საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

აკაკი შეყელაძე

საჯარო ადმინისტრირების ინფორმაციული უსაფრთხოების გამოწვევები და მათი მართვის ინოვაციური საშუალებები

დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარდგენილი დისერტაციის

ა ვ ტ ო რ ე ფ ე რ ა ტ ი

სადოქტორო პროგრამა: „ინოვაციებისა და ოპერაციათა მენეჯმენტი“

შიფრი: 0203

თბილისი

2023 წელი

სამუშაო შესრულებულია საქართველოს ტექნიკურ უნივერსიტეტში

ენერგეტიკის ფაკულტეტი

საწარმოო ინოვაციების და ოპერაციათა მენეჯმენტის დეპარტამენტი

ხელმძღვანელი: პროფესორი კ. ხმალაძე

რეცენზენტები:

დაცვა შედგება 2023 წლის ”--------” ”-------------------------” ”---------” საათზე საქართველოს ტექნიკური უნივერსიტეტის ენერგეტიკის ფაკულტეტის სადისერტაციო ნაშრომის დაცვის კოლეგიის სხდომაზე, კორპუსი VIII, სხდომათა დარბაზი.

მისამართი: 0160, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ის ბიბლიოთეკაში,

ხოლო ავტორეფერატისა - ფაკულტეტის ვებგვერდზე

ფაკულტეტის სწავლული მდივანი, პროფესორი გ. გიგინეიშვილი

ნაშრომის ზოგადი დახასიათება

თემის აქტუალურობა

მსოფლიოში მიმდინარე მოვლენებმა, რომელიც დაკავშირებულია ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე დამოკიდებულების ზრდასთან, განაპირობა როგორც კერძო, ასევე საჯარო სექტორში მიმდინარე პროცესების გაციფრულება, რაც საქმის წარმოების ელექტრონულ სისტემაზე გადასვლას გულისხმობს და ტექნოლოგიურ ინოვაციას წარმოადგენს. 21-ე საუკუნის დასაწყისიდან განვითარებად და განვითარებულ ქვეყნებში სახელმწიფო სერვისების უდიდესი ნაწილი ელექტრონულად იმართება, რაც დადებითი მოვლენაა და მომავლის პერსპექტივაზეა გათვლილი.

ცხადია, ქვეყნების გაციფრულების მაჩვენებლების დონე განსხვავდება, რადგანაც იგი დამოკიდებულია მრავალ ფაქტორზე. რამდენიმე ევროპულ და ამერიკულ ქვეყანაში უკვე არჩევნები ელექტრონულად ტარდება, თუმცა, ამ მხრივ არც საქართველოში შეიმჩნევა უარყოფითი ტენდენცია და სახელმწიფო ადმინისტრირებასთან დაკავშირებული სერვისების უდიდესი ნაწილი ან უკვე ელექტრონულია, ან მისი გაციფრულება დაგეგმილია უახლოეს მომავალში.

ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე დამოკიდებულების ზრდა დადებითი მოვლენაა. პროცესები, რომლებიც დაკავშირებულია საქმის წარმოებასთან, დოკუმენტბრუნვასთან, ინფორმაციის დამუშავება-გადაცემასთან და სხვა ოპერაციებთან, გაცილებით მარტივად და ეფექტურად მიმდინარეობს ელექტრონულ სივრცეში, ვიდრე მატერიალური საშუალებების გამოყენებით, რადგანაც ამას ახლავს ბუნებაზე ზრუნვის, ნაკლები დანახარჯების, შრომის ეფექტიანობის ზრდის და, ზოგადად, პროცესის გამარტივების სარგებელი.

მსოფლიოში ამჟამად ინდუსტრიული რევოლუციის მე-4 ეტაპია, რომელიც ინდუსტრია 4.0-ის სახელით მოიხსენიება და კიბერფიზიკური სისტემების დანერგვა-გამოყენებას გულისხმობს. მისი უმთავრესი შედეგი ბიზნეს-პროცესების ჭკვიან სისტემაზე გადაყვანაა, რაც გულისხმობს დროისა და რესურსის დაზოგვას თანამედროვე სისტემებისა და გადაწყვეტების დანერგვის თვალსაზრისით. აღნიშნული ხორციელდება IoT-ის (ნივთების ინტერნეტი) გამოყენებით, შემდეგ კი ერთვება მანქანური სწავლება და ის ინფორმაციას გარდაქმნის რელევანტურ

ინფორმაცია-ცოდნად, რის საფუძველზეც მიიღება გადაწყვეტილებები. მიუხედავად უდიდესი შესაძლებლობისა, რასაც ინდუსტრია 4.0 იძლევა, უკვე დადასტურდა, რომ მის წინაშე დგას უსაფრთხოებასთან დაკავშირებული რისკები, რასაც, ინფორმაციის დაცვის სათანადო დონეზე უზრუნველყოფის გარეშე, შეუძლია მიგვიყვანოს სავალალო შედეგებამდე, როგორიცაა: კომერციული საიდუმლოების, კონფიდენციალური მასალების გამჟღავნება და ადამიანების ჯანმრთელობის გაუარესება და ლეტალური შედეგი. ასეთი შემთხვევები განხილული და გაანალიზებულია ნაშრომებში, და, მათ შორის, მოიცავს ისეთ კიბერშეტევებს, რომელიც მიმართული იყო ქვეყნების ენერგოსისტემაზე (უკრაინის ტერიტორიის უდიდეს ნაწილში ელექტრონერგიის წყვეტა; გაზსადენის აფეთქება რუსეთში; აშშ-ში ნავთობსადენის ბლოკადა), ჯანდაცვის სისტემაზე (დიდ ბრიტანეტთი გადაუდებელი სამედიცინო დახმარების სერვისების კოლაფსი), კვების სექტორზე (ჩრდილოეთ ამერიკის უმძლავრესი ხორცპროდუქტების წარმოების შეჩერება) და მრავალი სხვა.

ზემოაღნიშნულთან ერთად, მანქანურ მოწყობილობებზე მუშაობას და ინფორმაციის შენახვას თან ახლავს გარკვეული რისკები, როგორიცაა: მანქანის დაზიანება, წყობიდან გამოსვლა, ქურდობა და მრავალი სხვა.

