ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი
სოციალურ და პოლიტიკურ მეცნიერებათა ფაკულტეტი

ხატია ჭილავა

კიბერუსაფრთხოების როლი საქართველოს ეროვნული უსაფრთხოების პოლიტიკაში:
2008-2017 წლების ანალიზი

პოლიტიკის მეცნიერების მიმართულება

სამაგისტრო ნაშრომი შესრულებულია პოლიტიკის მეცნიერების მაგისტრის ხარისხის მოსაპოვებლად

კურსის ხელმძღვანელი : პროფესორი ალექსანდრე კუხიანიძე

თბილისი
2018

კიბერუსაფრთხოების როლი საქართველოს ეროვნული უსაფრთხოების პოლიტიკაში: 2008-2017 წლების ანალიზი

ანოტაცია

საჰაერო, საზღვაო და სახმელეთო სივრცის შემდეგ კიბერსივრცე დაპირისპირების ახალ ფრონტად გადაიქცა. იგი სხვადასხვა სახელმწიფოების მიერ ხშირად გამოიყენება პოლიტიკური, სამხედრო და გეოპოლიტიკური მიზნების მისაღწევად. 2008 წლის აგვისტოს ომის მოვლენებმა, რომლის დროსაც რუსეთის ფედერაციამ საქართველოს წინააღმდეგ კიბერშეტევები განახორციელა, საქართველოს სახელმწიფო ხელისუფლებამ ნათლად დაინახა, ძლიერი კიბერპოლიტიკის არსებობის საჭიროება. ნაშრომის კვლევის საგანს წარმოადგენს კიბერუსაფრთხოების როლის შესწავლა საქართველოს ეროვნული უსაფრთხოების პოლიტიკაში. კვლევა აქტუალურია რადგან საქართველოში კვლევები, რომლებიც შეეხება კიბერუსაფრთხოებას საკმაოდ მცირეა,თემა არა პოპულარული და არა აქტუალურია სამეცნიერო წრეებში, ეს ყველაფერი კი მაშინ, როდესაც ასეთ კვლევებს უდიდესი სტრატეგიული მნიშვნელობა გააჩნია ჩვენი ქვეყნისა და მისი ეროვნული უსაფრთხოებისათვის. კვლევის მიზანს წარმოადგენს დადგინდეს საქართველოს სახელმწიფოს კიბერუსაფრთხოების დონესა და ეროვნული უსაფრთხოების დონეს შორის მიზეზ-შედეგობრივი კავშირი, თუ რა უშუალო ზეგავლენას ახდენს საქართველოს სახელმწიფოს მიერ ქვეყნის კიბერუსაფრთხოების კუთხით გაატრებული რეფორმები, ქვეყნის ეროვნულ უსაფრთხოებაზე. კვლევის ფარგლებში გაანალიზებულ იქნა სხვადასხვა სახის საერთაშორისო და სახელმწიფო დოკუმენტები, ქვეყნის საკანონმდებლო ბაზა. კვლევის დროს გამოყენებულ იქნა, როგორც თვისებრივი ,ასევე რაოდენობრივი კვლევის მეთოდი. კვლევის შედეგად გამოკვეთილ იქნა საქართველოს სახელმწიფოს მიერ გატარებული რეფორმების რაობა, ეფექტურობა და ის წინსვლა, რომელიც ქვეყანამ კიბერუსაფრთხოების პოლიტიკის დახვეწის კუთხით 2008 წლიდან - 2017 წლამდე განახორციელა. ამასთანავე, გამოკვეთილ იქნა ის ხარვეზები და სუსტი წერტილები, რომელთა აღმოფხვრაზეც სახელმწიფომ მომავალ წლებში აუცილებლად უნდა იზრუნოს.

Role of Cyber Security in Georgian National Security Policy: Analysis as at 2008-2017

Annotation

After the air, sea and land space, cyberspace became a new front of opposing. It is often used by various states to achieve the political, military and geopolitical goals. Due to the occurrences of the August 2008 war, during which the Russian Federation carried out the cyber attacks against Georgia, Georgian state authorities clearly saw the need for a strong cyber policy. The subject of the paper research is to study the role of cyber security in the national security policy of Georgia. The research is the urgent one as the studies related to cyber security are not very popular and not relevant in the scientific circles, while all these studies are of great strategic importance for our country and its national security.

The purpose of the study is to identify the causal-resultative links between the cyber security level of the state of Georgia and the level of national security, what direct impact is caused by the reforms made in the country concerning to cyber security. . Within the scope of the study, different types of international and state documents, the legislative base of the country were analyzed. During the research as a qualitative and quantitative research method have been applied. As a result of the research, the country's state-run reforms, efficiency and advancement have been shaped, which the country has implemented in terms of improving cyber security policy from 2008 - until 2017. At the same time, the shortcomings and weak points that the state has to take care to be remedied in the next years were emphasized.

სარჩევი

შესავალი

მიუხედავად იმისა, რომ ინტერნეტის განვითარებამ მსოფლიოს უდიდესი პროგრესი მოუტანა, ამასთანავე მან მსოფლიოს ახალი თავსატეხიც გაუჩინა ეს კიბერუსაფრთხოებაა. საჰაერო, საზღვაო და სახმელეთო სივრცის შემდეგ კიბერსივრცე დაპირისპირების ახალ ფრონტად გადაიქცა. იგი ხშირად გამოიყენება პოლიტიკური, სამხედრო და გეოპოლიტიკური მიზნების მისაღწევად. მსოფლიოში აქტიურად მიმდინარეობს გლობალური კიბერ-სივრცის ფორმირება. ქვეყნები აქტიურად მუშაობენ საკუთარი კიბერსივრცის მაქსიმალურად გასაძლიერებლად. ამასთანავე არ იშურებენ ძალებს კიბერ თავდასხმები განახორციელონ მათ მოწინააღმდეგე ქვეყნებზეც. საკუთარი ოფიციალური კიბერარმია ჰყავს ამერიკის შეერთებულ შტატებს, ინგლისს, საფრანგეთს, გერმანიას, ჩინეთს, რუსეთსა და რიგ სხვა ევროპულ ქვეყნებს. ამასთანავე, სხვადასხვა სახის დოქტინების შემუშავებით არიან დაკავებულნი ნატო, გაერთიანებული ერების ორგანიზაცია, ევროკავშირი. მაგალითისათვის აშშ კიბერთავდასხმების აქტებს აიგივებს ტრადიციულ სამხედრო მოქმედებებთან. აგრეთვე, დიდი ადგილი უკავია რუსეთის ეროვნული უსაფრთხოების დოქტრინაში რუსეთის კიბერუსაფრთხოების საკითხს.

გამომდინარე ზემოთ მოყვანილი მაგალითებიდან, ჩვენ ვხედავთ, რომ ნებისმიერი ქვეყნისათვის ძლიერი კიბერსივრცე პოტენციური ომის პირობებში უზრუნველყოფს ქვეყნის გამარჯვებისაკენ წინ გადაგმულ მნიშვნელოვან ნაბიჯს.

2008 წლის რუსეთ-საქართველოს ომმა და რუსეთის მხრიდან განხორციელებულმა კიბერშეტევებმა საქართველოს უჩვენა, რომ ეროვნული უსაფრთხოებისათვის საფრთხეს არა მარტო საჰაერო, საზღვაო და სამხელეთო შეტევა წარმოადგენდა, არამედ კიბერსივრცეც. რუსულმა კიბერშეტევამ, რომელიც 2008 წლის აგვისტოში რუსეთმა საქართველოს წინააღმდეგ აწარმოა საქართველოს ხელისუფლებას ნათლად დაანახა, რომ ქვეყნის კიბერსივრცის უსაფრთხოება მჭიდრო კავშირშია ეროვნულ უსაფრთხოებასთან.

დამოუკიდებლობის 26 წლიანი ისტორიის განმავლობაში საქართველოს სახელმწიფომ სამი ომი გადაიტანა ჩრდილოელ მეზობელთან - რუსეთის

ფედერაციასთან. ყველაზე მნიშვნელოვანი და საინტერესო დეტალი კი გახლავთ ის, რომ 90-იანი წლების ომისაგან განსხვავებით 2008 წლის აგვისტოში საქართველოს წინააღმდეგ რუსეთმა კიბერშეტევები წამოიწყო. სამწუხაროდ, ჩვენი ქვეყნის იმდროინდელი მდგომარეობიდან გამომდინარე კიბერომი ამ ფრონტზე საქართველომ „ უომრად“ წააგო. კიბერთავდასხმის შედეგად საქართველოში: ა): გაითიშა ქართული ვებ-გვერდები და ბ): რუსეთმა გამოიწვია ინფორმაციული ვაკუუმი. როგორც შემდეგ გახდა ცნობილი რუსეთის მიერ კიბერშეტევები საბრძოლო მოქმედებების დაწყებამდე რამდენიმე თვით ადრე იგეგმებოდა.

2008 წლამდე საქართველოს სახელმწიფო არ აქცევდა ჯეროვან ყურადღებას ქვეყნის ეროვნული უსაფრთხოებისათვის უმნიშვნელოვანეს საკითხს: კიბერუსაფრთხოებას. შესაბამისად, ქვეყნის დღის წესრიგში კიბერუსაფრთხოების პოლიტიკას არ ეკავა მნიშვნელოვანი და მოწინავე პოზიცია. 2008 წლის კიბერშეტევებმა კიბერუსაფრთხოებასა და ეროვნულ უსაფრთხოებას შორის მჭიდრო კავშირი გამოკვეთა. გამოიკვეთა , რომ ძლიერი კიბერსივრცის გარეშე სახელმწიფოს ეროვნულ უსაფრთხოებასა და სტაბილურობას დიდი საფრთხე ემუქრება. **კვლევის საგანს** წარმოადგენს: კიბერუსაფრთხოების როლი, საქართველოს ეროვნული უსაფრთხოების პოლიტიკაში.

თემის აქტუალობა : გამომდინარე ზემოთ მოყვანილი ფაქტებიდან და მსოფლიოში მიმდინარე პროცესებიდან, ჩვენ ვხედავთ თუ რაოდენ მნიშვნელოვანი ადგილი და როლი უკავია ქვეყნის ეროვნული უსაფრთხოების პოლიტიკაში კიბერუსაფრთხოების პოლიტიკას. ამ კუთხით, არც საქართველო არ არის გამონაკლისი. ჩვენ ვართ პატარა ქვეყანა, რომელსაც გააჩნია დიდი ამბიციები გახდეს ევროპული ოჯახის ღირსეული წევრი. ნატო და ევროკავშირი მოითხოვენ, რომ მისმა პარტნიორმა და ერთგულმა მოკავშირემ საქართველომ შეასრულოს მის მიერ აღებული ვალდებულებები. ამ აღებულ ვალდებულებებს შორის ჩვენ ვხვდებით - კიბერუსაფრთხოებასაც. კერძოდ, საქართველოს სახელმწიფოს მხრიდან კიბერუსაფრთხოების პოლიტიკის გაძლიერებასა და დახვეწას. ამასთანავე, გასათვალისწინებელია საქართველოს გეოგრაფიულ-სტარტეგიული მდებარეობაც.

ეს ფაქტორი კიდევ უფრო მეტად აუცილებელს ხდის მაქსიმალურად იქნას დაცული და გაძლიერებული ჩვენი ქვეყნის ეროვნული უსაფრთხოება. საქართველოს გეოგრაფიულ-სტრატეგიული მდებარეობიდან გამომდინარე ჩვენ ვართ გარშემორტყმულნი იმ სახელმწიფოებით, რომლებიც წარმოადგენენ სახელმწიფო - კიბერგიგანტებს. რეგიონში ამგვარი კიბერგიგანტ ორია: რუსეთი და ირანი.

2008 საქართველომ უკვე იწვნია რუსეთის ძლიერი კიბერ ხელი. აგვისტოს მოვლენებმა საქართველოს სახელმწიფოს კიდევ ერთხელ დაანახა ის, რომ კიბერსივცრის კუთხით საქართველო დაცული არ არის და რომ მისი ჩამოშლა მნიშვნელოვან და დიდ ზიანს აყენებს ქვეყნის ეროვნულ უსაფრთხოებას. ამასთანავე, ამ მოვლენამ დაგვანახა,რომ საქართველოს სახელმწიფოს მიერ გატარებული სოციალურ-ეკონომიკური რეფორმები არ არის ეროვნული უსაფრთხოების უზრუნველყოფის ერთერთი და ერთადერთი გარანტია. 2008 წლის აგვისტოს მოვლენებმა დაგვანახა ისიც , თუ რაოდენ დიდ ყურადღებას საჭიროებს ეროვნული უსაფრთხეობის პოლიტიკა. იგი მოითხოვს დახვეწასა და განახლებას.

კიბერუსაფრთხოება შედარებით ახალი ფენომენია. იგი დიდ თავის ტკივილს წარმოადგენს, როგორც განვითარებული და სტაბილური დემოკრატიების მქონე ქვეყნებისათვის, ასევე დემოკრატიის მშენებარე ქვეყნებისთვისაც, რომელთა რიგებშიც საქართველოც შედის. აღნიშნული კვლევა აქტუალური და ახალია, რადგან საქართველოში კვლევები, რომლებიც შეეხება კიბერუსაფრთხოებას საკამოდ მცირეა. კიბერუსაფრთხოების თემა არც თუ ისე აქტუალური და კვლევების მხრივ არც თუ ისე პოპულარულია. შესაბამისად, ამ კვლევის მთავარ მიზანს წარმოადგენს კიბერუსაფრთხოების თემის წინ წამოწევა და არსებული პრობლემების, ამოცანებისა და მასთან დაკავშირებული საკითხების უკეთ გამოკვეთა და შესწავლა. კიბერუსაფრთხოება, საქართველოსათვის ეს არის ის სივრცე, სადაც ჩვენ ქვეყანას ბევრი რეფორმა აქვს გასატარებელი. საქართველოს არ გააჩნია ერთიანი საკანონმდებლო ბაზა ის ჯერ კიდევ გაუმართავი და დასახვეწია. გასაძლიერებელია ან ახლიდან შესაქმნელია ტექნოლოგიურ-ადმინისტრაციული აპარატი. ეს ყოველივე მიუთითებს იმაზე თუ რაოდენ მნიშვნელოვანია კიბერუსაფრთხოების თემის კვლევა, რამდენად

აქტუალურია იგი ჩვენი სახელმწიფოსათვის და რაოდენ ბევრი ნაბიჯია გადასადგმელი სახელმწიფოს მხრიდან მის გასაძლიერებლად.

აუცილებელია ამ საკითხის სიღრმისეული კვლევა, რათა გამოვლინდეს ფაქტორები, რომლებიც განაპირობებენ ეროვნულ უსაფრთხოებაში კიბერუსაფრთხოების პოლიტიკის როლს. კვლევის შედეგად ჩვენ ვნახავთ, თუ რა მიზეზ-შედეგობრივი კავშირი არსებობს მათ შორის. კვლევა გვაძლევს შესაძლებლობას დავინახოთ ჩვენი სუსტი და ძლიერი მხარეები, რაც თავის მხრივ უმნიშვნელოვანესია , მოქნილი და ძლიერი ეროვნული უსაფრთხოების პოლიტიკის ფორმირებისათვის.

