საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

სალომე გუმბერიძე

ეროვნული უშიშროების თავისებურებანი ინფორმაციულ ეპოქაში

დოქტორის აკადემიური ხარისხის

მოსაპოვებლად წარდგენილი დისერტაციის

ა ვ ტ ო რ ე ფ ე რ ა ტ ი

სადოქტორო პროგრამა – საჯარო მმართველობა

შიფრი – 1109

თბილისი

2018 წელი

სამუშაო შესრულებულია საქართველოს ტექნიკური უნივერსიტეტის

ბიზნესტექნოლოგიების ფაკულტეტის

საჯარო მმართველობისა და ელექტრონული ბიზნესის დეპარტამენტში

სამეცნიერო ხელმძღვანელი: პროფესორი ოთარ ქოჩორაძე

რეცენზენტები:

დაცვა შედგება 2018 წლის —— ივლისს, —— საათზე

საქართველოს ტექნიკური უნივერსიტეტის ბიზნესტექნოლოგიების ფაკულტეტის სადისერტაციო საბჭოს კოლეგიის სხდომაზე, კორპუსი -----, აუდიტორია ---------

მისამართი: 0175, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ს ბიბლიოთეკაში,

ხოლო ავტორეფერატისა - სტუ-ს ვებგვერდზე.

სადისერტაციო საბჭოს მდივანი:

ასოცირებული პროფესორი,

Abstract

Aim of this dissertational work is to demonstrate how important protection of informational security and electronic information, newly conceptualizing dangers and problems standing before informational security, developing their solving ways and defining future action plan is for ensuring of national interests of the country.

The main aim of the theme is complex, systematic and structural estimation of the condition and tendencies of informational security of the country.

Text of dissertational work is made on 148 pages printed on the computer that consists of introduction, literature review, results made based on scientific research, done by the author, their discussing, conclusion and recommendations.

Actuality of the theme to be researched is discussed and the main aim and tasks, hypothesis, subject, object, innovation and research methodological and theoretical fundaments are given in the introduction of the dissertational work.

Analysis of the literature existing around the theme to be researched is given in the discussion of the literature, privately laws and conceptions existing about national security and informational safety is discussed. Cyber-safety of Germany, France, Great Britain, Finland and United State of America on existing strategies is discussed as well. Results of researches conducted by various international organizations are discussed.

Results and their judgment consists of the opinion of an author around the subject of scientific research, privately dangers and challenges towards informational security existing before Georgia are discussed, 2008 informational war against Georgia, protection mechanisms of informational security policy and critical informational infrastructure, development of relevant protection methods of informational security and working out of effective control mechanisms stipulating dangers and challenges existing before Georgia, cyber-security as the challenge of 21 century and the condition existing in Georgia towards this issue. Informational security policy of advanced countries in terms of international organizations and cyber-security is discussed as well.

Structured interviews with the specialists of beforehand selected informational security sphere and the employees of public services was represented as the instrument of research, sociological interview has been conducted

as well and information security subject defined under the law “on informational security” has been selected as research area.

The following recommendations are suggested in the dissertational work: to perform monitoring of Georgian online space by the country for revealing of foreign propagandist sources, to perform audit of informational technologies of that private sector, which owns critical informational infrastructure, to introduce study of cyber-security culture in educational institutions, to strengthen international relations with international organizations working in this sphere and state bodies, as well, to conduct some events for the purpose of raising of public consciousness.

National security problems in informational epoch are shortly given in conclusion, its solving methods are set up, and refining ways of the legislation are given as well. Opinion regarding sharing experience of various countries is suggested, as well, on the approach of the Georgian Government in relation of this problem, mutual collaboration between the state and private sector. According to above mentioned, we can discuss what effective steps may be made in relation of cyber-security for correction of the condition existing in Georgia.

For the aim of maximal decrease and avoiding dangers in cyber sphere, international organizations and abroad countries have started creation, development and refining process of organizational structural units, that is in direct relation with development of new technologies and increase of cyber crime. Their successful work has to ensure protection of cyber space and effectiveness of struggling with cyber crime. Actually institutionalism process is permanently going on and developing in the given sphere.

სადისერტაციო ნაშრომის ზოგადი დახასიათება

მსოფლიოში სახელმწიფოებს შორის გეოპოლიტიკურ მეტოქეობაში, პოლიტიკური გეგმების რეალიზაციაში მიმდინარეობსღია ძალისმიერი(ეკონომიკური, დიპლომატიური, სამხედრო) მეთოდებიდან და საშუალებებიდან ინფორმაციულ მეთოდებსა და საშუალებებზე გადასვლის ტენდენცია. სახელმწიფოს ეროვნული უშიშროების სისტემის უზრუნველყოფაში უმნიშვნელოვანესი ადგილი დაიკავა ინფორმაციულმა ფაქტორმა უკანასკნელი საუკუნის განმავლობაში.

ინფორმაცია კაცობრიობის დაუშრეტელ გლობალურ რესურსად იქცა, რამაც გამოიწვია ცივილიზაციის განვითარების სრულიად ახალი – ინფორმაციული რესურსის ინტენსიურად ათვისების ეპოქის დადგომა.ნებისმიერი სახელმწიფოს ეროვნულ უშიშროებაზე, ინფორმაცია სულ უფრო დიდ გავლენას ახდენს, ამიტომ მსოფლიოში მომხდარი ეს გლობალურ სოციალური ცვლილებები საზოგადოების ინფორმაციული გარემოს შესწავლასა და ობიექტურ ანალიზს მოითხოვს.

დღევანდელ სამყაროში საინფორმაციო და სატელეკომუნიკაციო ტექნოლოგიების განვითარების თანამდროვეტემპებმასაზოგადოების არსებობისათვის სრულიად ახალი პირობების შექმნა გამოიწვია. ჩვენთვის ცნობილია, რომ მოხდა რადიკალური, თვით რევოლუციური გადატრიალება ინფორმაციის სფეროში და ამან გამოიწვია ის, რომ ინფორმაცია განსაკუთრებულ როლის მატარებელია თანამედროვე სამყაროში. შესაბამისად შეგვიძლია ვივარაუდოთ, რომ მოსალოდნელია, ადამიანის ცხოვრების წესმა კარდინალური ცვლილებები განიცადოს.

თანამდროვე ცხოვრებაში უკვე წარმოუდგენელია პოლიტიკური, სოციალურ–ეკონომიკური და კულტურული ცხოვრების სფერო, სადაც პი-როვნების, საზოგადოებისა თუ სახელმწიფოს წინაშე მდგარი ამოცანების წ-არმატებულად და ეფექტიანად გადაწყვეტა მოხდეს გლობალურ საინფო-რმაციო სივრცეში საინფორმაციო ურთიერთქმედებების გამოუყენებლად.

საქართველო გარდამავალი ეკონომიკის განვითარებად ქვეყანათა რიგს მიეკუთვნება. გლობალიზაციის პირობებში, როდესაც ყალიბდება

გლობალური საინფორმაციო საზოგადოება, საქართველოს წარმატებული განვითარებისთვის საკმარისი აღარ იქნება ინდუსტრიული ეტაპის და სამოქალაქო საზოგადოების აღმშენებლობის კლასიკური თითქმის ასი წლის წინანდელი პოლიტიკური და სოციალურ–ეკონომიკური ლოზუნგების რეალიზაცია, შესაბამისი ამოცანების დასახვა და თუნდაც წარმატებული გადაწყვეტა. უფრო მეტიც: თუ საქართველო ვერ მოახერხებს საკუთარ შესაძლებლობათა სრულ მობილიზაციას საინფორმაციო საზოგადოების პოლიტიკურ, სოციალურ–ეკონომიკურ, ტექნოლოგიურ და კულტურულ წინაპირობათა შესაქმნელად, მას უახლოეს მომავალში ძალზე სერიოზული საფრთხე დაემუქრება. კერძოდ:

გლობალიზაციის პროცესის აქტიური იგნორირების და მისთვის წინააღმდეგობის გაწევის მცდელობის შემთხვევაში, მას ემუქრება სულ ცოტა პოლიტიკური, ეკონომიკური, ტექნოლოგიური და საინფორმაციო იზოლაცია, რაც უმოკლესი გზაა საქართველოს საბოლოო ეროვნული კატასტროფისაკენ.