თუმცა, დღეს აღნიშნული რისკები ნამდვილად მცირეა იმასთან შედარებით, რასაც 21-ე საუკუნის ახალი ტერმინი და სფერო - კიბერუსაფრთხოება მოიაზრებს. კიბერშეტევების შედეგად ინფორმაცია შეიძლება უნებართვოდ შეიცვალოს, მასზე წვდომა გაუქმდეს, განადგურდეს და გაიცეს არაავტორიზებულ პირზე. ამასთანავე, კიბერშეტევის ტიპიდან გამომდინარე, მას შეიძლება მოჰყვეს ფინანსური და რეპუტაციული ზიანი.

სახელმწიფოს წინააღმდეგ მიმართული კიბერშეტევები უფრო მძიმე შედეგებით გამოირჩევა, ვინაიდან მათ შეიძლება გამოიწვიონ სახელმწიფო სერვისების შეფერხება, საზოგადოებაში შიშისა და პანიკის დათესვა, რაც ქვეყნის დემოკრატიულ პროცესებს აზიანებს.

საქართველო მსოფლიოში ერთ-ერთი პირველი სახელმწიფო იყო, რომელზეც უშუალოდ სხვა ქვეყნის მხრიდან კიბერშეტევა განხორციელდა. ბოლო 20 წლის განმავლობაში ქვეყნის წინააღმდეგ რამდენიმე კიბერშეტევა იყო

მომართული, რომელთა მიზანიც რეპუტაციული ზიანის მიყენება ან ინფორმაციის მოპარვა იყო.

სადისერტაციო ნაშრომის აქტუალურობას განაპირობებს მსოფლიო მასშტაბით ინფორმაციული უსაფრთხოების კომპრომეტირების შემთხვევების როგორც სიხშირის, ასევე სიმძიმის ზრდა, განსაკუთრებით კი, სახელმწიფოების წინააღმდეგ. ბოლო წლების განმავლობაში ცხადი გახდა ასეთი შემთხვევების საფრთხე, ვინაიდან მათ, როგორც აღწერილია ნაშრომში, ძალუძთ ქვეყნების კრიტიკული ინფრასტრუქტურის გამოყვანა წყობიდან, მათ შორის: ელექტრო და წყალმომარაგება, ნავთობ და გაზსადენების მიყვანა აფეთქებამდე, ისეთი სერვისების შეფერხება, როგორიცაა სატრანსპორტო და სამედიცინო, ავტოგასამართი სადგურების მომსახურება, საარჩევნო პროცესები და ხელოვნური ინტელექტის გამოყენებით მართული სხვა ოპერაციები. ამას ემატება პერსონალური და კონფიდენციალური ინფორმაციის გასაჯაროების შედეგად მომდინარე რისკები, რომელსაც სახელმწიფოს დემოკრატიული საწყისების რღვევისკენ მივყავართ.

მიუხედავად იმისა, რომ დღეს გლობალური კიბერუსაფრთხოების დანახარჯები 6 მილიარდ დოლარს აღემატება და ქვეყნები ფინანსურ და ადამიანურ რესურებს არ იშურებენ ინფორმაციული უსაფრთხოების სისტემების დაცვისთვის, კიბერშეტევების რიცხვი ყოველწლიურად იზრდება. თუკი 2016 წელს შანტაჟის/გამოსასყიდი პროგრამის მეშვეობით განხორციელებული კიბერშეტევა 40 წამში ერთხელ ხორციელდებოდა, 2021 წელს ამ რიცხვმა, კვლევის შედეგად, 11 წამს მიაღწია.

ცხადია, ტექნოლოგიები ვითარდება და მათზე ჩვენი დამოკიდებულების ზრდა შეუძლებელია შეფასდეს უარყოფითად. მიუხედავად ამისა, როგორც ჩანს, ქვეყნების მიერ გაღებული ძალისხმევა ქვეყნის ინფორმაციული ინფრასტრუქტურის დასაცავად, კიბერსივრცის სპეციფიკიდან გამომდინარე, არასაკმარისად ეფექტურია.

თემის აქტუალურობას ხაზს უსვამს ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის მიდგომა კიბერუსაფრთხოებასთან მიმართებაში, რაც საყურადღებოა საქართველოსთვის, რომელიც ევროატლანტიკური ინტეგრაციისკენ ისწარფვის. NATO-მ კიბერსივრცე ოპერაციების არეალად

დაასახელა ჯერ კიდევ 2016 წელს, ხმელეთთან, ზღვასთან, საჰაერო და კოსმოსურ სივრცესთან ერთად. ამასთან, მსოფლიო მასშტაბით არსებული საერთაშორისო ორგანიზაციები ქვეყნებს უწესებენ ისეთ ვალდებულებებს, როგორიცაა ევროკავშირის GDPR რეგულაცია. აღნიშნული და სხვა მრავალი ფაქტორი ხაზს უსვამს იმას, რომ ქვეყანაში ინფორმაციული უსაფრთხოების უზრუნველყოფა დასავლურ სამყაროსთან სიახლოვის, ევროატლანტიკური ინტეგრაციის და დემოკრატიული ორიენტაციის მქონე ქვეყნის რეპუტაციის აუცილებელი პირობაა.

კვლევის მიზანი და ამოცანები

დღეს-დღეობით არც ერთ განვითარებულ თუ განვითარებად ქვეყანას არ აქვს იდეალური კიბერუსაფრთხოების სისტემა. აშშ, რომელიც გლობალური კიბერუსაფრთხოების ინდექსით პირველ ადგილს იკავებს მსოფლიოში, 2006-2020 წლებში 156 მძლავრი (შეტევა, რომლის შედეგად მიყენებული ზიანიც 1 მლნ დოლარს აღემატება) კიბერშეტევის მსხვერპლი გახდა. საქართველო, რომელიც კიბერაქტორების სიმცირით არ გამოირჩევა, ხოლო მის მიერ გადადგმული ნაბიჯები ინფორმაციული ინფრასტრუქტურის დაცვის კუთხით არაერთხელ აღმოჩნდა უცხოელი ექსპერტების აღნიშვნის ღირსი, თითქმის ყოველწლიურად ხდება კიბერშეტევის სამიზნე.