კვლევის მიზანი: დადგინდეს და გამოიკვეთოს საქართველოს სახელმწიფოს კიბერუსაფრთხოების დონესა და ეროვნული უსაფრთხოების დონეს შორის მიზეზ-შედეგობრივი კავშირი, თუ რა უშუალო ზეგავლენას ახდენს ქვეყნის კიბერუსაფრთხოების კუთხით გატარებული რეფორმები, ქვეყნის ეროვნულ უსაფრთხოებაზე.

ამოცანა : გაანალიზდეს ეროვნული უსაფრთხოების კუთხით გატარებული რეფორმები. გაანალიზდეს საქართველოს საკანონმდებლო ბაზა, რომელიც შეეხება უშუალოდ, როგორც ეროვნულ უსაფრთხოებას, ასევე ქვეყნის კიბერუსაფრთხოებასა და მის ძირითად საკითხებს. გაანალიზებულ იქნას ყველა ის საშინაო და საგარეო დოკუმენტი, რომლის შესრულებაზეც ხელი მოაწერა ან აიღო ვალდებულება საქართველოს სახელმწიფომ და რომელიც უშუალოდ ეხება ქვეყნის ეროვნულ უსაფრთხოებასა და კიბერუსაფრთხოების პოლიტიკას.

საკვლევი კითხვა : უზრუნველყოფს თუ არა საქართველოს სახელმწიფოს მიერ გატარებული რეფორმები კიბერუსაფრთხოების მაღალ დონეს?

ჰიპოთეზა: საქართველოს სახელმწიფოს მიერ კიბერუსაფრთხოების სფეროში გატარებული აქტიური და თანმიმდევრული ტექნიკურ-საკანონმდებლო რეფორმები უზრუნველყოფს ქვეყნის კიბერუსაფრთხოების დონის ზრდას, რაც საკუთრივ ზრდის ქვეყნის ეროვნულ უსაფრთხოებას.

ოპერაციონალიზაცია: აღნიშნული ჰიპოთეზიდან გამომდინარე ჩვენ ვხედავთ კორელაციას ქვეყნის ეროვნულ უსაფრთხოებასა და კიბერუსაფრთხოების პოლიტიკას შორის, კერძოდ რაც უფრო მეტად იზრდება ქვეყნის კიბერუსაფრთხოების დონე, მით უფრო მეტად მაღალია ქვეყნის ეროვნული უსაფრთხოების დონეც. შესაბამისად , კიბერუსაფრთხოების მენეჯმენტი ნაციონალური უსაფრთხოების კონტექსტში დაკავშირებული და ერთმანეთისათვის ურთიერთსასიცოცხლოა. დღევანდელ ციფრულ სამყაროში,სადაც კიბერსივრცე საომარი მოქმედებების ახალ ფრონტად იქცა ქვეყნები, რაც შეიძლება მეტად აძლიერებენ თავიანთ კიბერსივცრეს. ატარებენ რეფორმებს, რომლებიც უზრუნველყოფენ ამ უკანასკენლის დაცულობას. აუცილებელია, განვმარტოთ თუ რას მოიცავს ტექნიკურ-საკანონმდებლო რეფორმა/ები. ტექნიკურ-საკანონმდებლო რეფორმები ეს არის კომპლექსური რეჟიმის ერთობლიობა ,რომელიც საკუთრივ მოიაზრებს და თავის თავში გულისმობს, სხვადახვა საკანონმდებლო და ტექნოლოგიურ აქტივობებს,რომელთა განხორციელებაზე პასუხისმგებელია სახელმწიფო. კერძოდ, ეს არის სახელმწიფოს მხრიდან ციფრული სივრცის ინფორმაციულ-ტექნოლოგიურ მართვა, კონტროლის მენეჯმენტი , ინციდენტების იდენტიფიკაცია ,ინციდენტების მართვა და ინციდენტის/ების მართვის შედეგად გამოვლენილი დანაშაულის აღკვეთა ან აღკვეთის შეუძლებლობის შემთხვევაში ჩადენილი დანაშაულის საკანონმდებლო განკარგავა და საჭიროების შემთხვევაში კანონიერი დასჯა.

პოლიტიკურ ლექსიკონებში ტერმინი ეროვნული უსაფრთხოება განხილულია, როგორც სახელმწიფოს ერის, როგორც კულტურულ-პოლიტიკური ერთობის, ყველა იმ სასიცოცხლო პირობა, რომელიც უზრუნველყოფს მის არსებობასა და განვითარებას. ტრადიციულად, ეროვნული უსაფრთხოება გულისხმობდა ქვეყნის ტერიტორიული მთლიანობისა და მისი შინაგანი პოლიტიკური სტაბილურობის უზრუნველყოფას. ქვეყნის ეროვნული უსაფრთხოება განიხილება არა მხოლოდ სამხედრო-პოლოტიკურ, არამედ ეკონომიკურ სისტემასთან მჭიდრო კავშირში.

შესაბამისად, ქვეყნის ეროვნული უსაფრთხოების დასუსტება, პირდაპირ დარტყმას აყენებს სახელმწიფოს , როგორც კულტურულ-პოლიტიკურ ერთობას. რეფორმები კი, რომლებიც ახდენენ ამ ორ ცვლადს შორის დაბალანსებული

ურთიერთობის შენარჩუნებასა და ერთმანეთის შევსებასა და გაძლიერებას მოიცავენ: კრიტიკული ინფრასტურქტურის, საკანონმდებლო ბაზების,ტექნიკურ-მეცნიერული ჰაბებისა და ე.წ. ველების არსებობასა და დროულ თანმიმდევრულ დახვეწას. ამ კუთხით მნიშვნელოვანი როლი ენიჭება სახელმწიფოს აღმსარულებელი ხელისუფლებისა და კერძო სექტორს შორის თანმიმდევრულ თანამშრომლობას. შესაბამისად :

- კვლევის პერიოდში გამოვლენილი იქნა ის ძირითადი სამუშაო მიმართულებები ზემოთ ჩამოთვლილი ასპექტებიდან, რომლებიც საქართველოს სახელმწიფომ განახორციელა 2008 წლიდან 2017 წლამდე.

- მუშაობის თავისებურებები, გატარებული რეფორმები და მიმდინარე სამუშაოები წარმოჩენილია დოკუმენტების, გაფორმებული ხელშეკრულებებისა და საქართველოს სახელმწიფოს მიერ აღებული და შესრულებულ ვალდებულებებში, სწორედ მათი ანალიზის მეშვეობით შეგვიძლია დავადგინოთ რამდენად გაძლიერდა ან დასუსტდა კიბერუსაფრთხოების დონე საქართველოში და როგორ აისახებოდა ეს ქვეყნის ეროვნულ უსაფრთხოებაზე, როგორი იყო მათ შორის მიზეზ-შედეგობრივი კავშირი.

სახელმწიფოს მიერ გატარებული რეფორმები წარმოდგენილია, როგორც დამოუკიდებელი ცვლადი, შუამავალი ცვლადი აქ არის კიბერუსაფრთხოების დონე, დამოკიდებული ცვლადი კი ამ შემთხვევაში ეროვნული უსაფრთხოებაა.

როგორც ზემოთ ავღნიშნეთ, კვლევის პერიოდში განხილულ იქნა და გაანალიზებულ იქნა ყველა ის დოკუმენტები, აღებული ვალდებულებები და ხელმოწერილი ხელშეკრულებები, რომელიც განხორციელებული იქნა საქართველოს სახელმწიფოს მიერ 2008 წლიდან -2017 წლამდე. გაანალიზებულია ყველა ის რეფორმატორული ქმედება, რომელიც 9 წლის განმავლობაში განხორციელდა ქართული სახელმწიფოს მიერ.

- ამასთანავე, კვლევის განმავლობაში ყურადღება იქნა გამახვილებული 2008 -2017 წლების საქართველოს მიმართ განხორციელებული კიბერშეტევების ანალიზზე და სახელმწიფოს მხრიდან მათ მიმართ რეაგირებაზე. რამდენად იქნა

უზრუნველყოფილი სახელმწიფოს მხრიდან თავდასხმების რაოდენობის შემცირება და კიბერ თავდასხმებზე რეაგირების დროითი კოეფიციენტის შემცირება.

კვლევის მეთოდოლოგია : კვლევის მიზნიდან გამომდინარე, მთავარი იყო აღნიშნული საკითხის სიღრმისეულად შესწავლა. კითხვებზე როგორ და რატომ პასუხის მიღება და მიღებული ინფორმაციის გაანალიზება. ჩემ მიერ გამოყენებულია , როგორც თვისებრივი, ასევე რაოდენობრივი კვლევის მეთოდი. კვლევის ამგვარი მეთოდი გვეხმარება უფრო მეტად სიღრმისეულად შევისწავლოთ საკითხი და გამოვარკვიოთ მიზეზ-შედეგობრივი კავშირი. გამოკითხულ იქნენ და ჩატარებული იქნა სიღრმისეული ინტერვიუები ადამიანებთან ,რომლებიც მუშაობენ და არიან სპეციალიზებულნი კონკრეტულად ეროვნული უსაფრთხოებისა და კიბერუსაფრთხოების პოლიტიკის კუთხით. პირები, რომლებიც არიან კიბერუსაფრთხოებისა და ეროვნული უსაფრთხოების საკითხებზე მომუშავე ანალიტიკოსები, ქართველი და არაქართველი (ესტონელი, უკრაინელი) ექსპერტები, ინტერნეტ - სერვისის პროვაიდერები. აღმასრულებელი და საკანონმდებლო სფეროს წარმომადგენლები, სხვადასხვა არასამთვარობო ორგანიზაციის წარმომადგენლები.

ჯამში ინტერვიუ ჩატარდა 15 ადამიანთან ,რომლებმაც მოგვაწოდეს კვლევისათვის საჭირო და აუცილებელი ინფორმაცია. შერჩევის ტიპი გახლდათ: მიზნობრივი შერჩევა ანუ კონკრეტული ექსპერტებისა და ანალიტიკოსების შერჩევა. კვლევის პროცესში გამოყენებულ იქნა თოვლის გუნდის პრინციპი. ამასთანავე კვლევაში გამოყენებულია შედეგი ტიპის მასალები:

- კონტენტ-ანალიზი. ლიტერატურული მასალის მოძიება/ დამუშავება, თემის აქტუალურობის ოპერაციონალიზაციისთვის. სტატისტიკური მონაცემების მოძიება / დამუშავება/გამოყენება.
- ექსპერტთა გამოკითხვა-ექსპერტული ინტერვიუ .

კვლევის ობიექტი (ები) *:* პოლიტიკის დოკუმენტები, სტრატეგიები/ ხელშეკრულებები, რომლებიც საქართველოს კიბერუსაფრთხოების პოლიტიკასა და ეროვნულ უსაფრთხოებას შეეხება.

კვლევის ლიმიტი: 1. კვლევა არ ეხება და არ მოიცავს ფინანსურ და საბიუჯეტო საკითხებსა და დოკუმენტებს. 2. კვლევა არ ეხება იმ წლებს, რომლებიც არ შედის კვლევის კონკრეტულ დროის მონაკვეთში.

ლიტერატურის მიმოხილვა- თეორიული ჩარჩო:

თანამედროვე სამყაროს სწრაფი განვითარების ფონზე იცვლება თანამედროვე თავდაცვის საშუალებებიც. სახელმწიფოები სულ უფრო მეტ თანხებს ხარჯავენ თანამედროვე თავდაცვის სისტემების შემუშავებისათვის. ფინანსების დიდი ნაწილი ხმარდება თანამედროვე ტექნოლოგიების დახვეწასა და კიბერსივრცის სფეროს გაძლიერებას. თანამედროვე გამოწვევებიდან გამომდინარე ქვეყნები არა მარტო იცავენ თავს, არამედ თავს ესხმიან კიდეც ერთმანეთს. ის, რომ კიბერუსაფრთხოების სივრცის უსაფრთხოება პირდაპირ კავშირშია ეროვნულ უსაფრთხოებასთან დღესდღეობით არცერთი სახელმწიფოსათვის არ წარმოადგენს საიდუმლოს. კიბერთავდასხმების მსხვერპლი შეიძლება გახდნენ, როგორც სახელმწიფო სტრუქტურები, ასევე სხვადასხვა ჯგუფებისა და სასიცოცხლოდ მნიშვნელოვანი ინფრასტურქტურის წარმომადგენლებიც. ასეთ გარემოში არც საქართველო წარმოადგენს გამონაკლისს. ამის დასტურია 2008 წლის კიბერ ომიც, რომელიც მის წინააღმდეგ აწარმოა რუსეთმა. ევროკავშირთან გაფორმებული ასოცირების ხელშეკრულების თანახმად საქართველომ აიღო რიგი ვალდებულებებისა, რომ მაქსიმალურად შეუწყობს ხელს ქვეყნის კიბერსივრცის გაძლიერებას. ამასთანავე დოკუმენტში ხაზგასმულია ამ ნაბიჯების გადადგმის აუცილებლობასა და მის საჭიროებაზე, როგორც თავად საქართველოსთვის, ასევე მისი პარტნიორი ევროკავშირისათვისაც. გამომდინარე იქიდან, რომ მეოთხე ფრონტს თანამედროვე სამყაროში კიბერსივრცე წარმოადგენს საჭიროა სახელმწიფომ (ებმა) მაქსიმალაურად დახვეწოს(ონ) და გააძლიეროს (ონ), როგორც ტექნოლოგიური, ასევე ნორმატიულ-საკანონმდებლო ბაზა,რაც თავის მხრივ ხელს შეუწყობს ქვეყნის ეროვნული უსაფრთხოების კიდევ უფრო მეტად დაცვას.

სალიტერატურო მასალა,რომელიც ეხება კვლევასთან დაკავშირებულ საკითხს დღესდღეობით საკმაოდ მწირია,მიუხედავად ამისა, კიბერუსაფრთხოებასა და ეროვნულ უსაფრთხოებას შორის მჭიდრო კავშირის შესახებ საუბარი გვეხვდება

უმეტესობა მათგანში. ყურადღება გამახვილებული იქნა იმ ავტორებზე, რომლებიც მოგვითხრობენ პატარა ქვეყნების კიბერგამოცდილების შესახებ. თანამედროვე ტექნოლოგიურმა მიღწევებმა, მიუხედავად ცხოვრების გამარტივებისა, რიგი პრობლემები და ახალი გამოწვევები წარუდგინა,როგორც სახელწიფოს,ასევე მის თითოეულ მოქალაქეს.

საკუთარ სისტემაში გააჩნია რიგი სხვადასხვა სახის ინფორმაციისაა, რომელიც ეხება, როგორც სახელმწიფო უსაფრთხოების საკითხებს, ასევე საზოგადოებრივი ინტერესების საკითხებსაც. შესაბამისად, სახელმწიფო ფლობს როგორც კერძო, ასევე საჯარო სახის ინფორმაციას საკუთარ მოქალაქეებზე. შესაბამისად, უმნიშვნელოვანესია სახელმწიფოს ეროვნული უსაფრთოხებისათვის დაცული იქნას როგორც ორგანიზაციული, ასევე სახელმწიფო და პირადი ინფორმაციის შემცველი სისტემები. (LeClair, J . Keeley,G. 2015.) ამასთანავე, უმნიშვნელოვანესია სწორი კიბერპოლიტიკის არსებობაც. მნიშვნელოვანია ხაზი გავუსვათ იმასაც თუ რაოდენ დიდი გზის გავლა უწევს პატარა სახელმწიფოს, რათა მან მოახდინოს საკუთარი რესურსების სწორედ გადანაწილება და კიბერუსაფრთხოების თანამედროვე მოთხოვნილებებსა და გამოწვევებზე პასუხის გაცემა.