საინფორმაციო გარემოს გარდაქმნის დღეს მიმდინარე სტიქიური, ქაოტური და უკონტროლო პროცესის კრიტიკულზე უფრო დიდ ხანს გაგრძელების შემთხვევაში - პოლიტიკურ, ეკონომიკურ, ტექნოლოგიურ და კულტურულ სფეროებში ძლიერ სახელმწიფოებზე ტოტალური დამოკიდებულების უაპელაციოდ აღიარება, ეროვნული სუვერენიტეტის ნებაყოფლობით დათმობას, საბოლოო ჯამში– თავისუფალი პერსპექტივის საბოლოო გაქრობამდე მიგვიყვანს.

ამგვარ საფრთხეთა თავიდან ასაცილებლად აუცილებელია გლობალიზაციის ეპოქისათვის ადეკვატური ეროვნული განვითარების სტრატეგიის შემუშავება, მიღება და სწრაფად განხორციელება.

საკვლევი თემის აქტუალობა. სახელმწიფოს განვითარებისა და აღმშნებლობის პროცესში ყოველთვის დგას ეროვნული უშიშროების უზრუნველყოფისა და მისი მართვის სრულყოფის ამოცანა. უშიშროების პრობლემა კაცობრიობის გადარჩენის გლობალურ პრობლემად იქცა, რადგანაც საერთაშორისო პოლიტიკურ და ეკონომიკურ ურთიერთობებში

ყალიბდება ახალი საფრთხეები და რისკები. ამ მხრივ გამონაკლისი არც საქართველოა, დღითიდღე იზრდება ეკონომიკური, სოციალური, პოლიტიკური, იფორმაციული და სხვა პრობლემების ნეგატიური გამოვლინებები, მათი ეფექტური გადაჭრა კი შეუძლებელია

ქვეყნის განვითარების სტრატეგიაში ჩადებული სახელმწიფოებრიობისა და საზოგადოებრივი მშენებლობის პრიორიტეტული მიმართულებები განსაზღვრავენ ეროვნული უშიშროების ერთიანი სისტემის კონკრეტულ შინაარსს. სახელმწიფოს ეროვნული უშიშროების სისტემის ფორმირება ხდება იმის გამო, რომ დაცული იყოს 1. პიროვნება, მისი უფლებები და თავისუფლებები; 2. სახელმწიფოს კონსტიტუციური წყობილობა, სუვერენიტეტი და ტერიტორიული მთლიანობა; 3. საზოგადოება, მისი მატერიალური და სულიერი ფასეულობები; თანამედროვე ეტაპზე ეროვნული უშიშროების ერთიან სისტემაში მოიაზრება მრავალი კომპონენტი: პოლიტიკური უშიშროება (შიდასახელმწიფოებრივ–პოლიტიკური უშიშროება, საგარეო–პოლიტიკური უშიშროება); ეკონომიკური უშიშროება, ენერგეტიკული უშიშროება, საინფორმაციო უშიშროება და ა.შ.

ინფორმაციული სისტემების გამართულად ფუნქციონირებაზე დიდი გავლენა აქვს ისეთ ფაქტორებს, როგორებიც არის პროგრამული და აპარატული უზრუნველყოფის მწყობრიდან გამოსვლა, ინტერნეტზე შეტევა, ფიზიკური ზემოქმედების შედეგად მიყენებული ზიანი და ადამიანის როგორც მომხმარებლის მიერ მუშაობის პროცესში დაშვებული შეცდომები. ზემოთ ჩამოთვლილ ფაქტორებზე დაყრდნობით, შეგვიძლია ვთქვათ თუ რამდენად არის დამოკიდებული დღევანდელი მსოფლიო საზოგადოება ინფორმაციული სისტემების გამართულ მუშაობაზე.

ინფორმაცია ისეთივე არსებითი აქტივია, როგორც საქმიანობის მართვის სხვა მნიშვნელოვანი აქტივები და მას შესაბამისი დაცვა სჭირდება. ეს საკითხი განსაკუთრებით აქტუალური ხდება ურთიერთდამოკიდებულ და დაკავშირებულ გარემოში, რასაც შედეგად მოსდევს სისუსტეებისა და საფრთხეების მზარდი რაოდენობის მიმართ ინფორმაციის დაუცველობა.[1]

თანამედროვე მსოფლიოს კიბერსივრცეში არებული და პოტენციური რისკები/საფრთხეები საზოგადოებრივი ცხოვრების რეალობად იქცა ტექნოლოგიების განვითარებასთან ერთად უფრო რთული ხდება აღნიშნული საფრთხეების პრევენცია და დაძლევა. საერთაშორისო სტატისტიკის მიხედვით წარმატებული კიბერ ინციდენტების რიცხვი ყოველწლიურად მატულობს და შესაბამისად იზრდება კიბერინციდენტებით გამოწვეული ზარალი.

საქართველოს სახელმწიფო დიდ მნიშვნელობას უნდა ანიჭებდეს ინფორმაციულ უშიშროებას და ელექტრონული ინფორმაციის დაცულობას რადგანაც ინფორმაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად იზრდება თანამედროვე ტექნოლოგიებზე სახელმწიფოს ფუნქციონირებისათვის აუცილებელი კრიტიკული ინფრასტრუქტურის დამოკიდებულება, შესაბამისად ქვეყნის ეროვნული ინტერესების უზრუნველყოფისათვის აუციელებელი ფაქტორია კიბერდანაშაულთან ბრძოლა და კიბერსივრცეში სახელმწიფოს კრიტიკულ ინფრასტრუქტურაზე დამაზიანებელი ტიპის თავდასხმების მოგერიება.

კვლევის მიზანი და ამოცანები. სადისერტაციო თემის კვლევის მიზანს წარმოადგენს ახალ გეოპოლიტიკურ პირობებში საქართველოს ინფორმაციული უშიშროების მდგომარეობისა და ტენდენციების, კომპლექსური, სისტემური და სტრუქტურულ – ფუნქციონალური შეფასება. საქართველოს საჯარო ვირტუალური სივრცის სპეციფიკური ინტერესების, ამოცანებისა და შესაძლებლობების, გზებისა და მექანიზმების უზრუნველყოფის დასაბუთება.

ახლებურად უნდა იქნას გააზრებული ინფორმაციული უშიშროების უზრუნველყოფის წინაშე მდგარი საფრთხეები და ჩამოყალიბდეს მოსაზრებები მის გადაწყვეტასთან მიმართებაში. მსოფლიოში ამჟამად მიმდინარე პროცესები – კომუნიკაციისა და ინფორმაციის უბნებზე რევოლუციური გარდაქმნები, მასობრივი კომპიუტერიზაცია, უახლესი საინფორმაციო ტექნოლოგიების დანერგვა და სრულყოფა მიუთითებს ცივილიზაციის არნახულ მასშტაბებსა და პერსპექტივებზე.

აგრეთვე საინტერესო საგანს წარმოადგენს საქართველოს სახელმწიფოს კიბერუშიშროების ამჟამინდელი სისტემის ფუნქციონირების თავისებურებების განხილვა, უმნიშვნელოვანესი საფრთხეებისა და გამოწვევების გამოკვეთა და მოქმედების სამომავლო გეგმის პრიორიტეტების განსაზღვრა.

ინფორმაციული უშიშროების უზურუნველყოფა არ შეიძლება იყოს ერთჯერადი აქტი. ეს არის უწყვეტი და თანმიმდევრული პროცესი, რომელიც მდგომარეობს ინფორმაციის დაცვის სისტემის დახვეწისა და განვითარებისათვის უფრო მიზანშეწონილი მეთოდებისა და გზების მოძიებაში, დამკვიდრებასა და რეალიზაციაში. დაცვის სისტემის არსებული მდგომარეობის განუწყვეტელ კონტროლში, სისუსტეების გამოვლენაში დ ა მათ ზე რეაგირების მოხდენაზე.