სადისერტაციო ნაშრომში წარმოდგენილი კვლევის მიზანს წარმოადგენს აკადემიური ხასიათის სამეცნიერო ნაშრომის შექმნა, რომელშიც ასახულია ინფორმაციული უსაფრთხოების გამოწვევები და მართვის საშუალებები საქართველოს სახელმწიფო ადმინისტრირებასთან მიმართებაში.

ამისათვის, კვლევის ამოცანად სახელდება ინფორმაციული უსაფრთხოების რისკების გამოვლენა, ქვეყნების წინააღმდეგ განხორციელებული ცნობილი კიბერშეტევების შესაბამის ჭრილში განხილვა, საქართველოს ინფორმაციული ინფრასტრუქტურის წინაშე არსებული პრობლემების სიღრმისეული შესწავლა და ჩვენი ქვეყნის წინააღმდეგ განხორციელებული კიბერშეტევების წარმატების განმაპირობებელი ფაქტორების გამოვლენა.

კვლევის ამოცანად ასევე მიჩნეულია კიბერშეტევის დღეს არსებული ვექტორების გამოვლენა, განსაკუთრებით, კი სახელმწიფოსთან მიმართებაში.

ამისათვის ნაშრომში ხდება კონკრეტული კიბერშეტევების განხილვა ქვეყნების წინააღმდეგ, ჰაკერების ტაქტიკისა და შეტევების მავნე შედეგების გაანალიზებასთან ერთად.

სამეცნიერო კვლევის ამოცანაა უცხო ქვეყნების წარმატებული გამოცდილების შესწავლა და მათი ქართულ საჯარო მმართველობის ინფორმაციულ სისტემაზე გავრცელების შესაძლებლობის და ეფექტურობის განსაზღვრა. შედეგად, კვლევა მიზნად ისახავს გამოავლინოს პოტენციური ინოვაციური საშუალებები, რომელიც დაეხმარება საჯარო ადმინისტრირების სექტორს ინფორმაციული უსაფრთხოების რისკების მართვაში.

ქართულ სამეცნიერო ლიტერატურაში ინფორმაციული და კიბერუსაფრთხოების სფეროში ნაშრომების ნაკლებობას განვიცდით, რაც გახდა კვლევის უმთავრესი საფუძველი და მის მიზნად სწორედ ამ სფეროს შესწავლა, შესაბამისი რეკომენდაციების და დასკვნების მომზადება დავისახეთ. ამასთან, დისერტაცია შესაძლებელია გამოყენებული იქნას ძირითად ან დამხმარე ლიტერატურად ინფორმაციული უსაფრთხოების სასწავლო დისციპლინებისთვის უმაღლეს დაწესებულებებში.

კვლევა საინტერესო იქნება როგორც სამთავრობო, ასევე კერძო და აკადემიური სფეროს წარმომადგენლებისთვის, რადგან ახდენს საქართველოს ინფორმაციული უსაფრთხოების გარემოს ანალიზს, ხოლო შედეგს წარუდგენს აკადემიურ სექტორს, რომელშიც მოიაზრებიან კერძო მკვლევარები, კვლევითი ორგანიზაციები და უმაღლესი სასწავლო დაწესებულებები. იგი პრაქტიკულ დახმარებას გაუწევს კიბერუსაფრთხოების აქტორების თანამშრომლებსა და ინფორმაციული უსაფრთხოების მართვის პროცესში ჩართულ პირებს. მათ შეექმნებათ ნათელი წარმოდგენა არსებული ან მოსალოდნელი საფრთხეების თაობაზე და ეცოდინებათ როგორ გაუმკლავდნენ გამოწვევებს საპასუხო ქმედებებით.

კვლევის ობიექტი

ძირითადი საკვლევი საკითხები:

1. საქართველოს საჯარო ადმინისტრირების ინფორმაციული უსაფრთხოების სისტემა და მისი გამოწვევები;
2. კიბერშეტევის ტიპები, მავნე პროგრამული უზრუნველყოფა, მათი მახასიათებლები და მომდინარე საფრთხეები;
3. სახელმწიფოების წინააღმდეგ ბოლო წლების განმავლობაში განხორციელებული კიბერშეტევების შედეგად მიყენებული ზიანი;
4. საქართველოს წინააღმდეგ განხორციელებული კიბერშეტევები;
5. ინფორმაციული უსაფრთხოების საკანონდმებლო ბაზა საქართველოში;
6. საქართველოს კიბერუსაფრთხოების სტრატეგია;
7. კიბერუსაფრთხოების აქტორები და მათი როლი;
8. კიბერშპიონაჟი, მისი მიზნები, ტაქტიკა და საყურადღებო შემთხვევები;
9. საერთაშორისო გაერთიანებების (ნატო, ევროკავშირი) მიდგომა ინფორმაციული უსაფრთხოების დაცვის საკითხებთან მიმართებაში;
10. ინფორმაციული უსაფრთხოების მართვის საერთაშორისო სტანდარტები;
11. განათლების შესაძლებლობები საქართველოში ინფორმაციულ და კიბერუსაფრთხოებაში;
12. უახლესი აღმოცენებადი ტექნოლოგიები და მათი უსაფრთხოება.

კვლევისთვის გამოყენებული მეთოდები

კვლევისათვის გამოყენებულია სხვადასხვა ფართოდ გავრცელებული ანალიზის თვისობრივი კვლევის - ნარატიული და დესკრიფციული მეთოდები, რომელიც გულისხმობს წერილობითი წყაროების ანალიზს.

აღნიშნული 2 მეთოდი გამოყენებულია ნაშრომის თითოეულ თავში სხვადასხვა ლიტერატურის ანალიზისთვის, რათა დაინტერესებულ პირთათვის მიწოდებული იყოს საკვლევი ობიექტის თაობაზე არსებული შესაბამისი ყველაზე მნიშვნელოვანი ინფორმაცია.