კიბერთავდაცვა, ტექნოლოგიური განვითარება, სამეცნიერო წინსვლა, ადამიანური და საგანმანათლებლო კაპიტალი ერთად შეადგენენ კიბერუსაფრთხოების ნაციონალურ პოლიტიკას, რომელიც მჭიდრო კავშირშია ეროვნულთან. მას უდიდესი მნიშვნელობა ენიჭება განსაკუთრებით კი პატარა ქვეყნებისათვის . თანამედროვე სამყაროს კიბერ გამოწვევებიდან გამომდინარე სახელმწიფომ უნდა გაატაროს ისეთი კიბერპოლიტიკა,რომელიც უზრუნველყოფს მისი ქვეყნის დაცვას და მისი,როგორც კიბერ ლიდერის ჩამოყალიბებას (Tabansky,L. Israel,B. 2012) ინფორმაციული ომები, ასიმეტრიული ომის პრინციპის გამოყენება მნიშვნელოვანი თავსატეხია არა მარტო, განვითარებული დიდი რესურსების მქონე ქვეყნებისათვის, არამედ პატარა ქვეყნებისათვისაც. ნებისმიერი ქვეყნის მაგალითი და მათ მიერ გატარებული რეფორმები უნდა იყოს მისაბაძი მაგალითი. (Cavelty,M. 2014) ამის ცხად მაგალითს კი წარმოადგენს შვეიცარია. შვეიცარიის მაგალითიდან გამომდინარე მნიშვნელოვანი

ხდება კიბერსივრცის დაცვა და პირველ რიგიში რეფორმების გაატარება, განსაკუთრებით საკანონმდებლო-ნორმატიული ბაზების კუთხით.

კიბერსივრცეში ე.წ. ფერადი ქუდების თეორიის თანახმად, კიბერუსაფრთხოების სფეროში ჩვენ ვხვდებით ქუდების მეპატრონეებს, რომლებიც ამ ქუდებს ყოველდღე ატარებენ. შავი ქუდის პატრონები- ჰაკერები არიან, IT პროგრამების თანამშრომლები და სამეცნიერო ტექნოლოგიის წარმომადგენლები კი -თეთრი ქუდისა.

ცისფერი ქუდები- იცავენ უსაფრთხოებას, ხოლო წითელი ქუდები- თავს ესხმიან სხვა კიბერსივცრის სისტემებს. (Dalziel,M. 2014) ამ ქუდების ერთობლიობა უზრუნველყოფს ქვეყნის უსაფრთხოების დაცვას, როგორც სახელწიფო, ასევე არასახელმწიფო სტუქტურებში. აუცილებელია ქვეყანამ მოახერხოს და შექმნას ერთიანი სისტემა, რომელიც უზრუნველყოფს ქვეყნის კიბერუსაფრთხოების დაცვას. პოლიტიკურ ლექსიკონებში ტერმინი ეროვნული უსაფრთხოება განხილულია, როგორც სახელმწიფოს ერის, როგორც კულტურულ-პოლიტიკური ერთობის, ყველა იმ სასიცოცხლო პირობას, რომელიც უზრუნველყოფს მის არსებობასა და განვითარებას. ტრადიციულად, ეროვნული უსაფრთხოება გულისხმობდა ქვეყნის ტერიტორიული მთლიანობისა და მისი შინაგანი პოლიტიკური სტაბილურობის უზრუნველყოფას. ქვეყნის ეროვნული უსაფრთხოება განიხილება არა მხოლოდ სამხედრო-პოლოტიკურ, არამედ ეკონომიკურ სისტემასთან მჭიდრო კავშირში. მნიშვნელოვანია ყურადღების გამახვილება მოვახდინოთ იმ ფაქტორებზეც ,რომ უსაფრთხოების საკითხები არ არის მხოლოდამხოლოდ სამხედრო ხასიათის მატარებელი გამოწვევები. მნიშვნელოვანია საფრთხე დანახული იქნას სამხედრო პრიზმის მიღმაც. თანამედროვე სახელმწიფოს ეროვნული უსაფრთხოების პრობლემები არ მოიცავს მხოლოდამხოლოდ სამხედრო ხასიათის გამოწვევებს. სახელმწიფოს უსაფრთხოებას საფრთხეს უქმნის ყველა ის გამოწვევა, რომელიც აფერხებს მისთვის დამახასიათებელი ნებისმიერი ფუნქციის შეფერხებას ან შეჩერებას. (Collins,A. 2013) ეროვნული უსაფრთხოება არ მოიცავს მოლოდამხოლოდ სამხედრო საკითხებს (Morgenthau, H. 1948.). ეროვნული უსაფრთხოება მოიცავს ყველაფერ იმას, სადაც საზოგადოების უსაფრთხოებისა და წინსვლის საკითხები წყდება. (კენანი, ლიპმანი.)

ამერიკის შეერთებული შტატების თავდაცვის დეპარტამენტის ხელმძღვანელის ოფიციალურ მოხსენებაში ვკითხულობთ: *„სახელმწიფო, რომელიც აკონტროლებს კიბერსივრცეს, აკონტროლებს ომსა და საკუთარი ქვეყნის მშვიდობას. დღეს ტყვიები არ წყვეტენ არაფერს, დღეს მთავარი გაიტებია.“*

მეცნიერების ნაწილი საკუთარ სამეცნიერო გამოსვლებსა და პუბლიკაციებში ხაზს უსვამს ფაქტს იმის შესახებ, რომ თანამედროვე მსოფლიოში დღესდღეობით არ არსებობს ერთიანი შეთანხმებული აზრი კიბერუსაფრთხოების განსაზღვრების შესახებ. თითოეული მათგანი ახდენს კიბერუსაფრთხოებისა და მასთან მჭიდრო დაკავშირებული ტერმინების საკუთარ ინტერპრეტირებას. რასაც მივყავართ იქამდე, რომ ყოველი მათგანი ახდენს მის ინტერპრეტირებას თავისებურად. განსხვავება არსებობს, როგორც საკანონმდებლო-ნორმატიულ, ასევე ქვეყნების ეროვნული და კიბერუსაფრთხოების სტრატეგიებშიც. სახელმწიფომ არსებულ კიბერგამოწვევას უნდა შეხედოს კომპლექსურად; უნდა მოახდინოს საკუთარი პლიუსებისა და მინუსების გამჭირვალედ დანახვა.

რ.კლარკი (2010) უშუალოდ აკავშირებს ერთმანეთთან ეროვნულ უსაფრთხოებასა და კიბერუსაფრთხოებბის პოლიტიკას. საქართველოს მაგალითის პარალელურად მას ესტონეთის მაგალითიც მოჰყავს და ხაზს უსვამს იმ ფაქტს თუ რაოდენ მნიშვნელოვანია პატარა სახელმწიფოსათვის და მისი ეროვნული უსაფრთხოებისათვის გამართული კიბერსივრცე. 2008 წლის მოვლენების აღწერისას კლარკი სწორედ ამ ორ ცვლადს ერთმანეთთან აკავშირებს. კლარკი ხაზს უსვამს კიბერშეტევისათვის სახელმწიფოს მაქსიმალურად მომზადების საჭიროებას და იმ შედეგებს გამოთვლას ,რომელიც კიბერომმა შესაძლოა მოუტანოს ქვეყანას. კიბერსივრცე წარმოადგენს ომის ახალ ფრონტს, რომელშიც სახელმწიფომ უნდა გაიმარჯვოს. ავტორი აღიარებს სამხედრო პოტენიციალის მნიშვნელობას სახელმწიფოს თავდაცვის უნარიანობისათვის, თუმცა ამასთანავე ის აღნიშნავს იმას, რომ ომის სამხედრო კლასიკური ტრადიცია ნელნელა წარსულს ბარდება და რომ მის ადგილს კიბერშეტევები და კიბერომები იკავებენ. კლარკისათვის მნიშვნელოვანია, რომ სახელმწიფომ გაატაროს ძლიერი და მოქნილი პოლიტიკა. ამოავსოს ე.წ. ''თეთრი ლაქები'' და გააძლიეროს საკუთარი ეროვნული უსაფრთხოების პოლიტიკა. იგი აქ მოიაზრებს სხვადასხვა სახის რეფორმებსა და

ტექნოლოგიური /მეცნიერული განვითარების აუცილებლობას. (Clarke,R. and Knake,R. 2010).

ის ხაზს უსვამს იმას, რომ სახელმწიფო ვერ და არ იქნება სრულყოფილად დაცული, თუკი იგი არ უზრუნველყოფს საკუთარი ციფრული სივრცის 100%-იან დაცვას. და ეს ნამდვილად ასეცაა, რადგან სწრაფად განვითარებად და პროგრესულ სამყაროში, სადაც ყველაფერი ციფრულ, ელექტრონულ მმართველობაზეა , უმნიშვნელოვანესი ხდება ამ სივრცის მოწესრიგება და გამართული მუშაობა. შესაბამისად, აუცილებელია სახელმწიფოს მიერ გათვალისწინებული იქნას , როგორც ძველი კლასიკური საომარი თეორიები და ა.შ. ასევე თანამედროვე ჰიბრიდული ომისათვის დამახასიათებელი ასიმეტრიული ომისა ასპექტებიც.

თეორიული ჩარჩო : კვლევის შემთხვევაში გამოყენებული იქნება თამაშთა თეორია , რომელიც გულისხმობს თამაშებში ოპტიმალური სტრატეგიის შესწავლის მათემატიკურ მეთოდს.(Neumann; 1954) თამაშში იგულისხმება პროცესი, რომელშიც მონაწილეობს ორი ან მეტი მხარე, რომლებიც იბრძვიან საკუთარი ინტერესების რეალიზაციისთვის. თითოეულ მხარეს აქვს თავისი მიზანი და იყენებს გარკვეულ სტრატეგიას. თამაშთა თეორია გვეხმარება საუკეთესო სტრატეგიის არჩევაში სხვა მონაწილეების, მათი რესურსებისა და შესაძლო ქმედებების გათვალისწინებით. თამაშთა თეორია არ გამოიყენება მხოლოდამხოლოდ მათემატიკაში, ისე ასევე აქტიურად და წარმატებით არის გამოყენებული: სოციოლოგიაში, პოლიტოლოგიაში, ფსიქოლოგიაში, და ა.შ. იგი დაკავშირებულია კონტროლთან და ძალაუფლებასთან. თამაშთა თეორია მჭიდრო კავშირშია კიბერნეტიკასთან. იგი აგრეთვე შეუსაბამეს კიბერუსაფრთხოებასაც. კიბერდამნაშავე, რომელიც უტევს კიბერსივრცეს და კიბერსივრცის დამცველი (სახელმწიფო ინსტიტუტი თუ ბიურო) ჩაბმულნი არიან არა მარტო მუდმივ შეტევასა და თავდასხმაზე, არამედ მათ გააჩნიათ საკუთარი სტრატეგია და გეგმა,რომლის მიხედვითაც მოქმედებენ შეტევის დროს. მოთამაშეების და ამ შემთხვევაში ზემოთ აღნიშნული ორი სუბიექტის მთავარი მიზანია მოიპოვონ უპირატესობა, დაასუსტონ მოწინააღმდეგე და მიიღონ ამ სამი ვარიანტიდან ერთი შედეგი: A): ე.წ. ნეშის ეკვილიბრიუმი. ამ შემთხვევაში, ორი დაპირისპირებული მხარის ქმედება დამოკიდებულია მისი ოპონენტის ნაბიჯებზე.აქ

ორივე მათგანს აქვს დომინანტი სტრატეგია,რისი მიხედვითაც წარმართავს თამაშს.არც ერთი მათგანი არ ცვლის სტრსტეგიას,თუ ამის შანსი მიეცა. B): ნული ჯამის მოქნე რეზულტატი - ამ შემთხვევაში ერთი მოთამაშის მოგება ავტომატურად გულისხმობს მეორის წაგებას.როცა ერთი მხარე აღწევს გამარჯვებას, მეორე მარცხდება. C): პოზიტიური ან ნეგატიურ ჯამოვანი - დადებითი შედეგით მთავრდება, როცა ყოველი მოთამაშე იღებს სარგებელს ,იმ შემთხვევაშიც თუკი ერთის სარგებელი მეტია მეორეს სარგებელზე. ამ შემთხვევაში გამოკვეთილად წაგებული არავინაა.ნეგატიური ჯამოვანი რეზულტატის არსებობის შემთხვევაში თითოეული მოთამაშის მოქმედება ერთნაირად აყენებს ზიანს მასაც და დანარჩენ მოთამაშეებსაც.

ამ კვლევაში თამაშის თეორის გადმოტანით ვხედავთ ე.წ. - შეტევების ავტორს ჰაკერს ან კონკრეტულ A. „აგრესორ“ სახელმწიფოს. (რუსეთი-საქართველო 2008.წ.), ხოლო B „ მსხვერპლი“ წარმოდგენილია, როგორც მისი კონკურენტი სახელმწიფო ინსტიტუტი ან მასთან მებრძოლი კონკრეტული ბიურო. პირველის მიზანია თავისი ქმედებით გამოიწვიოს სავალალო შედეგი, ხოლო მეორესი- შეაჩეროს ის. კვლევაში აღნიშნული თეორია განხილულია ნულოვანი ჯამის შედეგის მიხედვით. სახელმწიფო ინსტიტუტები ან ეფექტურად იმუშავებენ და შეძლებენ გაუმკლავდნენ შეტევებს, მოხდება კიბერუსაფრთხოების სივრცის გაძლიერება, რაც საკუთრივ გულისხმობს არა მხოლოდ ტექნოლოგიურ, არამედ ადამიანური რესურსების გაძლიერებას (კიბერანალიტიკოსები,კიბერარმია და ა.შ.). რაც, საკუთრივ უზრუნველყოფს სახელმწიფო ინსტიტუტებზე შეტევისას ეროვნული უსაფრთხოების დაცვას და შესაბამისად „ ბრძოლის „ შემთხვევაში აგრესორის დამარცხებას ან დადგება მეორე შედეგი: სუსტი კიბერუსაფრთხოების სივრცის მქონე B სუბიექტი იწვნიებს დამარცხებას. რაც საკუთრივ დიდი ზიანის გამომწვევი და გარდამტეხი შეიძლება აღმოჩნდეს ეროვნული უსაფრთხოებისათვის.

