდან - სატელეკომუნიკაციო კომპანიები და კერძო სექტორის სხვა ინდუსტრიული მიმართულებები, რომლებსაც კანონის თანახმად, აქვთ ვალდებულება თავისთან იყოლიონ როგორც ინფორმაციული უსაფრთხოების მენეჯერები, ისე კიბერუსაფრთხოების სპეციალისტები.

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 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 და ამავდროულად, ძალაშია გარკვეულ პერიოდზე. ხოლო ლოკალურ დონეზე არსებული კურსები[9] არ იძლევა იმ დონის კვალიფიკაციას, რომ შესაძლებელი იყოს კარგად დასაქმება. სამწუხაროდ, არც სახელმწიფო არ სთავაზობს რაიმე სახის კვალიფიკაციის ასამაღლებელ კურსებს. აქვე უნდა აღინიშნოს დონორი ორგანიზაციების მიერ

[9] ფაქტიურად, შეიძლება ითქვას, რომ სულ ორი ორგანიზაციაა, რომელიც იძლევა შედარებით კარგ განათლებას სხვადასხვა სერტიფიცირებული კურსების შეთავაზებით. კერძოდ, ესენია Scientific Cyber Security Association https://scsa.ge/en/ და IT Academy Step https://ge.itstep.org/

დაფინანსებული კიბერუსაფრთხოების პროგრამა, რომელიც საქართველოს უნივერსიტეტის ინფორმაციული ტექნოლოგიების კოლეჯში ხორციელდება [8-9].

4. დასკვნა

ფაქტიურად, მოცემული მიმართულებით დარღვეული არის კავშირი საჯარო, კერძო სექტორსა და აკადემიურ წრეებს შორის, როცა ამ უკანასკნელისთვის შეიძლება თავად სახელმწიფო 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[10]. ეს არის აუცილებელი როგორც დარგის აკადემიურ დონეზე განვითარებისთვის, ისე ზოგადად, ქვეყნის კრიტიკული ინფრასტრუქტურის დაცულობის მაქსიმალურად გაზრდისთვის.

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. სვანაძე ვ. „კიბერუსაფრთხოების ახალი გამოწვევები და საქართველო“, 2022
2. სვანაძე ვ., გოცირიძე ა., კიბერ თავდაცვა: კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და ახალი გამოწვევები, თბილისი, 2015
3. ნაფეტვარიძე ვ., „ელექტრონული მმართველობის დანერგვა საქართველოში: პრობლემები და პერსპექტივები“, 2020
4. ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, „კიბერშეტევა ჯანდაცვის სამინისტროზე და რუსული კვალი“, 2020
5. Schwartz N., “Georgia health system's operations disrupted by cyberattack”, 2023
6. 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
7. 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
8. Cybersecurity education in a developing nation: the Ecuadorian environment, Frankie E. Catota1,2,*, M. Granger Morgan1 and Douglas C. Sicker, Journal of Cybersecurity, 2019.

[10] „მულტი სტეიქჰოლდერიზმი“, ანუ ყველა დაინტერესებული მხარის (საჯარო და კერძო სექტორები, სამოქალაქო საზოგადოება და აკადემიური წრეები) ჩართულობა და ერთობლივი თანამშრომლობა კონკრეტული დარგის განვითარებისთვის.