ლიტერატურის მიმოხილვისას ვიხელმძღვანელეთ შედარებითი ანალიზის მეთოდით მათი ურთიერთშეპირისპირების და მსგავსების დადგენის მიზნით.

დისერტაციაში ქართველი ავტორების გვერდით გაანალიზებულია უცხოელი ავტორების შრომები და გამოცემები.

კიბერ და უსაფრთხოების ექსპერტებისგან საჭირო ინფორმაციის მისაღებად და გასაანალიზებლად, გარდა პირისპირ გასაუბრებისა, გამოყენებული იქნა სიღრმისეული ინტერვიუ, რომელიც გულისხმობს რესპოდენტის მოსაზრებებზე დაფუძნებულ მსჯელობას.

საკვლევი თემის ჰიპოთეზა

ინფორმაციული უსაფრთხოების კომპრომეტირება წარმოადგენს გლობალურ საფრთხეს, განსაკუთრებით სახელმწიფოებისთვის. ინფორმაციაზე უნებართვო წვდომა, მისი შეცვლა ან განადგურება ვერ ჩაითვლება ნორმად. საკვლევი თემის ჰიპოთეზა მდგომარეობს შემდეგში: დღეისათვის, ინფორმაციული უსაფრთხოების განმტკიცებისთვის საჭირო პროაქტიული და რეაქტიული ღონისძიებები, რომელსაც სახელმწიფოები ატარებენ, არ არის საკმარისად ეფექტური და საჭიროა განსხვავებული მიდგომა, რომელიც მოიაზრებს სხვადასხვა ღონისძიებების კონსოლიდირებას და ინოვაციური გზების გამოცდას. აღნიშნული ჰიპოთეზის დასადასტურებლად ან უარსაყოფად, ნაშრომის ფარგლებში, პასუხი გავეცით შემდეგ კითხვებს:

- ინფორმაციული უსაფრთხოების რა გამოწვევები დგას სახელმწიფოების წინაშე;
- რა ზიანის მოტანა შეუძლია კიბერშეტევებს ქვეყნის კრიტიკული ინფრასტრუქტურისთვის და რა ასეთი შემთხვევები დადგა ბოლო წლების განმავლობაში;
- შესაძლებელია თუ არა ინფორმაციული უსაფრთხოების რისკების სრულად ელიმინირება;
- რა გამოცდილება აქვს საქართველოს კიბერშეტევებთან დაკავშირებით, რა იყო მათი მიზეზი და ტექნიკურად რა სიძლიერის იერიში მიიტანეს მასზე;
- რას უნდა ველოდოთ სამომავლოდ კიბერსივრცეში - შეტევების რაოდენობის და მათი სიმძიმის შემცირებას, თუ პირიქით;

- რა ნაბიჯებს დგამს საქართველო ინფორმაციული უსაფრთხოების უზრუნველსაყოფად საჯარო სისტემაში და სად საჭიროებს დამატებით ჩარევას;
- კიბერსაფრთხეებთან ბრძოლის რა საშუალებები გამოიყენება მოწინავე ქვეყნების მიერ და შეძლეს თუ არა მათ საფრთხეებისაგან თავდაცვის სრული უზრუნველყოფა;
- რამდენად შესაძლებელია მოწინავე ქვეყნების გამოცდილების გაზიარება საქართველოს საჯარო ადმინისტრირების სისტემაში და ეფექტურობისა და ეფექტიანობის რა ხარისხი ექნება მას.

სამეცნიერო სიახლე

ნაშრომში პირველად:

- სისტემურად განხილული და შეფასებულია საქართველოს საჯარო ადმინისტრირების ინფორმაციული უსაფრთხოების არსებული მდგომარეობა, გამოწვევები და მართვის საშუალებები.
- უახლეს (მათ შორის ბოლო თვეების) კვლევებსა და სამეცნიერო დოკუმენტაციაზე დაყრდნობით მოტანილი და გაანალიზებულია ბოლო ორი ათეული წლის განმავლობაში მომხდარი კიბერშეტევები და მათი შედეგები, გამოვლენილია პოლიტიკური, სოციალური, ეკონომიკური გავლენა და მზარდი უარყოფითი ტენდენციები.
- მიმოხილულია როგორც საქართველოს გამოცდილება, ასევე უცხო ქვეყნებში ინფორმაციული უსაფრთხოების გამოწვევებთან ბრძოლის აპრობირებული, ასევე ამჟამად დანერგვადი მეთოდები და საშუალებები.
- შეფასებულია ინფორმაციული უსაფრთხოების რისკები, გაანალიზებულია კიბერსივრცის მახასიათებლები, ბუნება, კიბერშეტევების ტიპები და ქვეყნების წინააღმდეგ არსებული ვექტორები ამ მიმართულებით.
- მეცნიერული ანალიზის საფუძველზე, შემოთავაზებულია პრობლემის გადაჭრის ინოვაციური გზები, რის გამოც, ნაშრომი, სათანადო წვლილს უდავოდ შეიტანს ინფორმაციული უსაფრთხოების კვლევის საკითხში და გაამდიდრებს არსებულ ცოდნას.

- შესწავლილია კიბერუსაფრთხოების მიმართება საჯარო ადმინისტრირების სისტემასთან. ქართულ და უცხოენოვან სამეცნიერო ლიტერატურაში კიბერუსაფრთხოებასთან დაკავშირებული ნაშრომები შეეხება ან კერძო სექტორს, ან ზოგადად ინფორმაციული უსაფრთხოების სფეროს. ჩვენ მიერ კი შესწავლის ობიექტად აღებულია სახელმწიფოს წინაშე არსებული ინფორმაციული უსაფრთხოების გამოწვევები. პრობლემების გადაჭრისა და რისკების შემცირების ახლადაღმოცენებული და ინოვაციური საშუალებები შეიძლება გავრცელდეს ორივე - კერძო და საჯარო სექტორზე.