თავი1. საქართველოს კიბერუსაფრთხოებისა და ეროვნული უსაფრთხოების საკითხები

2008 წლის აგვისტოში რუსეთის ფედერაციის მიერ საქართველოს წინააღმდეგ განხორციელებულმა კიბერშეტევებმა, მოახდინეს სამთავრობო და კერძო სექტორის ვებ-გვერდების გარკვეული დროით პარალიზება. რუსეთის მიერ საქართველოს მიმართ კიბერშეტევების დაწყება ჯერ კიდევ რამდენიმე თვით ადრე იქნა დაგეგმილი, სამხედრო საჰაერო, საზღვაო შეტევების კვალდაკვალ კიბერსივრცის პარალიზებამ საქართველოს სახელმწიფოს კიდევ ერთხელ დაანახა საკუთარი კიბერსივრცის სრული უსუსურობა და ქვეყნის წინაშე არსებული ახალი სტრატეგიული პრობლემის არსებობა. 2008 წლის აგვისტოს მოვლენებმა საქართველოს სახელმწიფოს დაანახა თუ რაოდენ მნიშვნელოვანია სწორი, გამართული და ძლიერი კიბერუსაფრთხოების პოლიტიკის ქონა. სახელმწიფომ გააცნობიერა, რომ საქართველოს ეროვნული უსაფრთხოება ვერ შედგება კიბერსივრცის უსაფრთხოების უზრუნველყოფის გარეშე. შესაბამისად, სახელმწიფოს მხრიდან მოხდა კიბერუსაფრთხოების თემის წინ წამოწევა. 2008 წლის შემდეგ საქართველომ შეიმუშავა, ქვეყნის კიბერუსაფრთხოების სტრატეგია , ასევე სახელმწიფომ მნიშვნელოვანი ცვლილებები შეიტანა ქვეყნის ეროვნული უსაფრთხოების კონცეფციაშიც.

1.1. საქართველოს კიბერუსაფრთხოების სტრატეგია

საქართველოს კიბერუსაფრთხოების სტრატეგია არის კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი, რომელიც ასახავს სტრატეგიულ მიზნებს, ძირითად პრინციპებს, აყალიბებს ამოცანებს და მათ შესასრულებლად განსაზღვრავს შესაბამის აქტივობებს. (საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგია და მის სამოქმედო გეგმა; გვ: 1)

ქვეყნის პირველი კიბერუსაფრთხოების სტრატეგია 2013 წლის 20 მაისს გამოქვეყნდა. სტრატეგია იმ პერიოდისათვის შემუშავებულ იქნა საქართველოს ეროვნული უშიშროების საბჭოსთან არსებული ეროვნული უსაფრთხოების

სტრატეგიული დოკუმენტების შემუშავების მაკოორდინირებელი მუდმივმოქმედი საუწყებათაშორისო კომისიის მიერ. 2013 წლის კიბერუსაფრთხოების სტრატეგია ეფუძნებოდა „ საქართველოს საფრთხეების შეფასების 2010-2013 წ.წ. დოკუმენტს“ და „ საქართველოს ეროვნული უსაფრთხოების კონცეფციას“. მასშივე მოცემული იყო 2013-2015 წ.წ. -ის სტრატეგიის განხორციელების სამოქმედო გეგმაც. მას ხელს საქართველოს მესამე პრეზიდენტი (2004-2013წ.წ.) მიხეილ სააკაშვილი აწერდა.

2017 წლის იანვარს საქართველოს მთავრობის მიერ გამოცემულ იქნა საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგია და მისი სამოქმედო გეგმა. დოკუმენტს ხელს საქართველოს პრემიერ-მინისტრი (2015-2018წ.წ.) გიორგი კვირიკაშვილი აწერს. სტრატეგია ეფუძნება „ საქართველოს საფრთხეების შეფასების 2015-2018 წლების დოკუმენტს“ და „ საქართველოს ეროვნული უსაფრთხოების კონცეფციას“.

ამასთანავე, აღსანიშნავია ის ფაქტიც, რომ 2013 წელს განხორციელებული საკონსტიტუციო ცვლილებების შედეგად, უშიშროების საბჭოს ჩამოერთვა რიგი უფლებამოსილებებისა. შესაბამისად, საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგია და მისი სამოქმედო გეგმა შემუშავებულ იქნა სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭოსა და მასთან არსებული ეროვნული უსაფრთხოების კონცეპტუალური დოკუმენტების შემუშავების მაკოორდინირებელი მუდმივმოქმედი უწყებათაშორისი კომისიის მიერ.

2013 წლის კიბერუსაფრთხოების სტრატეგიამ ხელი შეუწყო საქართველოს კიბერუსაფრთხოების სისტემის მდგრადობის ამაღლებას, რაც როგორც დოკუმენტში ვკითხულობთ, გამოწვეული იყო სახელმწიფოს მიერ დოკუმენტის სამოქმედო გეგმით გათვალისწინებული აქტივობების აბსოლუტური უმრავლესობის შესრულებით.

(საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგია და მისი სამოქმედო გეგმა, გვ:2) .

ახალი 2017-2018 წლების სტრატეგია ორიენტირებულია კიბერუსაფრთხოების სფეროს შემდგომ განვითარებაზე. ორივე სტრატეგიის უმთავრეს მიზანს წარმოადგენს საქართველოს მიერ იმგვარი კიბერუსაფრთხოების სისტემის შექმნა, რომელიც უზრუნველყოფს დაცული ინფორმაციული ინფრასტრუქტურის არსებობას.

სტრატეგიის მიხედვით საქართველოს სახელმწიფოსათვის გამოწვევას წარმოადგენს კიბერუსაფრთხოების იმგვარი სისტემის შექმნა, რომელიც უზრუნველყოფს ინფორმაციული ინფრასტრუქტურის დაცულობას კიბერსაფრთხეების წინაშე, რაც საკუთრივ უზრუნველყოფს მონაცემთა დაცვას ინფორმაციის გაცვლის პროცესში. ამასთანავე, სტრატეგიაში ხაზგასმულია კრიტიკული ინფორმაციული სისტემების დაცულობის მნიშვნელობაზე.

„კრიტიკული ინფორმაციული სისტემა“ - ინფორმაციული სისტემა, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის.“ (კანონი „ინფორმაციული უსაფრთხოების შესახებ,გვ: 1)

ეროვნული უსაფრთხოეებისათვის უმნიშვნელოვანესია აღნიშნული სისტემების მდგრადობა კიბერშეტევებისა და კიბერინციდენტების მიმართ. ამასთანავე, სტრატეგიის მიხედვით სახელმწიფოს მხრიდან უნდა განხორციელდეს დროული და ეფექტური რეაგირება კიბერინციდენტების მიმართ. 2013 წლის კიბერუსაფრთოხების სტრატეგიის თანახმად ამ ყველაფრის მისაღწევად საჭირო იყო სახელმწიფოს მიერ შემდეგი პრინციპებით ხელმძღვანელობა :

- საქართველოს მთავრობის ერთიანი მიდგომა.
- თანამშრომლობა კერძო და სახელმწიფო სექტორებს შორის.
- საერთაშორისო თანამშრომლობა.
- ინდივიდუალური პასუხისმგებლობა.
- ადეკვატური ზომები.

2017 წელს გამოქვეყნებულ საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიასა და მის სამოქმედო გეგმას დაემატა კიდევ ორი უმნიშვნელოვანესი პრინციპი. კერძოდ: კიბერუსაფრთხოება, როგორც ეროვნული უსაფრთხოების განუყოფელი ნაწილი - დოკუმენტში გაწერილია, რომ საქართველოს კანონმდებლობა და ეროვნული უსაფრთხოების ფუნდამენტურ კონცეპტუალური დოკუმენტები კიბერუსაფრთხოებას განსაზღვრავს, როგორც ეროვნული

უსაფრთხოების პოლიტიკის შემადგენელ მიმართულებას, რომლის მნიშვნელობაც ტექნოლოგიური პროგრესის პარალელურად განუზომლად იზრდება და მასზეა დამოკიდებული სახელმწიფოს ეფექტური განვითარება. მეორე ახალ პრინციპს, რომელიც ჩვენ გვხვდება 2017-2018 წლების საქართველოს კიბერუსაფრთხოების ეროვნულ სტრატეგიაში წარმოადგენს: ადამიანის უფლებათა და ძირითად თავისუფლებათა განუხრელი დაცვა და პატივისცემა. (საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგისა და მის სამოქმედო გეგმა; გვ:3)

2013 – 2015 სახელმწიფო კიბერუსაფრთხოების სამოქმედო გეგმის მსგავსად, 2017-2018 წლების ეროვნული სტრატეგიის ძირითად მიმართულებებად რჩება:

- კვლევა და ანალიზი.
- სამართლებრივი ბაზის შემუშავება და სრულყოფა.
- კიბერუსაფრთხოების სფეროში შესაძლებლობათა ამაღლება.
- საზოგადოებრივი ცნობიერების ამაღლება და საგანმანთლებლო ბაზის ჩამოყალიბება.
- საერთაშორისო თანამშრომლობა.

კიბერუსაფრთხოების სტრატეგიის მიხედვით საქართველოს სახელმწიფოსათვის უდიდეს გამოწვევას წარმოადგენს საკანონმდებლო ბაზის შემუშავება. 2010 წლიდან მოყოლებული საქართველოს გააჩნია კიბერუსაფრთხოების უზრუნველმყოფი ძირითადი სამართლებრივი ჩარჩო, რომელიც არეგულირებს სახელმწიფო კონტროლის მექანიზმებს. ამასთანავე, სწორედ ის განსაზღვრავს კერძო და საჯარო სექტორებს შორის უფლება-მოვალეობებს ინფორმაციული უსაფრთხოების დაცვის სფეროში. შესაბამისად, ამ კუთხით საქართველოს სახელმწიფოს მიერ შემუშავებულია კიბერუსაფრთხოების უზრუნველმყოფი ძირითადი სამრთლებრივი ჩარჩო:

- შემუშავებულია კანონქვემდებარე ნორმატიული აქტები.

- კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფის საქმიანობის სამართლებრივი საფუძვლები.
- განსაზღვრულია ამ კიბერუსაფრთხოების თემატიკაზე მომუშავე და უფლებამოსილი უწყებების კომპეტენციისა და საქმიანობის არეალი.

მიუხედავად ამისა, არსებობს რიგი ხარვეზებისა, რომელთა აღმოფხვრაც შესაძლებელია ადგილობრივ და საერთაშორისო დონეზე თანამშრომლობის შედეგად. ეს ყველაფერი კი შეუძლებელია სახელმწიფო ნების გარეშე, რაც გულისხმობს ამ კუთხთ არსებული ხარვეზების შესწორებას და სამრთლებრივი ბაზის გაძლიერებასა და დახვეწას.

საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგისა და მის სამოქმედო გეგმის თანახმად უნდა განხორციელდეს: კრიტიკული ინფრასტრუქტურის სისტემების კიბერუსაფრთხოების უზრუნველმყოფი სამართლე-ბრივი ბაზების გაანხლება; ინფორმაციული უსაფრთხოების მარეგულირებელი კანონმდებლობით გათვალისწინებული ვალდებულებების აღსრულების მექანიზმების შემუშავება; ევროპის საბჭოს 2001 წლის „ კიბერდანაშაულის შესახებ“ რატიფიცირების შედეგად აღებული ვალდებულებების შესრულების გაგარძელება; კრიტიკული ინფორმაციული ინფრასტრუქტურის განმსაზღვრელი და მისი კიბერუსაფრთხოების უზრუნველმყოფი ნორმატიული ბაზის შემდგომი დახვეწა და განვითარება.

ამასთანავე, 2013 წლის კიბერუსაფრთხოების სტრატეგიაში ქვეყნის კიბერსივრცისათვის საფრთხის მთავარ შემცველ სუბიექტს რუსეთი წარმოადგენს, მაშინ როდესაც 2017 -18 წლების სტრატეგიაში საუბარია რუსეთთან ერთად, დამატებით კიდევ მსოფლიო კიბერსივრცეში გამოჩენილ ახალ საფრთხეებზე, რომელიც წარმოდგენილია „ ისლამური სახელმწიფოს“ სახით და არა მარტო. აქვე, სტრატეგიის თანახმად სახელმწიფო უსაფრთხოებას საფრთხე შეიძლება შეუქმნას, დამოუკიდებლად მოქმედმა არასახელმწიფო აქტორებმა, რომლებიც შესაძლოა დაქირავებულნი იყვნენ კონკრეტული სახელმწიფოების მიერ. ნებისმიერ შემთხვევაში ჩვენ ვხედავთ წინა 2013-2015 წლების საქართველოს კიბერუსაფრთხოების სტრატეგიისგან განსხვავებით კიბერ საფრთხის შემცველი სუბიექტების მატებას.

იმისათვის, რათა თავიდან იქნას აცილებული ამ სუბიექტების მხრიდან და არა მარტო მათგან მომდინარე საფრთხეები, საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიასა და მის სამოქმედო გეგმაში გაწერილია კიბერუსაფრთხოების სფეროში შესაძლებლობების ამაღლების კუთხით გასატარებელი აქტივობებები. კერძოდ: კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფის შესაძლებლობების შემდგომი განვითარება; კომპიუტერული მონაცემების საექსპერტო კვლევის შესაძლებლობების შემდგომი განვითარება; სახელმწიფო საიდუმლოებების შემცველი ინფორმაციის მიმოცვლის დაშიფრული სისტემის შექმნა დ განვითარება. კიბერუსაფრთხოების ინციდენტების გამომწვევი სიტუაციურ სცენარებზე მორგებული ტრენინგებისა და კიბერ სავარჯიშოების ჩატარება.

მოქმედი სტრატეგიისათვის თანახმად სახელმწიფოსათვის პრიორიტეტს წარმოადგენს კიბერ-კვლევითი ლაბორატორიის ჩამოყალიბება, აგრეთვე კიბერ რეზერვის შექმნა, რომელიც მნიშვნელოვნად შეუწყობს ხელს ქვეყნის კიბერპოტენციალის გაძლიერებას. ამასთანავე, სტრატეგიის თანახმად უმნიშვნელოვანესია საქართველოს სახელმწიფოს მჭიდრო სამოკავშირეო ურთიერთობა საერთაშორისო დონეზე, რომელიც გამომდინარეობს ჩვენი ინტერესებიდან გავხვდეთ ნატოსა და ევროკავშირის წევრი ქვეყნები. ამასთანავე, სტრატეგიის მიხედვით საქართველომ უნდა განახორციელოს თანამშრომლობის კიდევ უფრო მეტად გაღრმავება ისეთ ორგანიზაციებთან, როგორებიცაა:

OECD - ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია.

OSCE- ევროპის უშიშროებისა და თანამშრომლობის ორგანიზაცია.

COE - ევროპის საბჭო

UN- გაერთიანებული ერების ორგანიზაცია

ITU -საერთაშორისო ტელეკომუნიკაციების კავშირი.

საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის თანახმად უდიდესი მნიშვნელობა ენიჭება საზოგადოების ცნობიერების ამაღლებას კიბერუსაფრთხოების კუთხით. ყოველივე ეს კი

უზრუნველყოფს გათვიცნობიერებული დაცული საზოგადოების ჩამოყალიბებას.

2017-2018 წლების სტრატეგიის მიხედვით შესრულებული სამუშაოების შედეგები ყოველწლიურად შეფასდება და ანგარიში წარედგინება სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭოს აპარატს, რომელიც საკუთრივ არსებული ანაგრიშის შედეგებს აცნობს უსაფრთხოებისა და კრიზისების მართვის საბჭოსთან არსებულ საქართველოს ეროვნული უსაფრთხოების მაკოორდინებელ საბჭოს.