დღევანდელი მდგომარეობით სახელმწიფოები აქტიურად იყენებენ კიბერშეტევებს პოლიტიკური, გეოპოლიტიკური, სამხედრო და სხვა მიზნების განსახორციელებლად. თანამედროვე კიბერშეტევები საფრთხეს უქმნის ქვეყნის უშიშროებას, განვითარებას და ხელს უშლის საზოგადოების ფუნქციონირებას. 2008 წლის აგვისტოს ომმა ნათლად დაგვანახა, რომ საქართველო არ იყო შესაბამისად მომზადებული ინფორმაციული უშიშრობის კუთხით.

შესაბამისად გლობალური უსაფრთხოების უზრუნველყოფის ერთ–ერთი მთავარი კომპონენტი სწორედ საკუთარი ქვეყნის კიბერთავდაცვაა, რაც ისეთივე მნიშვნელოვანია, როგორც სახმელეთო, საჰაერო და საზღვაო სივრცეების დაცვა. თითოეული სახელმწიფო რომელიც ტექნოლოგიური განვითარებისაკენ მიისწრაფვის საზოგადოების წინაშე ვალდებულია დაიცვას საკუთარი კიბერსივრცე.

კვლევის ამოცანები: კვლევის ამოცანები განაპირობებენ დასახული მიზნის მიღწევას და მდგომარეობენ შემდეგში: 1.თანამედროვე პირობებში საქართველოს ეროვნული უსაფრთხოებისა და ინფორმაციული უშიშროების ურთიერთკავშირისა და ურთიერთგანპირობებულების გამოვლენა. 2. საზღვარგარეთის ქვეყნების გამოცდილების გაანალიზება და

სისტემატიზირება საქართველოს ვირტუალური საჯარო სივრცის ინფორმაციული უშიშროების ეფექტიანობის ამაღლებისათვის. 3.საქართველოს ინფორმაციული უშიშროების,როგორც ქვეყნის ეროვნული ინტერესების დაცვის სისტემის განუყოფელი შემადგენელი ელემენტის, პრიორიტეტებისა და პერსპექტივების გამოკვლევა.

კვლევის ჰიპოთეზა: თანამედროვე საინფორმაციო კომუნიკაციურმა ტექნოლოგიებმა, წარმოშვეს პრინციპულად ახალი სახის გამოწვევები, რისკები და საფრთხეები. დღევანდელ პირობებში, როდესაც საქართველომ აიღო კურსი მმართველობითი სისტემების რეფორმირებასა და მოდერნიზაციაზე პრიორიტეტულად იქნა მიჩნეული ელექტრონული მთავრობისა და ელექრონული მმართველობის დახვეწა და განვითარება, აუცილებელია ეროვნული უშიშროების ინფორმაციულ სფეროში არსებული საფრთხეებისა და გამოწვევების საგნობრივი შესწავლა.

კვლევის ობიექტს წარმოადგენს თანამედროვე პირობებში საქართველოს ინფორმაციული უშიშროების ინსტიტუციონალური ასპექტები.

კვლევის საგანია ახალი მოვლენები და ფაქტორები, რომლებიც განსაზღვრავენ ვირტუალურ საჯარო სივრცეში, საქართველოს ინფორმაციული უშიშროების მდგომარეობასა და ტენდენციებს.

კვლევის სიახლე განპირობებულია თანამედროვე საქართველოს ვირტუალურ საჯარო სივრცეში ახალი გამოწვევებისა და რისკების წარმოშობით.

კვლევის მეთოდოლოგიურ და თეორიულ საფუძველი კვლევის მეთოდოლოგიური საფუძველია ინსტიტუციონალური, სისტემური და სტრუქტურულ–ფუნქციონალური მეთოდები.

ინსტიტუციონალური მიდგომის საშუალებით შესწავლილია ნორმატიულ სამართლებრივი ბაზა და ის ძირითადი ინსტიტუტები, რომლებიც უზრუნველყოფენინფორმაციულ უშიშროებას.

სისტემურმა მიდგომამ საშუალება მოგვცა გაგვეაზრებინა კვლევის ობიექტი, როგორც სისტემა მისი სტრუქტურიდან, ელემენტებიდან, ფუნქციებიდან და მიზნებიდან გამომდინარე.

სტრუქტურულ–ფუნქციონალური მიდგომის ფარგლებში ინფორმაციული პოლიტიკა დახასიათებულია, როგორც ქმედებათა ლოგიკური სქემა, რომელიც მოიცავს მოქმედების სუბიექტს, მიზნებს, რესურსებს, ნორმებსა და ღირებულებებს. ასევე გამოყენებულია კონკრეტული სიტუაციის ანალიზის მეთოდი და დოკუმენტების ანალიზი.

კვლევის მეთოდოლოგიად კვლევაში დასახული მიზნების მისაღწევად განხორციელებული იქნა რაოდენობრივი და თვისებრივი კვლევები: 1. სოციოლოგიური გამოკითხვა.2. სტრუქტურირებული ინტერვიუები წინასწარ შერჩეულ საინფორმაციო უშიშროების დარგის სპეციალისტებთან და ექსპერტებთან, ასევე საჯარო მოხელეებთან. სოციოლოგიური გამოკითხვის კვლევის არეალად შერჩეული იქნა „ინფორმაციული უსაფრთხოების შესახებ კანონი“– ის მიხედვით განსაზღვრული ინფორმაციული უსაფრთხოების სუბიექტები.

სისტემური ანალიზის გარეშე წარმოუდგენელია სახელმწიფოებრივი, და პოლიტიკურისაკითხების სათანადო დონეზე გადაწყვეტა, აღნიშნული გარემოება განსაკუთრებით დიდ დატვირთვას ეროვნული უშიშროების უზრუნველყოფაში იძენს, ვინაიდან საინფორმაციო საზოგადოების ეპოქაშიაშკარადგამოკვეთილია ინფორმაციული ასპექტების გადამწყვეტი როლი. თანამედროვე ინფორმაციული სისტემების დაცვას, ასევე კრიტიკული ინფორმაციული სუბიექტების დაცვას ინფორმაციულ უზრუნველყოფაში უმნიშვნელოვანესი ადგილი უნდა ეჭიროს ამ მიმართულებით ეფექტურ საქმიანობას განხორციელება,მხოლოდ სისტემური მიდგომით არის შესაძლებელი, რომ მთლიანობაში დავინახოთ არსებული მდგომარეობა.

გლობალიზაციის პერსპექტივის და ინფორმაციული ეპოქის ჩამოყალიბების ტენდენციების ფონზე, როდესაც კაცობრიობის განვითარების პროცესის დომინანტი ინფორმაცია ხდება, საქართველოს

სახელმწიფოს განსაკუთრებული ყურადღების საგანი უნდა გახდეს საინფორმაციო სივრცის ფორმირებისა და შესაბამისი თანამედროვე ტექნოლოგიური საშუალებების განვითარების პრობლემა.

აგრეთვე სახელმწიფო მმართველობის კომპლექსური მრავალგანზომილებიანი ამოცანისსაინფორმაციო პოლიტიკის რეალიზაციის პრობლემა, რომელიც მოიცავს ნორმატიულ-სამართლებრივ, ორგანიზაციულ-ტექნოლოგიურ, სოციალურ, ტექნიკურ ეკონომიკურ, და საგანამანათლებლო კომპონენტებს

სადისერტაციო ნაშრომი შესაძლებელიასაფუძვლად დაედოს მონოგრაფიას. ჩვენ მიერ შემუშავებული დასკვნები და რეკომენდაციები შესაძლებელია გამოყენებული იქნეს სახელმწიფო ხელისუფლების, პოლი-ტიკური პარტიებისა და საზოგადოებრივი ორგანიზაციების მუშაობის პროცესში ეროვნული უშიშროების უზრუნველყოფაში კიბერუშიშროების უზრუნველყოფისათვის მეცნიერულად დასაბუთებული ახალი მექანიზმის შემუშავების კუთხით.