სამუშაოს პრაქტიკული მნიშვნელობა და გამოყენების სფერო

შესაბამისი კიბერშეტევების მიმოხილვის, კიბერსივრციდან მომდინარე საფრთხეების და საქართველოს საჯარო ადმინისტრირების კიბერუსაფრთხოების ეკოსისტემის წინაშე არსებული გამოწვევების ანალიზის შედეგად, ვფიქრობთ, ნაშრომი შექმნის თეორიულ საფუძველს ქვეყნის საჯარო ადმინისტრირების სისტემის ინფორმაციული ინფრასტრუქტურის განვითარებისა და ინფორმაციული უსაფრთხოების კომპრომეტირების შემთხვევების თავიდან ასარიდებლად. მისი პრაქტიკული მნიშვნელობა გამოიხატება წარმოდგენილი რისკების თავიდან არიდების შესაძლო უკვე აპრობირებული და ინოვაციური მეთოდების გამოყენების შესაძლებლობაში.

ნაშრომის სიახლის, აქტუალურობის და კვლევის სპეციფიკიდან გამომდინარე, იგი პრაქტიკული და გამოყენებადი იქნება როგორც შესაბამისი სფეროთი დაინტერესებული პირებისთვის, ასევე საჯარო ადმინისტრირების, ინფორმაციული ტექნოლოგიების, კიბერუსაფრთხოების, უსაფრთხოების კვლევების საბაკალავრო და სამაგისტრო აკადემიური პროგრამების სტუდენტებისთვის. ასევე, ნაშრომი მნიშვნელოვანი ინფორმაციის შემცველი იქნება საქართველოს კიბერუსაფრთხოების აქტორების თანამშრომლებისთვის და გადაწყვეტილების მიმღები პირებისთვის, განსაკუთრებით უსაფრთხოების სექტორში.

სამუშაოს აპრობაცია

დისერტაციის თემაზე, საგანმანათლებლო პროგრამით გათვალისწინებული კვლევითი კომპონენტის სახით, საქართველოს ტექნიკური უნივერსიტეტის ენერგეტიკის ფაკულტეტის საწარმოო ინოვაციებისა და ოპერაციათა მენეჯმენტის დეპარტამენტში გაკეთდა პრეზენტაცია სამ კოლოქვიუმზე და წინასწარ დაცვაზე 2022 – 2023 წლებში.

გარდა ამისა, გაკეთდა მოხსენება შემდეგ საერთაშორისო სამეცნიერო კონფერენციებზე, ფორუმებზე და კიბერსწავლებებზე:

- მაისი, 2023: კიბერკონფლიქტის მე-15 საერთაშორისო კონფერენცია CyCon, ნატოს კოოპერაციული კიბერთავდაცვის დახელოვნების ცენტრი (CCDCOE), ტალინი, ესტონეთი
- მარტი, 2023: EU SecureConnect რეგიონული სამუშაო შეხვედრა: ინფრასტრუქტურის დაცვა და კიბერუსაფრთხოების გაუმჯობესება, ბუქარესტი, რუმინეთი
- ოქტომბერი, 2022: ინტერმარიუმ კიბერუსაფრთხოების ფორუმი 2022, საქართველოს თავდაცვის სამინისტრო, ევროკავშირის Cyber Security East პროექტი
- ოქტომბერი, 20222: საერთაშორისო კონფერენცია „ციფრული პარტნიორობა და მდგრადობა კიბერუსაფრთხოებაში“, ტელჩი, ჩეხეთი
- სექტემბერი, 2022: კიბერსავარჯიშო „Cyber Dawg 2022”, ატლანტა, აშშ
- აგვისტო, 2022: საზღვაო ოპერაციების ერთობლივი მართვის ცენტრის სამაგიდო სწავლება, აშშ-ს თავდაცვის საფრთხეების შემცირების სააგენტო, ბათუმი
- ივნისი, 2022: კიბერდანაშაულისა და კიბერუსაფრთხოების ექსპერტთა რეგიონული თანამშრომლობის ფორუმი, ევროკავშირის Cyber East და CyberSecurity East პროექტები, ბუქარესტი, რუმინეთი

დისერტაციის სტრუქტურა

სადისერტაციო ნაშრომი მოიცავს 155 ნაბეჭდ გვერდს: შესავალს, 5 თავს, 18 ქვეთავს, დასკვნასა და რეკომენდაციებს.

ნაშრომის ძირითადი შინაარსი

სადისერტაციო ნაშრომი „საჯარო ადმინისტრირების ინფორმაციული უსაფრთხოების გამოწვევები და მათი მართვის ინოვაციური საშუალებები“ წარმოდგენილია ოთხი ნაწილით - შესავალი, ლიტერატურის მიმოხილვა, შედეგების კვლევა და განსჯა, დასკვნა.

ლიტერატურის მიმოხილვაში წარმოდგენილია ნაშრომზე მუშაობისას შესწავლილი ქართული და უცხოური პუბლიკაციები, მონოგრაფიები და ჩატარებული კვლევების შინაარსი. ისინი საფუძვლად დაედო ინფორმაციული უსაფრთხოების მართვის საკითხის კვლევის ამჟამინდელ დონის შეფასებას. სფეროს სპეციფიკის შესაბამისად, ყურადღება გამახვილებულია უახლეს კვლევებზე, ექსპერტების მიერ მომზადებულ სტატიებზე და სამეცნიერო ნაშრომებზე.

შესავალში განსაზღვრულია საკვლევი თემის აქტუალურობა, კვლევის მიზნები და ამოცანები, მისი მეცნიერული სიახლე, კვლევის მეთოდოლოგია, თეორიული და პრაქტიკული მნიშვნელობა და ინფორმაცია ნაშრომის აპრობაციის შესახებ.

ნაშრომის ძირითადი ნაწილი წარმოდგენილია ხუთი თავით, რომელიც დაყოფილია ქვეთავებად. პირველ თავში ახსნილია ინფორმაციის როლი ციფრულ სამყაროში, ინფორმაციული უსაფრთხოების პირამიდა, მისი შემადგენელი პარამეტრები და მათი დაცვის აუცილებლობის საფუძვლები. სარწმუნო საერთაშორისო სტატისტიკაზე დაყრდნობით, ნაჩვენებია სამომავლო ტენდენციები, რომელიც ერთობ ამძაფრებს კიბერუსაფრთხოების გაძლიერების საჭიროებას როგორც საქართველოში, ისე მსოფლიო მასშტაბით, მით უფრო მე-4 ინდუსტრიული რევოლუციის და გამრღვევი ტექნოლოგიების აღმოცენების პირობებში. მოტანილია კოლექტიური თავდაცვის გამოწვევის ცნება და მიმოხილულია დასავლური სამყაროს მიერ გაღებული ძალისხმევა ამ მიმართულებით.