1.2. საქართველოს ეროვნული უსაფრთხოების კონცეფცია

საქართველოს ეროვნული უსაფრთხოების კონცეფცია არის ფუძემდებლური დოკუმენტი, რომელიც განმარტავს სახელმწიფოს ფუნდამენტურ და ეროვნულ ინტერესებს. ამასთანავე, იგი აყალიბებს ქვეყნის წინაშე არსებულ საფრთხეებსა და გამოწვევებს. იგი ადგენს ქვეყნის უსაფრთხოების პოლიტიკის ძირითად მიმართულებებს. საქართველოს ეროვნული უსაფრთხოების კონცეფციის განახლებულმა ვერსიამ დღის შუქი 2012 წლის იანვარში იხილა. მან 2005 წელს გამოქვეყნებული ეროვნული უსაფრთხოების კონცეფცია ჩაანაცვლა. 2012 წლის ეროვნულ კონცეფციაზე ზეგავლენა 7 წლის განმავლობაში საქართველოს საგარეო და საშინაო ასპარეზზე მიმდინარე მოვლენებმა მოახდინეს.

კონცეფციას, როგორც ფუძემდებლურ დოკუმენტს გააჩნია, როგორც პოლიტიკური, ასევე საინფორმაციო დატვირთვა. პირველ შემთხვევაში ის განსაზღვრავს, პოლიტიკურ მიზნებს, ამოცანებსა და რისკებს. საინფორმაციო ფუნქცია კი საზოგადოებას აცნობს და წარუდგენს სახელმწიფოს პოზიციებს ეროვნული უსაფრთხოების პოლიტიკასთან დაკავშირებით.

საქართველოს ეროვნული კონცეფციის ორივე დოკუმენტში საქართველოს მთავარ საფრთხის შემცველ საგარეო ობიექტად სახელდება რუსეთის ფედერაცია. 2008 წლის აგვისტოს მოვლენებმა და საქართველოს მიმართ რუსეთის ფედერაციის მიერ წარმოებულმა ახალი ტიპის ომმა, რიგი ცვლილებები შეიტანა ეროვნული

უსაფრთხოების დოკუმენტში. შეიცვალა საფრთხის შემცველი ფაქტორებისა და ობიექტების სია, ამასთანავე, 2008 წელს საქართველო მიმართ განხორციელებულმა კიბერშეტევებმა, რომლებიც რიგი ამერიკელი და ევროპელი ექსპერტების მიერ არის მოხსენიებული, როგორც კიბერომი თავისი საქმე გააკეთა .რამდენიმე საათიანმა სამთავრობო, მედიისა და კერძო სექტორის პარალიზებამ, რომელსაც პანიკა და ინფორმაციული ვაკუუმი უნდა გამოეწვია საქართველოში და საზოგადოებაში საქართველოს მთავრობას კიდევ ერთხელ დაანახა საინფორმაციო, კიბერსივცრის დაცვის აუცილებლობა და ის თუ რაოდენ დიდ ზეგავლენას ახდენს ეს ყოველივე ქვეყნის ეროვნულ უსაფრთხოებაზე.

ყოველივე ეს კი აისახა 2012 წლის ქვეყნის ეროვნული უსაფრთხოების კონცეფციაში, წამოწია წინ კიბერუსაფრთხოების პოლიტიკა და სახელმწიფოს მიერ ამ კუთხით გადასადგმელი ნაბიჯების განახლების აუცილებლობა. საქართველოს ეროვნული უსაფრთხოების კონცეფციის თანახმად, ქვეყნისათვის ეროვნული ღირებებულებს წარმოადგენს: ქვეყნის სუვერენიტეტი და ტერიტორიული მთლიანობა, თავისუფლება, დემოკრატია და კანონის უზენაესობა, უსაფრთხოება, კეთილდღეობა და მშვიდობა. (ეროვნული უსაფთხოების კონცეფცია; გვ: 7)

მნიშვნელოვანია, ყურადღება გავამახვილოთ თუ რა ადგილი უკავია ქვეყნის ეროვნული უსაფრთხოების კონცეფციაში კიბერსაფრთხეებსა და კიბერუსაფრთხოების პოლიტიკას. საქართველოს ეროვნული უსაფრთხოების კონცეფციის თანახმად , საქართველოსათვის უმნიშვნელოვანეს მიზანს წარმოადგენს იმგვარი კიბერპოლიტიკის შემუშავება, რომელიც უზრუნველყოფს ქვეყნის კიბერ სივრცის მაქსიმალურ დაცვასა და ძლიერი კომპიუტერული სისტემის შექნას.

კონცეფციის მეთორმეტე მუხლში ვკითხულობთ:

„ *საქართველოსთვის მეტად მნიშვნელოვანია ინფორმაციული სივრცის უსაფრთხოება და ელექტრონული ინფორმაციის დაცულობა. ინფორმაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად იზრდება მათზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულება. ამის გათვალისწინებით, დიდი მნიშვნელობა ენიჭება კიბერდანაშაულთან ბრძოლას და კიბერსივრცეში დივერსიული აქტებისგან თავდაცვას.*''

ეროვნული უსაფრთხოების კონცეფციის თანახმად კიბერუსაფრთხოების პოლიტიკის წარმოებისას, აუცილებელია როგორც საკანონმდებლო ბაზების მოწესრიგება, აგრეთვე ამ კუთხით საერთაშორისო თანამშრომლობა და აღებული საერთაშორისო ვალდებულებების შესრულება. ქვეყნისათვის პრიორიტეტულია კომპიუტერულ სისტემებში დაცული საიდუმლო დოკუმენტებისა და ინფორმაციის დაცულობის მაღალი ხარისხი. აქვე, ყურადღების გამახვილება უნდა მოვახდინოთ შემდეგ რამეზე, კერძოდ: ნატოც და ევროკავშირთან ასოცირების ხელშეკრულება საქართველოს ავალდებულებს დახვეწოს და გააუმჯობესოს/მოაწესრიგოს კიბერსივრცე და მასთან დაკავშირებული ყველა დეტალი იქნება ეს საკანონმდებლო ბაზა თუ ტექნოლოგიური შესაძლებლობები.

საქართველო 2012 წლიდან აქტიურად გადავიდა ელექტრონული მმართველობის რეჟიმზე. რაც გულისხმობს სხვადასხვა სახის ელექტონული ინფორმაციის განთავსებას კომპიუტერულ სისტემებში. აქ ჩვენ ვხვდებით სახელმწიფო საიდუმლო ინფორმაციის შემცველ დოკუმენტებს, რომლებიც სტრატეგიულად საომარი მოქმედებების დროს მეტად აუცილებელი და რიგ შემთხვევაში ტაქტიკურად სასიცოცხლოდ მნიშვნელოვანია. შესაბამისად : საქართველოსათვის კიბერუსაფრთხოების საკითხში ერთერთ მთავარ ამოცანას წარმოადგენს იმგვარი ინფრმაციული უსაფრთხოების სისტემის ჩამოყალბება, რომელიც უზრუნველყოფს ნებისმიერი სახისა და სიძლიერის კიბერშეტე-ვის/კიბერთავდასხმის მოგერიებას, ამასთანავე იმგვარი ტექნოლოგიურ/საკადრო ბაზის ქონას, რომელიც უზრუნველყოფს თავდასხმის შემთხვევაში რეაგირების უმოკლეს ვადებს და ზიანის აღმოფხვრას დროის უმოკლეს მონაკვეთში.

1.3. კიბერსაფრთხეების წარმოშობის წყაროები

როგორც ზემოთ ავღნიშნეთ კიბერსივრცემ შეიძლება სახელმწიფოს მოუტანოს, როგორც დადებითი ასვე უარყოფითი შედეგებიც. მისი მხრიდან მომდინარე საფრთხე დიდ ზიანს აყენებს, როგორც სახელმწიფოს, ასევე მის თითოეულ მოქალაქეს.

სახელისუფლებო ორგანოების პრიორიტეტულ საზრუნავს ქვეყნის ეროვნული უსაფრთხოებისა და კრიტიკული ობიექტებისა და ინფრასტუქტურის დაცვა წარმოადგენს. მათი მთავარი მიზანია ეს უკანასკნელნი არ გახდნენ სხვა სახელმწიფოების კიბერშეტევების მსხვერპლნი. თავიდან უნდა იქნას აცილებული ქვეყნის კიბერ სივრცეზე შეტევა, როგორც სხვა სახელმწიფოს სახელისუფლებო კიბერ რესურსების მქონე ინსტიტუტებისგან, ასევე არასახელმწიფო დაჯგუფებებისაგან, როგორებიცაა დაქირავებული ჰაკერები და ტერორისტული ორგანიზაციები. შესაბამისად, სახელმწიფო ორგანოების მიზანია მათ მიერ არიდებულ იქნას კომპიუტერული სისტემებიდან ინფორმაციის მოპარვა, ქსელის წყობიდან გამოყვანა; მათი მოვალეობაა სატელეკომუნიკაციო/ ელექტრომომარაგების, საფინანსო/ჯან-დაცვის, სატრანსპორტო/საზოგადოებრივი სისტემების დაცვა კიბერთავდასხმებისგან. თუმცა, ყველაფერი ასე მარტივი როდია. კიბერდანაშაულთან ბრძოლის დროს ყველაზე რთული ამოცანა გახლავთ დავადგინოთ თუ კონკრეტულად რომელი ქვეყანა ან დამნაშავეთა ჯგუფი იყო კიბერთავდასხმის ინიციატორი. კიბერსივრცეში შესაძლებელია დაიმალოს არ მარტო კიბრშეტევის ორგანიზების ადგილი, არამედ კიბერდამნაშავემ შესაძლოა დააფიქსიროს აბსოლუტურად სხვა დომენი, სხვა ქსელი და ამავდროულად იგი დარჩეს ანონიმური. შესაბამისად, განვიხილოთ ის ოფიციალური და არაოფიციალური სუბიექტები, რომლებიც კიბერ საფრთხეს წარმოადგენენ სახელმწიფო უსაფრთხოებისათვის:

სახელმწიფო(ები): ხშირ შემთხვევაში კიბერ თავდამსხმელი შეიძლება იყოს კონკრეტული სახელმწიფო, რომელიც საკუთარ კიბერრესურსებს იყენბეს ინფორმაციის შეგროვებისა და ჯაშუშობისათვის. ქმედებები შეიძლება იქნას განხორციელებული, როგორც მოკავშირე, ასევე მტერი სახელმწიფოს მიმართ. ამგვარი კიბერ ქმედებების მთავარ მიზანს წარმოადგენს პოტენციური მოწინააღმდეგის დაშინება ან კიბერ ომის წამოწყება. თუმცაღა, სახელმწიფოზე თავდასხმა არ გულისხმობს მხოლოდამხოლოდ სახელმწიფო სტრუქტურების ინსტიტუტების მუშაობის შეფერხებას, ბლოკირებას, პარალიზებას. თავდამსხმელი სახელმწიფო ახდენს მსხვერპლი სახელმწიფოს მოქალაქეების პირადი ინფორმაციის მოპარვას , მათ კლონირებას. არსებული უკანონოდ მოპოვებული ინფორმაციის საფუძველზე, მას

შეუძლია კონკრეტული მოქალაქეებზე სხვადასხვა სახის ფსიქოლოგიური ზეწოლის განხორციელება. მსოფლიო სახელმწიფო კიბერ გიგანტებს წარმოადგენენ: რუსეთი, ამერიკის შეერთებული შტატები, ირანი, ჩინეთი, ისრაელი. ჩვენი რეგიონის შემთხვევაში საქართველოსათვის საფრთხის შემცველ სახელმწიფოებს წარმოადგენენ: რუსეთი და ირანი.

რუსეთი: საქართველოს შემთხვევაში კიბერ საფრთხის შემცველ ნომერ პირველ სახელმწიფოს მისი ჩრდილოელი მეზობელი რუსეთის ფედერაცია წარმოადგენს. ამაზეა საუბარი, როგორც საქართველოს ეროვნული უსაფრთხოების კონცეფციაში, აგრეთვე საქართველოს კიბერუსაფრთხოების სტრატეგიაშიც. ამასთანავე, რუსეთი არასოდეს იშურებდა საკუთარ კიბერძალებს, რათა საკუთარი გეოპოლიტიკური ინტერესებისათვის გამოეყენებინა საკუთარი კიბერშესაძლებლოებები. ამის დაასტურს კი 2008 წლის რუსეთ-საქართველოს ომი წარმოადგენს.

2008 წლის რუსეთ-საქართველოს საომარი მოქმედებების დროს საქართველო რუსეთის მხრიდან კიბერ შეტევის მსხვერპლი გახდა. კიბერშეტევების შედეგად რამდენიმე საათით გაითიშა, როგორც სამთავრობო/სახელმწიფო სექტორის, ასევე საინფორმაციო სააგენტოების ვებ-გვერდები. განხორციელებული კიბერ შეტევების მთავრ მიზანს წარმოადგენდა ქვეყანაში შიშის, პანიკისა და უიმედობის დათესვა. კიბერ შეტევის დროს რუსეთის მხრიდან საქართველოს ვებ-გვერდებზე ხდებოდა დიდი რაოდენობით ქსელური პაკეტების გადმომისამართება და შეტევების განხორციელება , რამაც საბოლოოდ გამოიწვია არხების გადავსება და მათი რამდენიმე საათიანი მწყობრიდან გამოსვლა. საქართველოს ინფრასრტუქტურა და ადამიანური რესურსი არ აღმოჩნდა ძლიერი მოეგერიებინა კიბერ სივრცეში მიმდინარე შეტევები. საბოლოოდ პოლონელი სპეციალისტების დახმარებით მოხდა დიდი რაოდენობის ქსელური პაკეტების გადაგდება სხვადასხვა სერვერებზე. საინტერესოა, ისიც, რომ კიბერ თავდასხმის პარალელურად რუსეთის მიერ შექნილ იქნა ვებ-გვერდი Stopgeorgia.ru ,სადაც ნებისმიერ მსურველს შეეძლო მარტივად და რაც მთავარია სწრაფად ესწავლა თუ როგორ არის შესაძლებელი ქართული ვებ-გვერდების დაჰაკვა. ამასთანავე, ვებ-გვერდზე ჩამოთვლილი იყო ყველა ის კრიტიკული ობიექტების სია, რომელთა გამართული მუშაობა ქვეყნის ეროვნული უსაფრთხოების საწინდარია.

(ინფორმაციული უსაფრთხოებისა და ანალიზის ცენტრი- „ 2008-2010 წლის კიბერ-რეპორტი“)

რუსეთის მხრიდან კიბერშპიონაჟს ჰქონდა ადგილი 2011-2012 წლებში განხორციელებული კიბერ შეტევის GeorBot –ის ფარგლებში. რუსმა ჰაკერებმა დააინფიცირეს ის ქართული საინფორმაციო ვებ-გვერდები,სადაც განთავსებული იყო ინფორმაცია ნატო-ს დელეგაციის ვიზიტების, სამხედრო სიახლეების, ამერიკასთან ურთიერთობის შესახებ. მომხმარებელი,რომელიც ხსნიდა აღნიშნულ ვებ-გვერდებს ინფორმაციის მიღების მიზნით,ავტომატურად აინფიცირებდა მის კომპიუტერს ვირუსით.

შედეგად დაინფიცირებული კომპიუტერულ სისტემაში შეღწევის შემდეგ ვირუსი ავტომატურად ეძებდა იმ ფაილებს, რომელიც შეიცავდა სიტყვათა კომბინაციას (სამხედრო,საიდუმლო და ა.შ) , შედეგად ინფორმაციის გადაწერა ხდებოდა ვირუსის გამშვები პირის კოპიუტერზე. გროვდებოდა ყველა ინფორმაცია,რომელიც ეხებოდა საქართველო-ა.შ.შ-ს; სქართველო-ნატოსა და ევროკავშირს შორის არსებულ თანამშრომლობას. (ცნობილი კიბერშეტევების მაგალითები.)