სადისერტაციო ნაშრომის სტრუქტურა და ოდენობა. სადისერტაციო ნაშრომი შედგება შესავლის, 3 თავისა და 8 ქვეთავისაგან, დასკვნებისა და ლიტერატურის სიისაგან. ნაშრომი მოიცავს 148 გვერდს.

სადისერტაციო ნაშრომის ზოგადი შინაარსი

შესავალი
ლიტერატურის მიმოხილვა
შედეგები და მათი განსჯა
თავი I. საქართველოს წინაშე არსებული საფრთხეები და გამოწვევები ინფორმაციული უშიშროების კუთხით
1.1
რა არის ინფორმაციული უშიშროება
1.2
2008 წლის ინფორმაციული ომი საქართველოს წინააღმდეგ
1.3 ინტერნეტსივრცე, როგორცსადაზვერვოსაქმიანობის მნიშვნელოვანი ობიექტი

თავი II. საქართველოს წინაშე არსებული საფრთხეებისა და გამოწვევების გათვალისწინებით ინფორმაციული უშიშროების დაცვის

სათანადო მეთოდების დანერგვისა და ეფექტიანი კონტროლის მექანიზმების შემუშავება

2.1 საქართველოს ინფორმაციული უშიშროების პოლიტიკა

2.2 სახელმწიფოს კრიტიკული ინფორმაციული ინფრასტრუქტურა და მისი

დაცვისმექანიზმები

2.3. ინფორმაციული უშიშროება საჯარო სამსახურებში

2.4. საერთაშორისო ორგანიზაციებისა და საზღვარგარეთის ქვეყნების კიბერუშიშროების პოლიტიკა

თავი III. ეროვნული უშიშროების მმართველობითი პრობლემები თანამედროვე საქართველოში

3.1 კიბერუშიშროება – XX I საუკუნის გამოწვევა

3.2 კიბერუშიშროების კუთხით საქართველოში არსებული მდგომარეობა

დასკვნა

გამოყენებული ლიტერატურა

შესავალში გადმოცემულია საკვლევი თემის აქტუალობა, კვლევის მიზანი და ამოცანები კვლევის ამოცანები, კვლევის ჰიპოთეზა, კვლევის ობიექტი, კვლევის საგანი, კვლევის სიახლე, კვლევის მეთოდოლოგიური და თეორიული საფუძველი, კვლევის მეთოდოლოგია, სადისერტაციო ნაშრომის სტრუქტურა და ოდენობა.

ნაშრომის **ლიტერატურის მიმოხილვაში** ნაჩვენებია, რომ ეროვნულ უშიშროებასა და ინფორმაციული უშიშროების შესახებ გამოცემულია და მთელი რიგი ნაშრომები და ლიტერატურა, დამტკიცებულია სხვადასხვა კანონები და სტრატეგიები, როგორც ჩვენი ქვეყნისათვის ისე საზღვარგარეთის ქვეყნებშიც. მიუხედავად იმისა რომ ბოლო წლებში გაზრდილია ინტერესი აღნიშნული საკითხის მიმართ და ყურადღება ეთმობა ამ სფეროს საქართველოში, სათანადოდ მაინც არ განხორციელებულა ამ საკითხების რეალური კვლევა.

ნაშრომის პირველ თავში - საქართველოს წინაშე არსებული საფრთხეები და გამოწვევები ინფორმაციული უშიშროების კუთხით განხილულია ინფორმაციული უშიშროების არსი, კერძოდ რა არის ინფორმაცია, როგორ უნდა ხდებოდეს მისი დაცვა. ასევე განხილულია 2008

წლის ინფორმაციული ომი საქართველოს წინააღმდეგ და გაანალიზებულია თუ როგორი ჩავარდნა განიცადა სახელმწიფომ კიბერთავდასხმების მოგერიების საკითხში. აგრეთვე დეტალურად არის განხილული ქვეყნის კიბერსისვრცეზე როგორც სადაზვერვო საქმიანობის მნიშვნელოვან ობიექტზე.

ნაშრომის მეორე თავში - საქართველოს წინაშე არსებული საფრთხეებისა და გამოწვევების გათვალისწინებით ინფორმაციული უსაფრთხოების დაცვის სათანადო მეთოდების დანერგვისა და ეფექტიანი კონტროლის მექანიზმების შემუშავება მიმოხილულია საქართველოს ინფორმაციული უშიშროების პოლიტიკა, ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურა და მისი დაცვის მექანიზმები, ინფორმაციული უშიშროება საჯარო სამსახურებში და საერთაშოროსო ორგანიზაციებისა და კიბერუშიშროების კუთხით მოწინავე ქვეყნების კიბერუშიშროების პოლიტიკა.

ნაშრომის მესამე თავში - ეროვნული უშიშროების მმართველობითი პრობლემები საქართველოში განხილულია კიბერუშიშროება როგორც XXI საუკუნის გამოწვევა, კივბერუშიშროების კუთხით საქართველოში არსებული მდგომარეობის შესასწავლად გაკეთებულია ჩვენს მიერ რესპოდენტებისადმი ჩამორთმეული ინტერბიუები და მათი ანალიზი, ასევე განხილულია სოციოლოგიური კვლევის შედეგები.

დასკვნა

თანამედროვე ინფორმაციული ტექნოლოგიები უმნიშვნელოვანეს როლს ასრულებს ადამიანის, საზოგადოების, სახელმწიფოს ცხოველმოქმედების, საქმიანობის ფუნქციონირების ყველა სფეროში. ინფორმაციულ საზოგადოებაში სიტემური ანალიზის გარეშე წარმოუდგენელია სახელმწიფოებრივი, პოლიტიკური ეკონომიკური თუ სოციალური საკითხების სათანადო დონეზე გადაჭრა, ეს ფაქტორი განსაკუთრებით დიდ დატვირთვას ეროვნული უშიშროების უზრუნველყოფაში იძენს, ვინაიდან ინფორმაციულ ეპოქაში ცალსახად გამოიკვეთა ინფორმაციული ასპე-ქტების გადამწყვეტი როლი ეროვნული უშიშროების უზრუნველყოფაში. ამ მიმართულებით საქმიანობის ეფექტიანობის ამაღლებასა და მის ინფორმაციულ უზრუნველყოფაში უმნიშვნელოვანესი ადგილი უნდა ეჭიროს თა-ნამედროვე ინფორმაციულ სისტემებს.[2]

საინფორმაციო საზოგადოების შექმნის უმთავრესი საფუძველი პროგრესირებადი ინფორმატიზაციაა, დღეს ინფორმატიზაცია საქართველოში არაგეგმაზომიერად, ქაოტურად მიმდინარეობს, რის შემდეგადაც არათუ არ ყალიბდება, არამედ ბევრ შემთხვევაში ხელი ეშლება საინფორმაციო საზოგადოებისათვის სავალდებულო ეროვნული საინფორმაციო გარემოს შექმნას.

საინფორმაციო სივრცის სრულყოფილად ათვისება, მისი პოლიტიკური, სამეცნიერო და სხვა პრაქტიკული მიზნებისთვის გამოყენება შესაბამისი საინფორმაციო ანალიზური, პროგნოზული და კომპიუტერული ტექნოლოგიების ათვისება-მოხმარების საფუძველზე ხდება. ინფორმაციის დამუშავების პროცესის ყველა ეტაპი მოითხოვს შესაბამის ტექნოლოგიურ უზრუნველყოფასა და თანამედროვე საინფორმაციო ტექნოლოგიების გამოყენებას.

პოლიტიკური მოდერნიზაციის პროცესში სახელმწიფოს საი-ნფორმაციო პოლიტიკის წარმატების უზრუნველყოფის ერთ-ერთი გადამწყვეტი ფაქტორია ეროვნული საინფორმაციო რესურსების ერთიანი

ურთიერთდაკავშირებული სისტემის ფორმირება და განვითარება (ქვეყნის საინფორმაციო სივრცის ერთ მთლიანობაში ინტეგრირება).