მეორე თავში საუბარია საქართველოს საჯარო მმართველობის ინფორმაციული უსაფრთხოების სისტემაზე. გაანალიზებულია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი და მასთან დაკავშირებით არსებული კრიტიკა, კიბერუსაფრთხოების ეროვნული სტრატეგია,

კიბერუსაფრთხოებაზე პასუხისმგებელი პირები. გაანალიზებულია ინფორმაციის დაცვის სფეროში ქვეყნების შეფასების საერთაშორისო მეთოდოლოგია და მათი მუშაობის პრინციპი. განმარტებულია ის გამოწვევები, რომელიც დგას ამჟამად ქვეყნის წინაშე ხსენებული მიმართულებით. ამ თავშივე ვეხებით იმ ძალისხმევას, რაც მიმართულია ქვეყნის მიერ უსაფრთხოების რისკების მინიმიზებისკენ.

მესამე თავში განვიხილავთ სახელმწიფოს წინააღმდეგ განხორციელებულ ყველაზე მძლავრ და ცნობილ კიბერშეტევებს, მათ შორის საქართველოზე მომართულ შემთხვევებს. საუბარი ეხება იმ პროგრამულ საშუალებებს და ტექნიკურ პოტენციალს, რომლებიც ქმნის განგაშის საფუძველს, დღევანდელი მდგომარეობით, თანამედროვე კიბერსივრცეში და რომელიც ამჟამად ყველაზე დიდი რისკია საქართველოს საჯარო ადმინისტრირების ინფორმაციული უსაფრთხოების სისტემისთვის. განხილულია შედეგები არამარტო ინფორმაციულ სისტემებზე, არამედ ფიზიკურ ინფრასტრუქტურაზე. ანალიზის შედეგად წარმოდგენილია აღნიშნული საფრთხეების თავიდან აცილების შესაძლო გამოკვლეული და ჩემ მიერ შემოთავაზებული ინოვაციური საშუალებები.

მეოთხე თავში განიხილება ინფორმაციული უსაფრთხოების კომპრომეტირების ერთ-ერთი მეთოდი - კიბერშპიონაჟი, რომელიც, ბოლო პერიოდის შემთხვევებმა ცხადყო, რომ სახელმწიფოს წინაშე არსებული კიბერსაფრთხეებიდან უმთავრესია. ყურადღება გამახვილებულია კიბერშპიონაჟის მიზნებზე, ასევე იმ მეთოდებსა და საშუალებებზე, რომლებსაც ბოროტმოქმედები იყენებენ მავნე მიზნების მისაღწევად. მიზნების დემონსტრირების პროცესში წარმოდგენილია შესაბამისი აქტუალური სტატისტიკა და ინფორმაცია ბოროტმოქმედების ტაქტიკის შესახებ. აქვე მოყვანილია კიბერშპიონაჟის ცნობილი მაგალითები და მათი შედეგები. განიხილება საქართველოს წინააღმდეგ განხორციელებული კიბერშპიონაჟის შემთხვევა, რომელიც ერთ-ერთი პირველი იყო მსოფლიოში. მსჯელობის შედეგად შედგენილია იმ შესაძლო მეთოდების ნუსხა, რითაც საჯარო სექტორში მსგავსი შემთხვევების თავიდან არიდება და მავნე შედეგების მინიმიზებაა შესაძლებელი.

მეხუთე თავში მიმოვიხილავთ ინფორმაციული უსაფრთხოების რისკების მართვის საჭიროების მიზეზებს, მის სარგებელს, რისკების მართვის პროცესს

აღიარებული სტანდარტების მიხედვით და ამ პროცესში წარმოშობილ გამოწვევებს ქართული რეალობის კონტექსტში. აქვეა შემოთავაზებული რისკების მართვის ოპტიმიზაციისთვის საუკეთესო ნაბიჯები და ინფორმაციული უსაფრთხოების რისკების შემცირების ინოვაციური საშუალებები. ბოლო ქვეთავში ვეხებით უახლეს, ინოვაციურ ტექნოლოგიებთან დაკავშირებულ რისკებს და წარმოვადგენთ ხედვას, რომლის მიხედვითაც, ისინი, უპირველესად, უნდა აღვიქვათ არა საფრთხედ, არამედ შესაძლებლობად, შევიმუშავოთ დაცვის განვითარებული ავტომატიზებული სისტემები.

ნაშრომის დასკვნით ნაწილში, ჩატარებული კვლევის, შესწავლილი ლიტერატურის, პირადი გამოცდილების, საერთაშორისო კონფერენციების და კიბერსწავლების ფარგლებში ექსპერტებთან გაცვლილი ინფორმაციის საფუძველზე, ჩამოყალიბებულია დასკვნები და შეჯამებულია ის რეკომენდაციები, რომელიც იქნება პრაქტიკულად ღირებული ინფორმაციული უსაფრთხოების მართვისთვის. თითოეული ეს გადაწყვეტა, რომელთა დიდი ნაწილი არასოდეს გამოყენებულა ქართულ საჯარო ადმინისტრირების სისტემაში, ნაშრომში არის ახსნილი, გამყარებული საერთაშორისო კვლევებით ან/და გამოცდილებით და დასაბუთებული კონკრეტული სარგებლით. მხედველობაში მიღებულია მათთან დაკავშირებით არსებული შესაძლებელი დაბრკოლებებიც.

საკვლევი თემის განხილვის თითოეულ ეტაპზე გათვალისწინებულია მისი გამოყენება მენეჯმენტის კუთხით. შესაბამისად, ყურადღება გამახვილებულია არა ტექნიკურ გადაწყვეტებზე, არამედ საუკეთესო პრაქტიკაზე, რომელიც დაგვეხმარება ინფორმაციული უსაფრთხოების ადმინისტრირებაში.