ამერიკული ოგრანიზაციის კვლევის სტატისტიკის თანახმად, 2008-2014 წლებში საქართველო არაერთხელ გამხდარა სხვადასხვა სახის კიბერ შეტევების მსხვერპლი,რუსეთის მხრიდან. კიბერშეტევები ხორციელდებოდა საქართველოს შინაგან და საგარეო საქმეთა სამინისტროებზე. (FireEye; 2014)

ის, რომ რუსეთის კიბერშესაძლებლობები დიდია ამაზე არავინ დაობს : ამას უზრუნველყოფს, რუსეთის როგორც ფინანსური, ასევე ტექნოლოგიური/ადამიანური რესურსები. რუსეთის კიბერ განყოფილება კონტროლდება უმაღლესი სამხედრო განყოფილებებისა და აღმასრულებელი ხელისუფლების მიერ. ამასთანავე, რუსი ჰაკერები მსოფლიოში ერთერთ მოწინავე კიბერ ძალას წარმოადგენენ. რუსეთის ფედერაციის ბიუჯეტიდან გამოიყოფა დიდი რაოდენობით თანხები, რათა მოხდეს კიბერშესაძლებლობების კიდევ უფრო მეტად გაძლიერება. ბოლო დროს ბევრს საუბრობენ იმ ფაქტზეც, რომ გასული წლის 2016 წლის აშშ-ს საპრეზიდენტო არჩევნებზე ზეგავლენა სწორედ, რომ რუსმა ჰაკერებმა მოახდინეს.

ირანი: გარდა რუსეთისა, რეგიონის კიბერ გიგანტს წარმოადგენს ირანიც. ირანს ჰყავს მსოფლიოში ერთერთი უდიდესი კიბერარმია, კიბერპოლიცია. ჰაკერთა ჯგუფები, რომლებიც ემსახურებიან ირანის უმაღლეს აღმასრულებელ ხელისუფლებას. ისინი სახელმწიფოს დაკვეთით ასრულებენ კიბერდავალებებს, რომელთა მიზანი სხვადასხვაგავარია. შეიძლება ეს იყოს პროპაგანდისტული,დამაშინებელი, იდეოლოგიური და ა.შ. ამასთანავე, აღსანიშნავია ის ფაქტიც, რომ რუსეთის მსაგავსად მისი დაფინანსება ხდება სახელმწიფო უწყებებიდან.

რუსეთისგან განსხვავებით საქართველოს ირანთან არ ჰქონია კიბერ დაპირისპირების გამოცდილება. მიუხედავად ამისა, ირანმა მაინც განახორციელა „უწყინარი“ თავდასხმა საქართველოზე, როდესაც 2013 წელს, რამდენიმე კვირაში ზედიზედ ორჯერ შეუტია საქართველოს პარლამენტის ოფიციალურ ვებ-გვერდს.

ჰაკერები: არის კომპიუტერული დამნაშავე,რომელიც შესაძლოა მოქმედებდეს დამოუკიდებლად, ასევე მოქმედებდეს როგორც დაქირავებული სპეციალისტი, რომელსაც ქირაობენ, როგორც სახელმწიფოები, ასევე კორპორაციები და ტერორისტული ორგანიზაციები. ისინი ახორციელებენ კიბერშპიონაჟს, კიბერ შეტევებს, ავრცელებენ კონკრეტული სახის ინფორმაციას,რომელიც შესაძლოა იყოს, როგორც იდეოლოგიური, პორპაგანდისტული,ასევე რელიგიური ხასიათის მქონეც. კიბერ ომის შემთხევაში ისინი გამოყენებულნი არიან ,როგორც კიბერ ჯარისკაცები. ჰაკერები, შეიძლება იყვნენ დამოუკიდებელნი, ასევე ისინი შეიძლება იყვნენ დამოკიდებულებიც ანუ ხდებოდეს მათი მოქმედებებისა და მიზნების კონტროლი, ეს უკანასკნელნი მუშაობენ სახელმწიფო უწყებებში და ასრულებენ სახელმწიფო უწყების მიერ გაცემულ ბრძანებებს. IDI (Internet Development Initiative) წარდგენილი ანგარიშის თანახმად („საქართველოზე განხორციელებული კიბერ შეტევები“) :

2015 წლის 10 იანვარს ისლამურმა ჰაკერულმა დაჯგუფება „ახლო აღმოსა-ვლეთის კიბერარმია“ განახორციელა კიბერ თავდასხმა „კარფურის“ ქართული ფილიალის ვებ-გვერდზე.

ამავე წლის 16 აპრილს კი მეორე ისლამურმა ჰაკერულმა დაჯგუფება„ ელ მოჰაჯირმა“ მოახდინა „საქართველოს მოსამართლეთა ერთობის“ ვებ-გვერდზე კიბერთავდასხმა. მიზანი სახელდება,როგორც პროპაგანდისტული.

2015 წლის 6 ივლისს ISIS ჰაკერული ჯგუფის კიბერშეტევის მხვერპლი გახდა საქართველოს სახელმწიფო აპარატის ევროპულ და ევროატლანტიკურ სტუქტურებში ინტეგრაციის საკითხების ვებ-გვერდი.

ტერორისტები: მათი კიბერ შეტევების მთავარ მიზანს არეულობის, შიშისა და პანიკის დათესვა წარმოადგენს. სათქმელის მიტანა კონკრეტულ აუდიტორიამდე, მათზე ფსიქოლოგიური ზეგავლენის მოხდენის მიზნით. ამ შემთხვევაშიც მათ კიბერ შეტევებს შესაძლოა ჰქონდეს, როგორც იდეოლოგიურ-პროპაგანდისტული, ასევე რელიგიური სარჩულიც. ნებისმიერ შემთხვევაში ისინი სახელმწიფო უსაფრთხოებისათვის დიდი საფრთხის შემცველნი არიან.

საქართველოს შემთხვევაში გამოსაყოფია ტერორისტული ორგანიზაცია „ისალმური სახელმწიფო“ . „ისლამურ სახელმწიფოზე“ არის საუბარი ქვეყნის 2017 -2018 წლების კიბერუსაფრთხოების სტრატეგიაშიც და იგი მოხსენიებულია, როგორც საფრთხის შემცველი ერთერთი კიბერ სუბიექტი. 2015 წლის ნოემბერში მათ მიერ გავრცელებულ იქნა ვიდეო, სადაც ტერორისტული დაჯგუფების წევრები მიმართვდნენ ქართველ ხალხს. ეს ვიდეო კონკრეტულად ემუქრებოდა ქვეყნის სტაბილურობასა და საქართველოს სახელმწიფოს ეროვნულ უსაფრთხოებას.

2015 წელი ყველაზე მეტად დახუნძლული აღმოჩნდა კიბერ შეტევების კუთხით, რომელიც უშუალოდ ხორციელდებოდა საქართველოს სამთავრობო უწყებებზე: IDI (Internet Development Initiative) წარდგენილი ანგარიშის თანახმად („საქართველოზე განხორციელებული კიბერ შეტევები“)

2014 წლის 21 დეკემბერს კიბერ შეტევის მსხვერპლი გახდა საქართველოს სოფლის მეურნეობის სამინისტრო.

19 იანვარი კიბერ თავდასხმა დიასპორის საკითხებში სახელმწიფო მინისტრის აპარატის ვებ-გვერდზე.

2 თებერვალი დავირუსებული ელექტრონული წერილები,რომლებსაც ასევე იღებენ სახელმწიფო სექტორის წარმომადგენლები. ელექტრონული წერილები შედგენილი იყო სხვადასხვა ენებზე. შინაარსის მთავარ მიზანს წარმოადგენდა მსხვერპლისათვის ეცნობებინა, რომ მას გადაერიცხა თანხა კონკრეტულ ანგარიშზე,

წინააღმდეგ შემთხვევაში 96 საათის განმავლობაში დაინფიცირებული კომპიუტერულ სისტემაში არსებული ფაილი(ები) სამუდამოდ განადგურდებოდა.

5 თებერვალი კიბერ შეტევა განხორციელდა საქართველოს საგრეო საქმეთა სამინისტროზე. მიუხედავად, კიბერ სპეციალისტების აქტიური მუშაობისა მაინც ვერ მოხერხდა დადგენილიყო წყარო, საიდან მომდინარეობდა კიბერშეტევის განხორციელება.

თავი 2. საქართველოს კიბერუსაფრთხოება და მისი სუბიექტები

2008 წლის აგვისტოს რუსეთ-საქართველოს ომის დროს რუსეთის მხრიდან განხორციელებული კიბერ შეტევების შემდეგ, საქართველოს სახელმწიფომ დიდი მონდომებით დაიწყო საკუთარი კიბერ სივრცის გაძლიერება. ელ-მმართველობაზე გადასვლის პარალელურად სულ უფრო მეტად საჭირო ხდებოდა ქვეყნის კიბერსივრცის გაძლიერება, რათა თავიდან ყოფილიყო არიდებული კიბერ შეტევების შედეგად ქვეყნის ეროვნული უსაფრთოხებისათვის მნიშვნლოვანი ინფორმაციის გადინება. საქართველოში დღესდღეობით არსებობენ სუბიექტები,რომლებიც უზრუნველყოფენ საქართველოს სახელმწიფოს კიბერ სივრცის დაცვას, კიბერ სივრცეში მომხდარ ინციდენტებზე რეაგირებას , კიბერ შეტევების აღკვეთას და ა.შ.

შესაბამისად, ამ თავში საუბარი იქნება იმ სუბიექტებზე, რომლებიც ახორციელებენ აღნიშნულ სამუშაოს. აღნიშნული სუბიექტები ექვემდებარებიან სხვადასხვა სამინისტორებს, კერძოდ: იუსტიციის, თავდაცვისა და შინაგან საქმეთა სამინისტროებს. ფუნქციები, რომლებიც მათთვის არის მინიჭებული განსხვავებულია, თუმცა ყოველი მათგანი უმნიშვნელოვანესია ქვეყნის ეროვნული უსაფრთხოებისა და ძლიერი კიბერპოლიტიკსათვის.

2.1. მონაცემთა გაცვლის სააგენტო

იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი – მონაცემთა გაცვლის სააგენტო 2010 წელს შეიქმნა.მის მთავარ მიზანს წარმოადგენს სახელმწიფო ხელისუფლების განხორციელებისას ელექტრონული მმართველობის პრინციპებზე დაფუძნებული ერთიანი სისტემის შექმნა, ინფორმაციული ტექნოლოგიების (სისტემების) და, რაც მთავარია, ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა. მნიშვნელოვანია ყურადღება გავამახვილოთ იმაზე, რომ სააგენტოს უფლებამოსლება ინფორმაციული უსაფრთხოების საკითხებში ვრცელდება მხოლოდამხოლოდ საჯარო სექტორსა და კრიტიკულ ინფრასტრუტურაზე.

სწორედ ამ სააგენტოს ბაზაზე შეიქმნა 2011 წლის იანვარში კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფი (CERT.GOV.GE) .

ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას,ასევე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ სხვა ,მასთან დაკავშირებულ საქმიანობას,რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება,ახორციელებს მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინიდენტებზე დახმარების ჯგუფი CERT.GOV.GE (კანონი „ინფორმაციული უსაფრთხოების შესახებ“, თავი III; მუხლი 8;)

კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფის (CERT.GOV.GE) მთავარ მიზანს წარმოადგენს რეაგირება მოახდინოს საქართველოს სამთავრობო და კრიტიკული ინფრასტრუქტურის სექტორში დაფიქსირებულ ინციდენტებზე. იქიდან გამომდინარე, რომ საქართველოში არ არსებობს კომპიუტერულ ინციდენტებზე რეაგირების ნაციონალური ჯგუფი აღნიშნული სამუშაოს სწორედ ეს ჯგუფი ახორციელებს. იგი იკვლევს საქართველოს სახელმწიფოში მომხდარ ყველა კომპიუტერულ ინციდენტს, რეაგირების შემდეგ იგი ახდენს მის ანალიზს და გასცემს შესაბამის რეკომენდაციებს. ამ ჯგუფის არსებობა ,თავისთავად უზრუნველყოფს კიბერ ინციდენტების რაოდენობის კლებას.

CERT.GOV.GE ახდენს:

- გაფრთხილებებსა და შეტყობინებებს;
- ინციდენტებთან გამკლავებას;
- უსაფრთხოების აუდიტსა და სისუსტეების შეფასებას;
- საგანმანათლებლო ტრენინგებსა და სამუშაო შეხვედრებს;
- IDS სისტემების გამართვას.

2.2. საქართველოს კიბერუსაფრთხოების ბიურო

საქართველოს კიბერუსაფრთხოების ბიურო,თავდაცვის სამინისტროს დაქვემ-დებარებაში მყოფი უწყებაა, რომელიც 2014 წელს შეიქმნა. ბიუროს მთავარ მიზანს წარმოადგენს საქართველოს თავდაცვის სამინისტროს სამოქალაქო ოფისის

შეიარაღებული ძალების გენერალური შტაბის სტრუქტურული ქვედანაყოფებისა და სამინისტროში შემავალი საჯარო სამართლის იურიდიული პირებისათვის ინფორმაციული და და კომუნიკაციების ტექნოლოგიების სტაბილური , ეფექტური და უსაფრთხო სისტემების შექმნა და გაძლიერება. სამხედრო ინფრასტრუქტურის წინააღმდეგ კიბერინციდენტების აღკვეთა და პრევენცია 24/7 ის რეჟიმში. ბიურო მჭიდროდ თანამშრომლობს სხვადასხვა უწყებებთან როგორ ეროვნულ, ასევე საერთაშორისო დონეზე. თანამშრომლობა მოიცავს,როგორც სამხედრო პერსონალის გადამზადებაში ხელშეწყობას კიბერუსაფრთხოების თანამედროვე სტანდარტების შესაბამისად ,ასევე არსებული გამოცდილების ურთიერთგაზიარებას. ყოველივე ამის უზრუნველოსაყოფად ბიურო საკუთარ დაქვემდებარებაში არსებული ინფრასტრუქტურის შესწავლას, უსაფრთხოების მექანიზმების დანერგვასა და მათ შემდგომ განვითარებას უზრუნველყოფს.

2.3.კიბერდანშაულთან ბრძოლის სამმართველო

საქართველოს სახელმწიფოს კიბერ სივრცეში წესრიგის დამყარება და კიბერ სივრცის უსაფრთხოება პრიორიტეტულია და მნიშვნელოვანია საქართველოს შინაგან საქმეთა სამინისტროსთვისაც. ითვალისწინებს რა იმას, რომ კიბერ დანაშაული სახელმწიფო უსაფრთხოებისათვის დიდ გამოწვევას წარმოადგენს, 2012 წლის დეკემბერში საქართველოს შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანშაულთან ბრძოლის სამმართველო. ამ ორგანოს ევალება კიბერ სივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენა, აღკვეთა და პრევენცია. გარდა, ამისა, შსს-ს საექსპერტო–კრიმინალისტიკური მთავარი სამმართველოს შემადგენლობაში ჩამოყა-ლიბდა კომპიუტერულ–ციფრული ექსპერტიზის ქვეგანყოფილება, რომელიც უშუალოდ ახორციელებს ციფრული მტკიცებულებების პირველად მოპყრობასა და მათ შემდგომ ექსპერტიზას.