ინტერნეტის ხელმისაწვდომობის მზარდ ტემპთან ერთად, დღეს მსოფლიოში უფრო და უფრო იზრდება კიბერუშიშროების პრობლემები. დღეს-დღეისობით ინფორმაციული უშიშროება იმდენად აქტუალურია, რომ სხვადასხვა ქვეყნის მთავრობები დილემის წინაშე დგანან, როგორ განახორციელონ მათი კიბერსივრცის დაცვა.

ერთი რამ ცხადია საერთაშორისო არენაზე ქვეყნების მიერ მსოფლიო მოვლენებზე გავლენის მოპოვების შესაძლებლობა სულ უფრო და უფრო დამოკიდებული ხდება საინფორმაციო ინფრასტრუქტურის განვითარების დონეზე, საიდანაც შესაბამისად სახელმწიფოს ექმნება შესაძლებლობა ექსპლუატაცია გაუწიოს სხვა ქვეყნების ინტელექტუალურ პოტენციალს, გააფართოვოს და ჩანერგოს თავისი იდეური ღირებულებები, თავისი კულ-ტურა და ენა.

მსოფლიოში საქმის ამგვარი მდგომარეობა საქართველოსთვის იმის მომასწავებელი უნდა იყოს, რომ გააცნობიეროს ინფორმაციული მუქარის არსებული რეალობა ეროვნულ უშიშროებაში და მიიღოს შესაბამისი ზომები სახელმწიფოს საინფორმაციო ინფრასტრუქტურისა და ინფორმაციული სივრცის დასაცავად.

საქართველოში ამ ეტაპზე არ არსებობს საინფორმაციო უშიშროების ჩამოყალიბებული პოლიტიკა . ნებისმიერი სახელმწიფო დაწესებულება თუ კერძო სექტორი საინფორმაციო რესურსების, სისტემებისა და ქსე-ლების დაცვას საკუთარი ძალებით ახორციელებს. აქვე უნდა აღინიშნოს ის ფაქტიც რომ ძირითად შემთხვევაში საინფორმაციო უსაფრთხოების პირო-ბების დაცვის აუდიტი საერთოდ არ ხდება სახელმწიფოს მხრიდან.

ყველა სახელმწიფო სტრუქტურა თუ კერძო ორგანიზაცია ძირითად აქცენტს აკეთებს საინფორმაციო ინფრასტრუქტურის ფიზიკურ დაცვაზე (კომპიუტერული ტექნიკისა და ქსელების შემთხვევითი თუ ფორ-სმაჟორული ფაქტორების გამო დაზიანებისაგან, როგორიცაა მოპარვისაგან, დენის ვარდნისგან დაცვა და ა.შ.) და ინვესტიციებიც მათი მხრიდან სწო-

რედ ამ მიმართულებით მიდის. საინფორმაციო სისტემებისა და რესურსების დაცვისათვის უმეტესწილად გამოიყენება ინტერნეტში ხელმისაწვდომი უფასო ანტივირუსული პროგრამები. ადგილობრივი ქსელების შემთხვევაში, ძირითადად იყენებენ ქსელის დამცავები (firewall). ხოლო რაც შეეხება სასწავლო დაწესებულებს, აქ არსებყული კომპიუტერული ტექნიკა ვერ აკმაყოფილებე საინფორმაციო უშიშროების ელემენტარულ ნორმებსაც კი.

ამრიგად, სახელმწიფო საინფორმაციო პოლიტიკის გრძელვადიან სტრატეგიულ მიზნად უნდა იქცეს საქართველოში ღია საინფორმაციო საზოგადოების განვითარების პროცესის სახელმწიფო ინტერესებთან შესაბამისობაში მოყვანისათვის ხელის შეწყობა, რაც მსოფლიო თანამეგობრობის განვითარების გლობალური ტენდენციების გათვალისწინებით აუცილებლობას წარმოადგენს მისი თანამედროვეობის შესატყვისი სოციალურ–ეკონომიკური, კულტურული და პოლიტიკური განვითარებისათვის, პოლიტიკური მოდერნიზაციის პროცესების სრულყოფისათვის.

იმის გათვალისწინებით რომ კიბერუშიშროების მთავარი ფაქტორი შეიძლება იყოს ჰაკერი, კრიმინალი ექსტრემისტი ან სახელმწიფო. შესაბამისად განსხვავებულია კიბერუშიშროების დონეებიც. ინდივიდუალური, ორგანიზაციული, სახელმწიფო, მოკავშირეების და მსოფლიო იგივე საყოველთაო. აქედან გამომდინარე ზომები, რომლებიც უნდა გაატა-როს თითოეულმა სახელმწიფომ ინფორმაციის დაცვის უზრუნველსაყოფად რამდენიმე მიმართულებით იყოფა. ესენია: 1. ტექნიკური; 2. ორგანიზაციული; 3. სამართლებრივი; 4. საგანმანათლებლო. საქართველო ყველა იმ რისკების გათვალისწინებით უნდა უზრუნველყოფდეს თითოეულ დონეზე სათანადო მეთოდების დანერგვას და ახორციელებდეს ეფექტურ კონტროლს.

როგორც ჩემს მიერ ჩატარებული კვლევიდანაც ჩანს კიბერუშიშროება ძალიან დინამიური სფეროა და აქ ყოველდღე ჩნდება ახალი საფრთხეები, შესაბამისად პრევენცია ძალიან რთულია, მაგრამ უნდა არსებობდეს სათა-

ნადო რეაგირების მექანიზმები, ანუ კრიტიკულ სიტუაციებში მოქმედების გეგმები და ასევე ამ გეგმების განხორციელების რესურსები, რათა სახელმწიფო სტრუქტურები შესაბამის დონეზე იყოს დაცული კიბერთავდასხმისაგან.

დღესდღეისობით ქვეყნის ინფორმაციულ ინფრასტრუქტურაში შემავალი პროგრამულ–ტექნიკური ბაზა პრაქტიკულად მთლიანად სხვა ქვეყნების მიერ გამოშვებული პროდუქციით ყალიბდება. იგი ყოველგვარი სპეცშემოწმების და სერტიფიცირების გარეშე გამოიყენება ყველა დონის ინფორმაციულ სისტემაში, სახელმწიფო მართვის დონის ჩათვლით.

საქართველო მიისწრაფის ევროინტეგრაციისაკენ, მიისწრაფის ნატოსკენ, სადაც ერთ-ერთი მოთხოვნა არის ინფორმაციის დაცვა. შესაბამისად საქართველოში ინფრასტრუქტურა, რომელიც ამას უზრუნველყოფს, ისე უნდა იყოს მოწყობილი როგორც ეს საზღვარგარეთის სხვა ქვეყნებშია. თუნდაც ესტონეთში, თუნდაც გერმანიასა და ამერიკაში. ამ დონის მიღწევა აუცილებელია, რომ ნატოს პოტენციურმა მოწინააღმდეგემ ვერ მოახ-დინოს შეღწევა.

შეიძლება ითქვას, 2008 წლიდან მოყოლებული პირველი ნაბიჯები გადაიდგა და გარკვეული პროგრესიც არის, თუმცა მისი შეფასება რთულია, რადგან არ არსებობს ემპირიული მონაცემები, არ ვიცით რამდენად არის დამოკიდებული სხვადასხვა ინფრასტრუქტურა ინფორმაციულ სის-ტემებზე და გარდა მაგისა, შესადარებლად 2008წლის შეტევების აღება შეიძლება კონტროპროდუქტიული გამოდგეს. ერთის მხრივ მას შემდეგ 9 წელი გავიდა (დღეს გაცილებით მეტად ვართ დამოკიდებული ინფორმაციულ სისტემებზე) მეორეს მხრივ, კი არავინ იცის რამდენად გამოიყენა მოწინააღმდეგ მაშინ თავისი სრული შესაძლებლობები.