თვალსაჩინოებისთვის ნაშრომში წარმოდგენილია ნახაზები და ცხრილები, რომელთა ნაწილი ჩემ მიერაა შედგენილი, ნაწილი კი მოტანილია უახლესი, სფეროს აღიარებული ექსპერტების მიერ მომზადებული კვლევებიდან და ანგარიშებიდან.

კვლევის ეტაპზე გათვალისწინებულია ქართული, ევროპული და ამერიკული გამოცდილება. ინფორმაციული უსაფრთხოების არსებული გამოწვევების დაძლევის გზებზე ექსპერტებთან ვისაუბრე საერთაშორისო სამუშაო შეხვედრების ფარგლებში ჩეხეთსა და რუმინეთში, კონფერენციების ფარგლებში თბილისსა და ტალინში, ასევე კიბერსწავლების ფარგლებში ატლანტაში, აშშ.

ნაშრომი საინტერესო იქნება როგორც სამთავრობო, ასვეე კერძო სექტორის წარმომადგენლებისთვის, ვინაიდან ინფორმაციული უსაფრთხოების მართვის წარმოდგენილი ინოვაციური საშუალებები დანერგვადია ორივე სექტორში. მითუმეტეს, რომ, აქვე, კვლევით შესწავლილია კერძო-საჯარო პარტნიორობის ევროპული მექანიზმები და შემოთავაზებულია ქართულ რეალობაში დანერგვის შესაძლებლობა. კვლევა არანაკლებ გამოყენებადი იქნება აკადემიური სფეროს წარმომადგენლებისთვის.

დასკვნა

როგორც ქართული, ისე უცხოური გამოცდილების გაანალიზების შედეგად, ვხედავთ, რომ ინფორმაციული უსაფრთხოების სათანადო დონეზე დაცვა ნებისმიერი ქვეყნისთვის ნომერ პირველი თუ არა, ერთ-ერთი უმნიშვნელოვანესი ამოცანაა XXI საუკუნეში, რათა სახელმწიფო არ დადგეს ისეთი რეპუტაციული, ფინანსური, საოპერაციო თუ უსაფრთხოების პრობლემების წინაშე, რომელიც კიბერშეტევებს ახასიათებს.

განხილული საყურადღებო შემთხვევები გვიჩვენებს, რომ კიბერუსაფრთხოება ეროვნული უსაფრთხოების ქვაკუთხედია და სახელმწიფომ დიდი ძალისხმევა უნდა გაიღოს ინფორმაციული უსაფრთხოების გაძლიერებისთვის, რათა შესაბამისი რისკები მინიმუმამდე იყოს შემცირებული. აღნიშნულს კი სჭირდება სფეროს მმართველობა, რომელშიც პროცესები უნდა იყოს სტანდარტიზებული და პასუხობდეს უახლეს გამოწვევებს კიბერსივრცეში.

საქართველოს ნამდვილად აქვს წინგადადგმული ნაბიჯები ინფორმაციული უსაფრთხოების ადმინისტრირების მიმართულებებით, რისი ყველაზე ნათელი მაგალითიც ინსტიტუციური განვითარებაა. თუმცა, 2020-იან წლებში, ჩვენ მიერ აღწერილი ძალისხმევაც ვერ იქნება საკმარისი აღმოცენებად საფრთხეებთან გასამკლავებლად. ინდუსტრია 4.0-ის და მისი დამახასიათებელი სერვისების მრავალფეროვნებიდან გამომდინარე, დამოკიდებულება ინფორმაციულ ტექნოლოგიებზე უფრო და უფრო იზრდება და ვხედავთ, რომ ფიზიკური სახით ინფორმაცია საჯარო ადმინისტრირების პროცესში უფრო და უფრო ნაკლებად გვხვდება, ხოლო ის ნაწილი, რომელიც ჯერ კიდევ ამგვარი სახით არსებობს, ნელ-ნელა ციფრულდება. ეს ხაზს უსვამს ინფორმაციის დაცვის პროცესში კიბერუსაფრთხოების როლს და კიბერშპიონაჟს, როგორც უმთავრეს საფრთხეს სახელმწიფოს ინფორმაციული ინფრასტრუქტურის წინააღმდეგ.

კვლევის ფარგლებში განაალიზებული მაგალითებისა და საერთაშორისო სტატისტიკის საფუძველზე შეიძლება ითქვას, რომ საბოლოო მომხმარებლები - დასაქმებულები, არიან თავდაცვის წინა ხაზზე, რის გამოც, ინფრასტრუქტურის დაცვის საკვანძო მიმართულება სწორედ პერსონალის ცნობიერების ამაღლება უნდა

იყოს, რომ ისინი არ გახდნენ ფიშინგ-შეტევების მსხვერპლი და არ გაამჟღავნონ პირადი და სენსიტიური ინფორმაცია. როდესაც დასაქმებულს ესმის პოტენციური საფრთხე, ასევე აქვს ცოდნა იმ საშუალებების შესახებ, რითაც ხდება ინფორმაციული უსაფრთხოების რისკების შემცირება, ის უკვე ნაკლებად მოწყვლადია და შეუძლია თავიდან აირიდოს ამგვარი შეტევები, რაც საბოლოოდ ხელს უშლის მოწინააღმდეგე სახელმწიფოს მიერ დაფინანსებულ ბოროტმოქმედებს მიზნების მიღწევაში.