ამასთანავე, 2015 წელს შინაგან საქმეთა სამინისტროში განხორციელებული რეფორმების შედეგად,მას გამოეყო ეროვნული უსაფრთხოებს განყოფილება,რომელიც ჩამოყალიბდა დამოუკიდებელ სამსახურად. კერძოდ - სახელმწიფო უსაფრთხოების სამსახურად. ამ უწყების მთავარ მიზანს წარმოადგენს კიბერ-სივრცეში ეროვნული უსაფრთხოებისათვის საფრთხის შემცველი კიბერ ინციდენტების გამოვლენა, მათი ანალიზი და შემგდომი აღკვეთა. სახელმწიფო უსაფრთხოების სამსახურს, აგრეთვე მოქმედი კანონმდებლობის თანახმად უფლება აქვს აწარმოოს ფარული საგამოძიებო საქმიანობა. ეს მისი ექსკლუზიური უფლებამოსილებაა.

თავი3. საქართველოს კიბერუსაფრთხოების პოლიტიკა და მისი გამოწვევები

3.1. კიბერუსაფრთხოების პოლიტიკა

როდესაც ვსაუბრობთ ქვეყნის კიბერპოლიტიკაზე აუცილებელია ყურადღება გავამახვილოთ იმაზეც თუ რას აკათებენ კონკრეტული კიბერ სივრცის დაცვაზე მომუშავე სუბიექტები და სახელწმიფო უწყებები, იმისათვის, რომ ქვეყანას გააჩნდეს ძლიერი კიბერ სივრცე. საბოლოოდ გატარებული რეფორმები, აქტიური კიბერ ქმედებები ზეგავლენას ახდენენ ქვეყნის კიბერ იმიჯზე,როგორც რეგიონალურ,ასევე მსოფლიო მასშტაბით. ძლიერი კიბერ პოლიტიკა საკუთარ თავში მოიაზრებს, როგორც ძლიერ ადამიანურ, ასევე ტექნოლოგიურ რესურსებს. ამისათვის კი აუცილებელია,რომ საქართველომ აქტიურად ითანამშრომლოს როგორც ეროვნულ, ასევე საერთაშორისო დონზეც.

2015 წლის მონაცემთა გაცვლის სააგენტოს მიერ გაკეთებული ანგარიშის თანახმად :

შეიქმნა სპეციალიზებული სახელმძღვანელოები კიბერ-ინციდენტებზე ,რომელიც მოიცავს: კიბერ-შეტევების სიმპტომების ანალიზს,მათზე რეაგირების გზების დასახვას. სახელმძღვანელო შეეხება ისეთ საინტერესო თემებს , როგორებიცაა : კიბერ-შანტაჟი, ინფორმაციის გაჟონვა, გარე და ინსაიდერული საფრთხეები.

დაინერგა DNS- სერვისების შემმოწმებელი სისტემა. DNS გააჩნია მნიშვნელოვანი ვებ-გვერდების სია. მისი ამოქმედების შედეგად, DNS სერვისის მუშაობის შედეგად ვებ მისამართების შემოწმება ჯერ ლოკალური სერვისის მიხედვით ,შემდეგ კი DNS სერვერების მიხედვით. ღია და ლოკლაური სერვერებს სორის განსხვავებული მონაცემების არსებობის შემთხვევაში, მაშინ სერვისი ელ-ფოსტის მეშვეობით აგზავნის შესაბამის შეტყობინებას ადრესატთან. მნიშვნელოვანი საიტების სიასი შედიან: სამთავრობო; საბანკო ვებ-გვერდები; სხვადასხვა სოციალური ქსელები.

განახლდა Check My IP -ი, რომლის მიზანს წარმოადგენს საქრთველოს მოქალქეების კუთვნილი კომპიუტერებში მავნე კოდების აღმოჩენა და მათი

გაუნვებელყოფას. პორტალი უფასოა და ხელმისაწვდომია საქართველოს მოქალაქეებისათვის.

CERT.GOV.GE – ის მიერ ქსელური უსაფრთხოების მოწყობილობის PRA NSI – 5100 სერიის ინსტალაციის შედეგად, შესაძლებელი ხდება მავნე პროგრამებისა და ჰაკერული შეტევების დაფიქსირება. მის მიერ გაანალიზებულ იქნა 11-მდე სამთავრობო ორგანიზაციის ქსელური ნაკადი; CERT.GOV.GE -მა აგრეთვე მოახდინა HONEYPOT სისტემის ინსტალირება, რომელიც უზრუნველყოფს, მის მეშვეობით შესაძლებელი იმის დაფიქსირება თუ ვინ ახორციელებს შეტევებს ქართიღ სამტვარობო კომპიტერულ ინფრასტრუქუტრაზე; CERT.GOV.GE -ის ნაყოფიერი მუშაობის შედეგად, მის ფარგლებში ხორციელდება დამატებითი, ახალი სერვისები: დომენების შემოწმების სისტემა;მავნე კოდის ანალიზიზს სისტემა ;შეტევების აღმოჩენნის სისტემა (HONEYPOT); დაემატა ახალი ტიპის სენსორი,პაკეტების ღრმა ანალიზი.

ამასთანავე აქტიურად ხდება კიბერ სპეციალისტებისა,სამთვარო და კერძო სექტორის გადამზადება,მათი პროფესიონალიზმის დონის ამღლების კუთხით,როგროც ეროვნულ ,ასევე საერთაშორისო დონეზე.მოხდა უსაფრთხოების მართვის სიტემის დანერგვა,2015 წელს საქართველოს სერვისების განვითარების სააგენტოსა და ეროვნულ ბანკში.

საქართველოში ყოველ წელს ტარდება, Cyber EXE Georgia - რომლის მთავარ მიზანს წარმოადგენს CERT.GOV.GE - ის საქმიანობის მიზნებისა და ამოცანების შესახებ ცნობიერების ამღლების კუთხით ინფროამციული ტექნოლოგიების სპეციალისტების საკომუნიკაციო ქსელის განვითარება და კრიზისულ სიტუაციებში კონტაქტების გამოყენების მექანიზმების ,მასსი მონაწილეობას ირებენ,როგორც ქართველი,ასვეე უცხოელი კიბერ სპეციალისტები.

OTRS,რომელიც წარმოადგენს კიბერ-ინციდენტების მართვის განახლებული სისტემის ცაშვება 2014 წლის ბოლოსათვის მოხდა,შდეეგად 2015 წელს 9 თვის განმავლობაში დაფიქსირდა 650 ინცდიენტი,რომლიდანაც 471 მოდიოდა კრიტიკული ინფროამციულ სისტემეების სუბიექტებში, კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფმა ყველა მათგანზე მოახდინა რეგირება და საწირო რეკომენდაციის მიცემა იმ

სუბიექტებისათვის,რომელნიც გახნდენ კიბერ-ინციდენტის მსხვერპლნი. (მონაცემთა გაცვლის სააგენტოს 2015 წლის წლიური ანგარიში)

2015 წლის 21-25 მაისს საქართველოს საფინანსო ორგანიზაციებზე განხორიელდა მასობრივი DDOS -შეტევა. სულ შეტეტვაში მონაწილეობას ირებდა 300,00 მდე უნიკლაური IP მისამართი,160 ქვეყნიდან,ამ სემტხვევაში საქართველოს არანაირი მნიშვნელოვანი ზარალი არ მიუღია. გამომდინარე იქიდან,რომ 2008 წლისგან გასხვავებით მისი კიბერ სისტემა მზად იყო შებრძოლებოდა ამგვრი მასშტაბურ შემოტევას (IDI – Intenet Development Initiative, „ საქართველოზე განხორციელებული კიბერშეტევები“ 2015; გვ: 2)

საინტერესოა შინაგან საქმეთა სამინისიტროს ოფიციალური სტატისტიკური მონაცემებით, ამ კუთხით კიბერ-სივრცეში დაფიქსირებული სხვადასხვა სახის წვრილმანი კიბერდანაშაულებების რიცხვის მატება აღინიშნება და ეს ერთგვარად ამ რგოლისათვის გამოწვევად რჩება. მაგალითისათვის 2014 წელთან , შედარებით 2015 წელს იანვარსა და აგვისტოში 11,11% ით მოიმატა კიბერდანაშაულთა რაოდენობამ. (შინაგან საქმეთა სამინისტრო, სტატისტიკა 2015 წლის იანვარ-აგვისტო) 2016-2017 წლებში კი 54-დან 90 - მდე გაიზარდა;

გარდა ეროვნული ქმედებებისა,რომელიც მიმართულია საქართველოს კიბერსივრცის გასაძლიერებლად, საქართველო აგრეთვე თანამშრომლობს საერთაშორისო დონეზე და მონაწილეობას იღებს სხვადასხვა აქტივობებსა თუ სწავლებებში, რომელიც ხელს უწყობს ქვეყნის კიბერსივრცის დაცულობის უზრუნველყოფას. საქართველოს კიბერუსაფრთხოების სფეროში მომუშავე სუბიექტები აქტიურად თანამშრომლობენ ესტონელ კოლეგებთან. ურთიერთობა თავდაცვის სამინისტრომ საკუთარი კიბერშესაძლებლობების განვითარების პოლიტიკის დახვეწისათვის ესტონეთთან 2013 წელს დაიწყო; ნატოს სამეკავშირეო ოფისის თაოსნობით(NLO) ესტონელმა ექსპერტებმა შეისწავლეს სამინისტროში არსებული მდგომარეობა. სწორედ ამ თანამშრომლობის შედეგად შეიქმნა „განვითარების დოკუმენტი“ (“Roadmap”), რომელმაც ხელი შეუწყო კიბერუსაფრთხო-ების ბიუროს დაარსებას. ამ ურთიერთობის შედეგად 2014 წლიდან მოყოლებული დღემდე ესტონური მხარის მიერ შემუშავებული ტრენინგების ფარგლებში, როგროც

სამთავრობო,ასევე კერძო სექტორის კიბერუსაფრთხოების სფეროში მომუშავე სპეციალისტები გადიან შესაბამისი უნარებისა და ცნობიერების ამაღლების ტრენინგებსა და კურსებს.

საქართველოსა და ა.შ.შ. შორის მჭიდრო და ყოვლისმომცველი ურთიერთობა კიბერუსაფრთხოების პოლიტიკის გაძლიერების კუთხით, 2015 წლიდან დაიწყო. FMF (Foreign Military Financed Program), რომელიც მოიცავს 5 წლიან სამოქმედო გეგმას, უზრუნველყოფს ამერიკელ და ქართველ კიბერ კოლეგებს შორის ინფორმაციის, ცოდნისა და გამოცდილების ურთიერთგაზიარებას. რაც ყველაზე მთავარია სამოქმედო გეგმის ფარგლებში ხდება ტექნოლოგიური და პროგრამული უზრუნველყოფა.

Locked Shields ორგანიზებულია ნატოს კოოპერაციული კიბერთავადაცვის ცენტირს მიერ, იგი ყოველწიურად ტარდება. მას ატარებს ნატოს კოოპერაციული სასწავლო ცენტრი (NATO CCDCOE) .

2015 წლიდან საქართველოს კიბერუსაფრთხოების ბიურო,მონაწილეობას ღებულობდა,როგორც სწავლების დამკვირვებელი სტატუსის მქონე ქვეყანა, 2017 წლიდან კი საქართველო ლიტვის დაჟინებული მოთხოვნითა და მხარდაჭერით უკვე როგორც სრულუფლებიანი წევრი ღებულობს სწავლებაში მონაწილეობას. Locked Shields სწავლების მიზანია კრიტიკულ ინფორმაციული სისტემების,ქსელებისა და სერვისების დაცულობის ამაღლება.

3.2. ევროპის საბჭოს კონვენცია „ კიბერდანაშაულის შესახებ“

ევროპის საბჭოს კონვენცია კიბერ დანაშაულის შესახებ, 2001 წლის 23 ნოემბრს იქნა მიღებული. ეს არის პირველი საერთაშორისო იურიდიული ხელშეკრულება ინტერნეტითა და სხვა კომპიუტერული ქსელებით ჩადენილი დანაშაულების შესახებ. მათ შორის ბავშვთა პორნოგრაფიის ჩათვლით.(Civil ენციკლოპედიური ლექსიკონი, 2004) ევროპის საბჭოს კონვეცნიის „კიბერდანაშაულის შესახებ” მთავარ მიზანს წარმოადგენს კიბერდანაშაულის წინააღმდეგ მისი ხელმომწერ სახელმწიფოებს შორის საერთო კრიმინალური პოლიტიკის გატარებას. იგი მიზანმიმართულია საზოგადოება

დაიცვას კიბერკრიმინალისაგან. ამასთანავე, კონვენცია მოუწოდეს ქვეყნებს ურთიერთანამშრომლობის გზით ებრძოლონ კიბერ-სფეროში არსებულ დანაშაულს. დოკუმენტი განსაზღვრავს კიბერ დანაშაულის სახეებს და ახდენს მათ კლასიფიცირებას. კონვენცია მოუწოდებს ქვეყნებს შექმნან ან დახვეწონ საკუთარი ნორმატიულ -საკანონმდებლო ბაზა, რათა მოხდეს ჩადენილი კიბერდანაშაულის სათანადო დასჯა. ამ კონვეცნიის მიხედვით ადგენენ კონვეცნიის ხელმომწერი ქვეყნები სისხლის სამართლის პასუხისმგებლობას კონკრეტულ კიბერ დანაშაულზე.

საქართველომ კონვენციის რატიფიცირება 2012 წელს მოახდინა. ამ კონვენციის რატიფიცირებით მან საკუთარ თავზე აიღო ვალდებულება მოაწესრიგოს /დახვეწოს საკუთარი საკანონმდებლო ბაზა. ამასთანავე, საქართველო ,როგორც კონვენციის მოთხოვნების ერთგული შემსრულებელი აქტიურად თანამშრომლობს, როგორც რეგიონალურ, ასევე საერთაშორისო დონეზე .