საქართველოს სახელმწიფო მიზანი უნდა იყოს შექმნას ინფორმაციული უშიშროების ისეთი სისტემა, რომლის დროსაც ნებისმიერი კიბერშეტევის საზიანო შედეგები მინიმუმამდე იქნება შემცირებული და ასეთი შეტევის შემდეგ უმოკლეს დროში გახდება შესაძლებელი ინფორმაციული ინფრასტრუქტურის ფუნქციონირების სრული აღდგენა, ამასთან

ინფორმაციული უშიშროების ერთიანი სისტემის შექმნის მიზანია კრიტიკული ინფორმაციული სისტემების მდგრადობის ამაღლება კიბერშეტევებისადმი და ეფექტიანი ღონისძიებების გატარება პოტენციური კიბერშეტევების პრევენციის მიზნით.

მიმაჩნია რომ საქართველოს სახელმწიფოს სტრატეგიულ მიზნად უნდა იქცეს, საინფორმაციო პოლიტიკის და ღია საინფორმაციო საზოგადოების განვითარების პროცესის ხელშეწყობა და საინფორმაციო პოლიტიკის რეალიზაციის პირობების შექმნასთან დაკავშირებული პრობლემების გადაჭრა. საქართველოსთვის მისი გეოპოლიტიკური მდებარეობის, ოკუპირებული ტერიტორიების არსებობისა და მეზობელ ქვეყნებში მიმდინარე პროცესების შესაძლო გავლენების გათვალისწინებით ეროვნული უშიშროების განუყოფელი ნაწილის კიბერუშიშროების დაცვის სფეროში ეფექტური პოლიტიკისა და სტანდარტების განაზღვრა სასიცოცხლოდ მნიშვნელოვანია.

აუცილებელია ეროვნული უშიშროებისა და თავდაცვის სტრატეგიული მიმოხილვის პროცესებში **სამოქალაქო საზოგადოების** აქტიური ჩართვის უზრუნველყოფა. სასურველია აღნიშნული პროცესის ინსტიტუციონალიზაცია.

უმნიშვნელოვანესი თემაა **სამოქალაქო ცნობიერების ამაღლება,** რათა მოქალაქეს შეეძლოს საწყის დონეზე მაინც კომპიუტერში პირადი მონაცემების დაცვა კიბერშეტევისაგან, თითოეული მოქალაქე საწარმო თუ საჯარო დაწესებულება ვალდებულია ინდივიდუალურად უზრუნველყოს მის მფლობელობასა და განკარგულებაში არსებული ინფორმაციული სისტემების უსაფრთხოება.

ინდივიდუალური პასუხისმგებლობა. ინდივიდუალურ დონეზე ძირითადი საფრთხის შემცველია ინტერნეტი, რომლის მომხმარებელთა საერთო რაოდენობა მთელი მსოფლიოს მასშტაბით 1,5 მილიარდ ადამიანს აჭარბებს და სოციალური ქსელები რაც პიროვნული ინფორმაციის მისაწვდომობას ზრდის.

ამ ფაქტორების გათვალისწინებით ინტერნეტი თავისი ფართო მასშტაბის გამო ყველაზე უფრო ძნელად გასაკონტროლირებადი სივრცეა. სწორედ ამიტომ თითოეული მოქალაქე, საწარმო თუ საჯარო დაწესებულება ვალდებულია ინდივიდუალურად უზრუნველყოს მის მფლობელობასა და განკარგულებაში არსებული ინფორმაციული სისტემების უსაფრთხოება. აღნიშნული სისტემების მფლობელებმა და უშუალოდ მომხმარებლებმა უნდა მიიღონ ყველა საჭირო ზომა მათი უსაფრთხო ფუნქციონირების უზრუნველაყოფად.

სახელმწიფოსა და ორგანიზაციის დაცულობა. ორგანიზაციულ დონეზე საფრთხის შემცველია ძირითადი მომსახურე პერსონალი. ამიტომ სახელმწიფო სექტორისათვის უნდა შეიქმნას სპეციალური სამოქმედო გეგმა და შიდა მარეგულირებელი წესები, უნდა მოხდეს ინფორმაციის დაცვა ადმინისტრაციულ დონეზე მომსახურე პერსონალის სათანადო მომზადების გზითა და შესაბამისი ინფრასტრუქტურით, პროგრამულ-აპარატული საშუალებებით უზრუნველყოფილი უნდა იყოს ფიზიკური დაცულობა.

რაც შეეხება სახელმწიფო დონეს, როცა საქმე ეხება განსაკუთრებით მნიშვნელოვანი ინფორმაციის დაცვას, აუცილებელია, რომ შეიქმნას თანამედროვე სტანდარტების შესაბამისი მატერიალურ-ტექნიკური ბაზა, რათა ინფორმაციის ბრუნვა კონტროლდებოდეს. ეს შეიძლება იყოს აპარატული უზრუნველყოფა, პროგრამული უზრუნველყოფა თუ კავშირი და კომუნიკაცია. ტექნოლოგიური პროგრესის მზარდი ტემპებით მიმდინარეობის პირობებში სტანდარტიზაცია მნიშვნელოვანი ფაქტორია.

აქტიური საერთაშორისო თანამშრომლობა. საქართველოს მთავრობა უნდა აცნობიერებდეს, რომ არც ერთ მთავრობას მსოფლიოში არ შეუძლია მხოლოდ საკუთარი რესურსებით უზრუნველყოს კიბერუშიშროების სფეროში არსებულ გამოწვევებთან და საფრთხეებთან გამკლავება. შესაბამისად საქართველოს მიზანს წარმოადგენს ქტიური ითანამშრომლობა პარტნიორ ქვეყნებთან კიბერუშიშროების სფეროში, როგორც ორმხრივ ისე მრავალმხრივ ფორმატში.

ვინაიდან კიბერსაფრთხეები მუდმივად იცვლება (ჩნდება ახალი კომპიუტერული ვირუსები, არასანქცირებული შეღწევისაგან დამცავი სისტემების დარღვევის ახალი საშუალებები და ეს პროცესი კიდევ უფრო ვითარდება საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარების პარალელურად), უნდა შემუშავდეს საინფორმაციო უშიშროების პროცედურების მუდმივი სწავლებისა და ტრენინგის სისტემა, საინფორმაციო სისტემებისა და მათი ექსპლუატაციის პირობების პერიოდული აუდიტის, უსაფრთხოების თვალსაზრისით მათი შეფასებისა და სერტიფიცირების სისტემა.[22]

ყოველივე ზემოთ აღნიშნულიდან გამომდინარე შეიძლება შემდეგი დასკვნის გამოტანა რომ, კიბერუშიშროების უზრუნველყოფის მიზნით **საერთაშორისო თანამშრომლობის** განვითარებისათვის საქართველომ უნდა ჩაატაროს ქვემოთ ჩამოთვლილი ღონისძიებები:

- კიბერუშიშროების საკითხებზე საერთაშორისო ურთიერთობების განმტკიცება ამ სფეროში მომუშავე საერთაშორისო ორგანიზაციებთან და სახელმწიფო ორგანოებთან ინტენსიური კონტაქტი
- საერთაშორისო ინიციატივებში აქტიურად ჩართვა და მონაწილეობის მიღება კიბერუშიშროების კუთხით, შემდგომში უკვე ამ ინიციატივების მხარდაჭერის განხორციელება რეგიონის მასშტაბით
- მუდმივს რეჟიმში უნდა მოხდეს სხვა ქვეყნების CERT-ებთან კიბერუშიშროების სფეროში თანამშრომლობის ინიცირება.
- საქართველომ ინტენსიური თანამშრომლობა უნდა გააგრძელოს კიბერუშიშროების კუთხით კარგი გამოცდილების მქონე ქვეყნებთან და ასევე მიზანშეწონილია განისაზღვროს, სახელმწიფოს პარტნიორი და პოტენციურად მოწინააღმდეგე ქვეყნები. საინტერესო იქნება სტრატეგიულ ქვეყნებთან საერთო კიბერუშიშროების სისტემაზე მუშაობა.