კონვენციის თანახმად შეტანილია ცვლილებები საქართველოს სისხლის სამართლის კოდექსშიც, რომლის თანახმადაც სისხლის სამართლებრივ დევნას იწვევს კიბერ დამანაშავის მიერ კომპიუტერულ სისტემაში(ებში) ჩადენილი რიგი ქმედებებისა. კერძოდ: საავტორო უფლებების დარღვევა, ბავშვთა პორნოგრაფიის გავრცელება. კომპიუტერული სისტემიდან (ებიდან) ინფორმაციის უკანონო მოპოვება, კომპიუტერულ სისტემებში უკანონო შეღწევა, უკანონოდ მოპოვებული ინფორმაციის უკანონო გამოყენება. (საქართველოს სისხლის სამართლის კოდექსი, XXXV თავი, მუხლი 284,285,286)

3.3. კანონი „ ინფორმაციული უსაფრთხოების შესახებ “

2012 წლის ივნისში საქართველოს პარლამენტის მიერ, დამტკიცებული იქნა საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“. კანონის „ინფორმაციული უსაფრთხოების შესახებ“ მთავარ მიზანს წარმოადგენს ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას. ამასთანავე, კანონი აწესებს უფლება-მოვალეობებს ინფორმაციული უსაფრთხოების

დაცვის სფეროში საჯარო და კერძო სექტორის წარმომადგენელთათვის. კანონი, ასევე განსაზღვრავს კიბერუსაფრთხოებაზე პასუხიმგებელ და მაკოორდინირებელ სახელმწიფოს უწყებას. ამ კანონისვე, საფუძველზე საქართველოს პრეზიდენტის ბრძანებულებით დაამტკიცდა „ კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხა“. პრეზიდენტის მიერ დამტკიცებულ ნუსხაში შედიან ყველა ის სუბიექტები/დაწესებულებები, რომელთა გამართული და დაცული ფუნქციონირება საქართველოს ეროვნული უსაფრთხოების საწინდარია. კანონი განსაზღვრავს სახელმწიფო კონტროლის მექანიზმებსაც. კანონი განმარტავს კიბერ სივრცესთან დაკავშირებულ ტერმინებს. მაგალითისათვის, კანონის მიხედვით:

კიბერ შეტევა : ქმედება, როდესაც ელექტრონული მოწყობილობა ან/და მასთან დაკავშირებული ქსელი ან სისტემა გამოიყენება კრიტიკულ ინფრომაციულ სისტემაში სემავალი სისტემების,ქონების ან ფუნქციების მთლიანობს დარღვევის ,შეფერხების ან განადგურების ან ინფრომაციის უკანონოდ მოპოვების გზით. (კანონი „ინფორმაციული უსაფრთხოების შესახებ“გვ:3)

გარდა კიბერ სივრცესთან დაკავშირებული ტერმინების განმარტებისა,როგორც ზემოთ ავღნიშნე კანონი აგრეთვე განსაზღვრავს კიბერუსაფრთხოებაზე პასუხისმგე-ბელ და მაკოორდინირებელ სახელმწიფო უწყებას. კანონის მიხედვით ეს არის იუსტიციის სამინისტროს დაქვემდებარებაში მყოფი 2010 წელს შექმნილი მონაცემთა გაცვლის სააგენტო ბაზაზე 2011 წელს შექმნილი კომპიუტერულ ინციდენტებზე სწაფი რეაგირების ჯგუფი. CERT. GOV.GE.

კანონი აგრეთვე, უზრუნველყოფს კიბერ სივრცეში და კიბერუსაფრთხოების სფეროში დასაქმებულთა უფლება - მოვალეობების განსაზღვრასა და დამტკიცებას. განსაზღვრულია კრიტიკული ინფორმაციული სისტემის სუბიექტის მხრიდან პასუხიმგებელი პირის განსაზღვრის აუცილებლობაც.

3.4. კიბერუსაფრთხოების გლობალური ინდექსი და საქართველო

გაერთიანებული ერების ორგანიზაციის სპეციალიზებული ორგანო - საერთაშორისო სატელეკომუნიკაციო კავშირი (ITU) 2 წელიწადში ერთხელ ადგენს კიბერუსაფრთხოების გლობალურ ინდექსს. ბოლო 2017 წლის კვლევის მონაცემებით საქართველომ მსოფლიოს 165 ქვეყანას შორის მე-8 ადგილზეა. ITU-ს კვლევა კვლევ 2015-17 წლების პერიოდს მოიცავს კიბერუსაფრთხოების თვალსაზრისით საქართველო აღიარებულია, როგორც მსოფლიოში ერთ-ერთი ყველაზე დაცული და უსაფრთხო ქვეყანა. კვლევაში ასევე აღნიშნულია ისიც,რომ საქართველო მნიშვნელოვან რეფორმებს, ატარებს ქვეყნის კიბერსივრცის დაცვის კუთხით,რაზეც რა თქმა უნდა მეტყველებს კიდეც მისი მოწინავე პოზიციები და მისი დაწინაურება გლობალური კვლევის ინდექსში. ამასთანავე, ქვეყანაში კიბერუსაფრთხოების მაღალი დონის მიღწევა და შემდგომ მისი შენარჩუნება/განვითარება კომპლექსური საკითხია და სხვადასხვა უწყების კოორდინირებულ მუშაობს მოითხოვს. საქართველო ისეთ ქვეყნებს უსწრებს,როგორებიცაა: კანადა, იაპონია. (ITU; Global Cybersecurity Index 2017)

ევროპული ქვეყნების რეიტინგის ჭრილში საქართველო ესტონეთის შემდეგ მეორე - მესამე ადგილს საფრანგეთთან ინაწილებს. 0.819 სარეიტინგო ქულით.

საქართველომ კვლევის ხუთივე კომპონენტში -საკანონმებლო ბაზა, ტექნიკური მზაობა, ორგანიზაციული მოწყობა, შესაძლებლობების განვითარება და თანამშრომლო-ბისათვის ღიაობა მაღალი შეფასება მიიღო, რამაც გამოიწვია აღნიშნული მაღალი ციფრული კოეფიციენტის მიღება და შესაბამისად მსოფლიო რეიტინგში მოწინავე პოზიციაზე ყოფნა. საერთაშორისო სატელეკომუნიკაციო კავშირის მიერ მომზადებული ინდექსის მიზანია გაზომოს მსოფლიოს სხვადასხვა ქვეყნის კიბერუსაფრთხოების უზრუნველყოფის დონე, შეიმუშაოს კონკრეტული რეკომენდაციები.რაც საკუთრივ ხელს უწყობს აღმოჩენილი სუსტი მხარეების აღმოფხვრას. კვლევის ერთ-ერთი მიზანია ხელი შეუწყოს სახელმწიფოებს შორის კიბერუსაფრთხოების პოლიტიკის გაძლიერების კუთხით ურთიერთთანამშრომლობის გაძლიერებას.

Annex 2 – GCI 2017 Score

Member State	Score	Global Rank
Singapore	0.925	1
United States of America	0.919	2
Malaysia	0.893	3
Oman	0.871	4
Estonia	0.846	5
Mauritius	0.830	6
Australia	0.824	7
Georgia	0.819	8
France	0.819	8
Canada	0.818	9
Russian Federation	0.788	10
Japan	0.786	11
Norway	0.786	11
United Kingdom	0.783	12
Republic of Korea	0.782	13
Egypt	0.772	14
Netherlands	0.760	15

3.5. საქართველოს კიბერ რეზერვი

მაშინ, როდესაც ვსაუბრობთ კიბერუსაფრთხოებაზე, კიბერომზე და კიბერთავდაცვაზე უმნიშვნელოვანესი ჩვენ ვხვდებით კონკრეტულ კომპიუტერულ სივრცეს,სადაც საბრძოლო ველი კომპიუტერული სივრცეა, ჯარისკაცი კი კიბერ ჯარისკაცი ანუ ადამიანი ,რომელიც კარგად ერკვევა IT საკითხებში და ფლობს შესაბამის ცოდნას. მსოფლიოს მრავალ ქვეყანაში, რომელთათვისაც კიბერუსაფრთხოების პოლიტიკა უმნიშვნელოვანესია დაკავებულნი არიან ქვეყნის კიბერ რეზერვის გაუმჯობესებითა და მისი განახლებით. მსოფლიოს მასშტაბით საკუთარი კიბერრეზერვი ჰყავს ა.შ.შ-ს, რუსეთს, ევროპულ ქვეყნებს, ირანს.

საქართველოში კიბერ რეზერვის შექმნის შესახებ საუბარი ქვეყნის თავდაცვის ყოფილმა მინისტრმა თინა ხიდაშელმა 2015 წლის დეკემბერში დაიწყო. კიბერ რეზერვის მნიშვნელობაზე საუბარი საქართველოს 2017-2018 წლების კიბერუსაფრთხოების ეროვნულ სტრატეგიაშიც. კიბერ რეზერვისტის ძირითად ფუნქციებს: კიბერსივრცის დაცვა, სახელმწიფო და კერძო ორგანიზაციებზე ჰაკერული თავდასხმების თავიდან აცილება წარმოადგენს. საინტერესოა ის ფაქტიც, რომ კადრების შერჩევა მოხდება სამოქალაქო, საბანკო, საჯარო და სხვადასხვა სექტორებში დასაქმებული ადამიანებისაგან. რეზერვისტების შერჩევისას ყურადღება მიექცევა არა ფიზიკურ პარამეტრებს, არამედ ინტელექტუალურ კომპონენტს. კიბერ რეზერვის რიგების დაკავება შეეძლებათ მათ ვისაც აქვს შესაბამისი განათლება ინფორმაციული ტექნოლოგიების სფეროში. მნიშვნელოვანია ის ფაქტორი,რომ საქართველო იქნება პირველი ქვეყანა სამხრეთ კავკასიის რეგიონში,რომელსაც ეყოლება საკუთარი კიბერ რეზერვი. ამგვარი წინსვლა ქვეყნისათვის უმნიშვნელოვანესია, რადგან ყოველივე ეს უზრუნველყოფს საქართველოს ეროვნული უსაფრთხოების გაძლიერებას.

დასკვნა

2008 წლის აგვისტოს რუსეთ - საქართველოს ომის დროს საქართველოს წინააღმდეგ რუსეთის ფედერაციის მიერ კიბერ შეტევის გამოყენებამ, ქვეყანას ძლიერი კიბერუსაფთხოების პოლიტიკის არსებობის საჭიროება დაანახა. ჩვენი ქვეყნის მიერ კიბერუსაფრთხოების სფეროს გაძლიერების კუთხით საქართველომ კოლოსალურად დიდი და რთული ნაბიჯები გადადგა. კვლევის შედეგად გამოვლინდა, რომ აუცილებელია საქართველოს ჰყავდეს ერთიანი ნაციონალური მაკოორდნირებელი სტრუქტურული ერთეული; კიდევ უფრო მეტად უნდა დაიხვეწოს საქართველოს საკანონმდებლო ბაზა, რომელიც შეეხება კრიტიკული ინფრასტრუქტურის სისტემებსა და საერთოდ კიბერპოლიტიკასთან დაკავშირებულ საკითხებს. ამასთანავე, აუცილებელია მაქსიმალურად მოხდეს საზოგადოების ცნობიერების ამაღლება კიბერუსაფრთოხების პოლიტიკის კუთხით. ძლიერი კიბერუსაფრთხოების პოლიტიკა ძლიერი ეროვნული უსაფრთხოების საწინდარია. ძლიერი კიბერუსაფრთხოების უზრუნველსაყოფად, აგრეთვე, აუცილებელია სახელმწიფო და კერძო სექტორს შორის ურთიერთთანამშრომლობა, სახელმწიფო სექტორებს შორის მჭიდრო ურთიერთკავშირი. როგორც ნაშრომში არის აღნიშნული ეროვნული უსაფრთხოება მოიცავს სახელმწიფოსათვის სასიცოცხლო ყველა სფეროს, სწორედ ამიტომ საჭიროა, კიდევ უფრო მეტად მკაფიოდ მოხდეს საქართველოს კიბერუსაფრთხოების წინააღმდეგ მიმართული საფრთხეების გამოკვეთა. ამასთანავე, 2008-2017 წლებში საქართველოს მიერ გატარებულმა სამართლებრივ-ნორმატიული რეფორმებმა, სხვადასხვა კიბერ უსაფრთხოების სფეროში მომუშავე სუბიექტების გაძლიერებითა და მასში განახლების პოლიტიკის გატარებით უზრუნველყო კვლევის აღნიშნულ წლებში საქართველოს ეროვნული უსაფრთხოების გაძლიერება და მისთვის ამ წლებში კიბერ სივრციდან მომავალი საფრთხეების აღმოფხვრა.

გამოყენებული ლიტერატურა

1. საქართველოს ეროვნული უსაფრთხოების კონცეფცია. იხილეთ: http://factcheck.ge/erovnuli-usaphrthkhoebis-kontsephtsia-2011.pdf. 2011წ. საქართველო,თბილისი.
2. საქართველოს კიბერუსაფრთხოების სტრატეგია, საქართველოს პრეზიდენტის ბრძანებულება N312, 2013 წლის 17 მაისი. საქართველო,თბილისი. იხილეთ: https://matsne.gov.ge/ka/document/view/1923932
3. საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული უსაფრთხოების სტრატეგია და სამოქმედო გეგმა. საქართველოს მთავრობის დადგენილება N14 13/01/2017.წ. საქართველო, თბილისი. იხილეთ: https://matsne.gov.ge/ka/document/view/3548407
4. საქართველოს სისხლის სამართლის კოდექსი. იხილეთ: https://matsne.gov.ge/ka/document/view/16426
5. „კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხა“.იხილეთ: https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1867646&lang=ge
6. ’’საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ.“ იხილეთ: https://matsne.gov.ge/ka/document/view/1679424
7. საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების პოლიტიკა . იხილეთ: www.csbd.gov.ge
8. https://www.fireeye.com/
9. საქართველოს იუსტიციის სამინისტრო,სსიპ „ მონაცემტა გაცვლის სააგენტო“ http://www.cert.gov.ge/
10. საჯარო სამართლის იურიდიული პირის-კიბერუსაფრთხოების ბიუროს დებულების დამტკიცების შესახებ, საქართველოს თავდაცვის მინისტრის ბრძანება№8; 2014წ. 6 თებერვალი. https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=2235212&lang=ge
11. ევროპის საბჭოს კონვენცია „კიბერდანაშაულის შესახებ“ - http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
12. << Global Cybersecurity Index 2017. >> იხილეთ: www.itu.int. ნანახია 8/06/2018
13. საქართველოს პარლამენტის ვებ-გვერდს ჰაკერებმა შეუტიეს-

HTTP://WWW.TABULA.GE/GE/STORY/78750-SAQARTVELOS-PARLAMENTIS-VEB-GVERDS-HAKEREBMA-SHEUTIES *ბოლო ნახვა.* 8/06/2018

14. ''ახალი გამოწვევა საქართველოს ინტერნეტ სივრცისთვის.“ IDI (Internet development Initiative) - http://indein.net/wp-content/uploads/2015/09/New-Challenges-for-Georgian-Cyber-Space.pdf
15. საქართველოს იუსტიციის სამინისტროს საჯარო სამართლის იურიდიული პირის-მონაცემთა გაცვლის სააგენტოს წლიური ანგარიში (2015). https://matsne.gov.ge/ka/document/view/3083950
16. საქართველოს სინაგან საქმეთა სამინისტროს სტატისტიკა. იხილეთ: http://police.ge/ge/useful-information/statistics/statistics1
17. *„Грузия создаст Киберрезерв“* - იხილეთ: https://digital.report/gruziya-sozdast-kiberarmiyu/
18. Castells, M. (1995). The Rise Of The Network Society. John Wiley&Sons,NY.
19. Leclair, J. Keeley, B. (2015) - Cybersecurity in our digital lives, Hudson Whiteman, USA, NY.
20. Tabansky, L. Israel, B. (2015) – Cybersecurity in Israel, Springer Cham, NY.
21. Cavelty, M. (2014) Cybersecurity in Switzeland, Springer Cham, NY.
22. Dalzier, M. (2014) –Introduction to US Cybersecurity Careers.Waltham, Elsevier, USA.

დანართი#1

Ivane Javakhishvili Tbilisi State University

Social and Political Science Faculty

Khatia Tchilava

Role of Cyber Security in Georgian National Security Policy: Analysis as at 2008-2017

Political Science course

The Master of work is implemented for obtaining the Master's Degree of Political Science

The course instructor: Professor Aleksandre Kukhianidze

Tbilisi

2018