საქართველოს მიზანი უნდა იყოს შექმნას კიბერუშიშროების ისეთი სისტემა რომელიც ხელს შეუწყობს ერთი მხრივ ინფორმაციული ინფრასტრუქტურის დაცულობას კიბერსაფრთხეების წინაშე და მეორე მხრივ იქნება დამატებითი ფაქტორი ქვეყნის შემდგომი ეკონომიკური და

სოციალური განვითარებისათვის. ამ მიზნის მიღწევისათვის მნიშნელოვანია თანამშრომლობის შემდეგი პრინციპების განხორციელება:

• **საქართველოს მთავრობის ერთიანი მიდგომა**- 1. კიბერუშიშრიების გასაძლიერებლად ქვეყანაში ერთ–ერთი აუცილებელი ფაქტორია რომ მთავრობამ დიდი მნიშვნელობა უნდა მიანიჭოს უსაფრთხოების პოლიტიკის და მისი კომპეტენციის განხორციელების მექანიზმების ინსტიტუციონალიზაციას, ამ მხრივ კიბერუშიშროების უზრუნველსაყოფად მნიშვნელოვანია სახელმწიფო უწყებებს შორის თანამშრომლობა და ისეთი მექანიზმის განვითარება, რომელიც კიბერუშიშროების პოლიტიკის დაგეგმვისა და განხორციელებისას ხელს შეუწყობს საქართველოს მთავრობის ერთიან მიდგომას და სხვადასხვა სახელმწიფო უწყების გამართულ კოორდინირებულ მუშაობას.

2. კიბერუშიშროების სფეროში არსებული მდგომარეობის გათვალისწინებით, საქართველოს სახელმწიფო არც თუ ისე მარტივი პრობლემის წინაშე დგას, რაც პირველ რიგში დაკავშირებულია საჭირო საკანონმდებლო ბაზის არ არსებობით ქვეყანაში. მხოლოდ, უკვე არსებული კანონი "ინფორმაციული უსაფრთხოების შესახებ" და კიბერუსაფრთხოების სტრატეგია არ არის საკმარისი, უნდა შეიქმნას შესაბამისი კანონმდებლობა, რაც და არეგულირებს უკვე არსებული თითოეული სუბიექტის - მონაცემთა გაცვლის სააგენტოს, კიბერუსაფრთხოების ბიუროსა და შსს კიბერდანაშაულთან ბრძოლის სამმართველოს ურთიერთკოორდინირებულ საქმიანობას, განსაზღვრავს თითოეული სუბიექტის მოქმედების ფარგლებსა და დამატებით ვალდებულებებს, ასევე რაც ყველაზე მნიშვნელოვანია კანონმებლობაში უნდა იყოს განსაზღვრული კერძო სექტორის, ინტერნეტ მომწოდებლების ვალდებულებები და სახელმწიფო სუბიექტების კოორდინირებული მუშაობის კონკრეტული ასპექტები.

3. აუცილებელია ჩამოყალიბდეს სახელმწიფო ინსტიტუტები, რომელიც კონტროლს გაუწევს ყველა საშუალებების მუშაობას. აუცილებელია სხვადასხვა ეროვნული სტრატეგიების შექმნა ყველა შესაძლო ვარიანტების გათვალისწინებით, რათა მაქსიმალურად იქნეს გაანალიზებული

მოსალოდნელი საფრთხეები და განისაზღვროს მისი პრევენციის ზომების მიღება.

4. რუსეთის ფედერაციის საინფორმაციო ომი ჩვენი ქვეყნის წინააღმდეგ მომართული ოფიციალურად განისაზღვრული უნდა იყოს საფრთხედ შესაბამის დოკუმენტებში, რადგანაც მის მერ განხორციელებული პროპაგანდა საფრთხის შემცველია საქართველოს უსაფრთხოებისათვის და აფერხებს საქართველოს დემოკრატიულ განვითარებას, შესაბამისად ის აუცილებლად უნდა აისახოს საქართველოს ეროვნული უსაფრთხოების კონცეფციაში.

5. ჩვენი აზრით, ქვეყანაში უნდა შეიქმნას ისეთი ორგანო, რომელიც კოორდინაციას გაუწევს კიბერუშიშროების საკითხებზე მიმდინარე სამუშაო პროცესებს, ეს ორგანო პირდაპირ უნდა დაექვემდებაროს პრემიერ მინისტრს. შესაბამისად კიბერსივრცის დაცვის საკითხებზე იმუშავებდა არა უსაფრთხოებისა და კრიზისების მართვის საბჭო, ან უშიშროების საბჭო, არამედ პრემიერ მინისტრის ინსტიტუტი. ორგანო კოორდინირებას გაუწევს სახელმწიფო სუბიექტების, კერძოდ სამოქალაქო სექტორების საქმიანობას, იზრუნებს საზოგადოებაში ცნობადობის ამაღლებაზე, სამეცნიერო-კვლევითი და ანალიტიკური საქმიანობის განვითარებაზე, პასუხისმგებელი იქნება საკანონმდებლო ბაზის შექმნასა და მის მუდმივ განახლებაზე, ეს მაკოორდინირებელი ორგანო ასევე ზედამხედველობას გაუწევდა ქვეყანაში ახალი ტექნოლოგიების შეწავლისა და დანერგვის პროცესს, რაც თავისთავად ხელისშემწყობი ფაქტი იქნებოდა კიბერსივრცის მეტად დაცვისათვის,უნდა ითქვას, რომ თითქმის ყველა წამყვან ქვეყანაში არსებობს მსგავსი ორგანო.

• **თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის** - კიბერ-უშიშროების უზრუნველსაყოფად მნიშვნელოვანია თანამშრომლობის მექანიზმის განვითარება როგორც სახელმწიფო უწყებებს, ასევე სახელმწფო და კერძო სექტორებს შორისაც. საქართველოს კრიტიკული ინფრასტრუქტურის მნიშვნელოვანი ნაწილი კერძო ბიზნესის ხელშია და ამ სფეროში არსებული გამოცდილება და ცოდნა ძირითადად თავმოყრილია კერძო

კომპანიებში, გამომდინარე აქედან მნიშვნელოვანია თანამშრომლობის მექანიზმის შემუშავება, რომელიც ხელს შეუწყობს ერთის მხრივ კრიტიკული ინფორმაციული ინფრასტრუქტურის გამართულად მუშაობას, მათ შორის კრიზისების დროს და მეორეს მხრივ, დამატებითი მასტიმულირებელი ფაქტორი იქნება ეკონომიკის განვითარებისთვისაც.

ასე რომ საჯარო სამსახურების და კერძო კომპანიების ერთმანეთთან მჭიდრო კავშირი, ისე თავდაცვის სისტემაში შემავალი სტრუქტურული ერთეულების მჭიდრო თანამშრომლობა, ასევე უწყებათაშორისი ძალისხმევა და კოორდინირებული მუშაობა არასამთავრობო სექტორთან არათუ საჭირო არამედ აუცილებელიც კი არის.

• **სამოქალაქო ცნობიერების ამაღლება - 1.** კიბერუშიშროების ძირეულ საკითხებზე შემუშავდეს მოკლე ბრიფინგები და დისკუსიები და მიეწოდოთ საქართველოს მაღალი თანამდებობის პირებს. ასევე შემუშავდეს და მიეწოდოთ მარტივი კომპიუტერული ჰიგიენის კურსები საჯარო მოხელეებს.

2) საზოგადოების ცნობიერების ამაღლების მიზნით დაიგეგმოს და განხორციელდეს სპეციალური პროგრამები, კერძოდ მოხდეს ვიდეო-ორგოლების გადაღება, რათა საზოგადოებამ უკეთ გაიგოს თუ რა რისკების მომტანია კიბერდანაშაული მათთვის.მნიშვნელოვანია საზოგადოების ცნობიერების ამაღლება პრევენციული ზომებისა და შეტყობინების აუცილებლობის შესახებ.

3) კიბერუშიშროების სფეროში წარმატებული ქვეყნების მთავრობათა კიბერუშიშროების საუკეთესო პრაქტიკაზე დაყრდნობით, შემუშავდეს სპეციალური სახელმძღვანელო, თანდართული ტრენინგ-პროგრამებით.

4) ეტაპობრივად უნდა ხდებოდეს, მეტი შეხვედრების, ფორუმების, ტრენინგების ჩატარება ინფორმაციული ტექნოლოგიებისა და კიბერ-უშიშროების მიმართულებით, რაც საშუალებას მისცემდა ამ მიმართულებით მომუშავე ადამიანების კიდევ მეტ დახვეწას და განვითარებას.

რეკომენდაციები:

1. ეროვნული უსაფრთხოების კონცეფციის საფუძველზე, იმ ქვეყნების მიერ წარმოებული პროგრამული უზრუნველყოფა არ მოხდეს ვირტუალურ საჯარო სავრცეში, ხოლო მათ ონლაინ რესურსებზე განხორციელდეს მონიტორინგი;

2. სახელმწიფოს მხრიდან განხორციელდეს ქართული ონლაინ სივრცის მონიტორინგი , უცხო ქვეყნის პროპაგანდისტული წყაროების გამოსავლენად.

3. განხორციელდეს იმ კერძო სექტორის ინფორმაციული ტექნოლოგიების აუდიტი წელიწადში ორჯერ, რომლებიც ფლობენ კრიტიკულ ინფრასტრუქტურას.

4. სახელმწიფო დაუბრუნდეს კიბერრეზერვის ახალი პროგრამის განხილვას.

5.საგანმანათლებლო დაწესებულებებში დაინერგოს კიბერუშიშროების კულტურის სწავლება.

6. კიბერუშიშროების საკითხებზე საერთაშორისო ურთიერთოებების განმტკიცება ამ სფეროში მომუშავე საერთაშორისო ორგანიზაციებთან და სახელმწიფო ორგანოებთან.

7. საზოგადოების ცნობიერების ამაღლების მიზნით მარეგულირებელმა კომისიამ დაავალოს ინტერნეტპროვაიდერებს მომხმარებელს მიაწოდოს ინფორმაცია კიბერსაფრთხეებისგან თავდაცვის მექანიზმებზე.

საქართველოს სახელმწიფოს მიზანს უნდა წარმოადგენდეს გახდეს რეგიონის ლიდერი კიბერუშიშროების სფეროში და რა თქმა უნდა ეს ხელს შეუწყობს აიმაღლოს რეპუტაცია მსოფლიოს მაშტაბით და შეინარჩუნოს უსაფრთხო კიბერსივრცე ჩვენს ქვეყანაში.

საქართველოს ხელისუფლების განსაკუთრებული ყურადღების საგანი მუდმივად უნდა იყოს სახელმწიფო მმართველობის კომპლექსური მრავალგანზომილებიანი ამოცანის – საინფორმაციო პოლიტიკის რეალიზაციის პრობლემა, რომელიც მოიცავს ნორმატიულ–სამართლებრივ, ორგანიზაციულ–ტექნოლოგიურ, ტექნიკურ–ეკონომიკურ, სოციალურ და

საგანმანათლებლო პროგრამებს. დიდი ინფორმაციის დამუშავება კი მოვლენების მუდმივი ხედვის არეში მოქცევას, ახალი ინფორმაციული ტექნოლოგიების გამოყენებას მოითხოვს.

დისერტაციის შესრულება:

მომზადდა დოქტორანტურაში სწავლის დებულებით გათვალისწინებული და დაცული **ორი თემატური სემინარი:**

1. სემინარი: უსაფრთხოება და საერთაშორისო ტერორიზმი თარიღი: 17.02.2016 წ.

2. სემინარი: საერთაშორისო ტერორიზმი - გლობალური პოლიტიკის პრობლემა თარიღი: 26.06.2017 წ.

სამი კოლოკვიუმი:

1. კოლოკვიუმი: "საქართველოს წინაშე არსებული საფრთხეები და გამოწვევები". თარიღი: 17.02.2016 წ.

2. კოლოკვიუმი: „საქართველოს წინაშე არსებული საფრთხეებისა და გამოწვევების გათვალისწინებით ინფორმაციული უშიშროების დაცვის სათანადო მეთოდების დანერგვისა და ეფექტინი კონტროლის მექანიზმების შემუშავება". თარიღი: 15.07.2016 წ.

3. კოლოკვიუმი: „ეროვნული უშიშროების მმართველობითი პრობლემები საქართველოში" თარიღი: 27.02.2017 წ.

სადისერტაციო ნაშრომის ძირითადი შედეგები გამოქვეყნებულია შემდეგ პუბლიკაციებში:

სამეცნიერო სტატიები:

1. ავტორი: დოქტორანტი სალომე გუმბერიძე სტუ. სამეცნიერო ჟურნალი

„ხელისუფლება და საზოგადოება (ისტორია, თეორია, პრაქტიკა)". სტატია: "2008 წლის ინფორმაციული ომი საქართველოს წინააღმდეგ" 2016 წელი, ტომიII. გვ 88-93

2. ავტორი: დოქტორანტი სალომე გუმბერიძე სტუ. სამეცნიერო ჟურნალი „ხელისუფლება და საზოგადოება (ისტორია, თეორია, პრაქტიკა)“. სტატია: „ინფორმაციული უშიშროება საჯარო სამსახურებში“ 2016წელი ტომიI. გვ 61-66

3. ავტორი: დოქტორანტი სალომე გუმბერიძე სტუ. სამეცნიერო ჟურნალი „ხელისუფლება და საზოგადოება (ისტორია, თეორია, პრაქტიკა)“. სტატია: „საერთაშორისო ორგანიზაციებისა და საზღვარგარეთის ქვეყნების კიბერუშიშროების პოლიტიკა“. 2018წელი. გვ47-54

4. ავტორი: დოქტორანტი სალომე გუმბერიძე. სტუ. სამეცნიერო ჟურნალი სამეცნიერო - პრაქტიკული კონფერენციის „ეროვნული და კორპორაციული უსაფრთხოება“ - მასალები. შრომების კრებული I. სტატია: „კიბერსივრცე, როგორც სადაზვერვო საქმიანობის მნიშვნელოვანი ობიექტი. მაისი 2017 წელი. გვ16-24

კონფერენციები:

1. სტუ-ს სტუდენტთა 83-ე ღია საერთაშორისო სამეცნიერო კონფერენცია „საქართველოს წინაშე არსებული საფრთხეები და გამოწვევები ინომრაციული უსაფრთხოების კუთხით“. საქართველო. თბილისი. საქართველოს ტექნიკური უნივერსიტეტი .2015 წელი

2. სტუ-ს სტუდენტთა 84-ე ღია საერთაშორისო სამეცნიერო კონფერენცია „ეროვნული უშიშროების მმართველობითი პრობლემები თანამედროვე საქართველოში კიბერუშიშროების კუთხით. საქართველო. თბილისი. საქართველოს ტექნიკური უნივერსიტეტი . 2016 წელი

3. სტუ-ს სტუდენტთა 85-ე ღია საერთაშორისო სამეცნიერო კონფერენცია „ საქართველოს ინფორმაციული უშიშროების პოლიტიკა“ საქართველო. თბილისი. საქართველოს ტექნიკური უნივერსიტეტი . 2017 წელი

4. სამეცნიერო პრაქტიკული კონფერენცია ეროვნული და კორპორაციული უსაფრთხოება „ კიბერსივრცე, როგორც სადაზვერვო საქმიანობის მნიშვნელოვანი ობიექტი“. საქართველო თბილისი.ეროვნული

და კორპორაციული უსაფრთხოების სასწავლო კვლევითი ცენტრი. 2017 წლის მაისი.