ნაშრომის შესავალში წარმოდგენილ კითხვებზე კვლევისა და მსჯელობის შედეგად გაცემული პასუხებით დასტურდება ჩვენი ჰიპოთეზა: დღეისათვის, ინფორმაციული უსაფრთხოების განმტკიცებისთვის საჭირო პროაქტიული და რეაქტიული ღონისძიებები, რომელსაც სახელმწიფოები ატარებენ, არ არის საკმარისად ეფექტური და საჭიროა განსხვავებული მიდგომა, რომელიც მოიაზრებს სხვადასხვა ღონისძიებების კონსოლიდირებას და ინოვაციური გზების გამოცდას. შესაძლო ღონისძიებები და ინოვაციურ გზები აღწერილია დისერტაციის სხვადასხვა თავებში, რომლებიც წარმოდგენილია: სფეროში პირადი გამოცდილების, კვლევის, სიღრმისეული ინტერვიუს, ქართული და უცხოური ლიტერატურის შესწავლის, ადგილობრივ და უცხოელ ექსპერტებთან გასაუბრების, საერთაშორისო კონფერენციებში, სამუშაო შეხვედრებსა და სწავლებებში მონაწილეობის შედეგად. გადაწყვეტის შემოთავაზებული გზები მოითხოვს გარკვეულ ფინანსურ რესურსს, გადაწყვეტილებებს მმართველობით დონეზე, პროცესების ადმინისტრირებას, აგრეთვე, რიგ შემთხვევაში, საკანონმდებლო ცვლილებებს, რისთვისაც სახელმწიფო, კერძო სექტორთან და საზოგადოებასთან ერთად, მზად უნდა იყოს. ნაშრომში წარმოდგენილი, გამოკვლეული, უცხო ქვეყნების მიერ აპრობირებული, და ინოვაციური გადაწყვეტის გზების შეჯამებას კი ქვემოთ წარმოგიდგენთ.

რეკომენდაციები:

1. საქართველოში არსებულმა კიბერაქტორებმა ზედმიწევნით სწორად უნდა შეასრულონ კანონით დადგენილი ნორმები და ვალდებულებები, თუმცა, სფეროს განვითარების ტემპის პროპორციულად, ქვეყანამ

აუცილებლად უნდა გაითვალისწინოს წარსული გამოცდილება საქართველოს კანონის „ინფორმაციული უსაფრთხოების შესახებ“, ასევე კიბერუსაფრთხოების ეროვნული სტრატეგიის დაგვიანებულ ცვლილებასთან დაკავშირებით, ასევე პარტნიორი და სხვა ქვეყნების ძალისხმევა ამ მიმართულებით და პირველივე საჭიროებისთანავე განაახლოს აღნიშნული კანონი და ამ სფეროს სრული საკანონმდებლო ბაზა;

2. გამოცდილება, რომელიც გვქონდა 2012 წლის „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით განსაზღვრული ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შეუსრულებლობასთან დაკავშირებით, უნდა იყოს გათვალისწინებული და საჭიროა დაწესდეს შესაბამისი, გონივრული ვადა, თითოეული კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში, რომელიც დაეფუძნება ამ სუბიექტის კრიტიკულობის ხარისხს, მისი ინფორმაციული სისტემების სიდიდეს და სხვა მნიშვნელოვან პარამეტრებს. მინიმალური მოთხოვნები უნდა პასუხობდეს აღნიშნულ პარამეტრებს, და არა აუცილებლად კონკრეტულ საერთაშორისო სტანდარტს;
3. საჭიროა ინფორმაციის გაცვლა და შესაბამისი გადაწყვეტილებების მიღება ისეთი მავნე პროგრამული უზრუნველყოფის შესახებ, რომელიც მიმართულია ფიზიკური ინფრასტრუქტურის განადგურებისკენ. მიზანშეწონილია კიბერშეტევების კლასიფიკაციის გადახედვა და ხსენებული ტიპის პროგრამული უზრუნველყოფის ცალკე გამოყოფა;
4. ცნობიერების ამაღლების პროგრამებმა უნდა მოიცვან საჯარო სამსახურში დასაქმებულთა ყველა რგოლი, მათ შორის უმაღლესი რგოლის მენეჯმენტი. ინფორმაციული უსაფრთხოების საკითხებზე ცნობიერების ასამაღლებლად უნდა დაიგეგმოს და აღსრულდეს სხვადასხვა სახის პროგრამები, რომელსაც ექნება მაღალი ხელმისაწვდომობა. ეს შეიძლება იყოს ლექციები, დისტანციური კურსები თუ სხვა ღონისძიებები;

5. კიბერუსაფრთხოების საკითხებზე ცნობიერების ამაღლების პროგრამებს აუცილებლად უნდა ჰქონდეს სავალდებულო ხასიათი. მათი შინაარსი კი უნდა იყოს მორგებული ცოდნის ყველა დონის მქონე პირისთვის. ამასთან, კიბერჰიგიენის საკითხები აუცილებლად უნდა იყოს ინტეგრირებული ზოგადსაგანმანათლებლო დაწესებულებების სასწავლო გეგმაში;
6. მეტი პირის მიერ დაინტერესების მიზნით, საჭიროა კიბერრეზერვის პროექტზე ინფორმირებულობის ზრდა საზოგადოებაში, მათ შორის კერძო სექტორთან თანამშრომლობის გზით. კიბერრეზერვის პროექტის სარგებლიანობა და ეფექტურობა უნდა შეფასდეს უწყებათაშორისო სწავლებების პირობებში, როგორიცაა „დიდგორი“;
7. პრიორიტეტად უნდა დასახელდეს ინფორმაციული უსაფრთხოების საბაკალავრო და სამაგისტრო პროგრამების შემუშავება, რომელიც იქნება ფინანსურად ხელმისაწვდომი დაინტერესებული პირთა ფართო წრისთვის. აქვე მნიშვნელოვანია საბაკალავრო პროგრამის არსებობა სახელმწიფო ენაზე;
8. საქართველოს განათლებისა და მეცნიერების სამინისტრომ მხარი უნდა დაუჭიროს და გამარტივებული აკრედიტაციის პროცესი შესთავაზოს პრიორიტეტულ დისციპლინას უმაღლეს საგანმანათლებლო დაწესებულებებში (ინფორმაციული უსაფრთხოება, კიბერუსაფრთხოება);
9. აუცილებელია სახელმწიფო შესყიდვების პროცესში ინფორმაციული უსაფრთხოების საკითხების გათვალისწინება. აღნიშნული, სასურველია, მოხდეს საკანონმდებლო დონეზე;
10. რეკომენდებულია ქვეყანაში ინფორმაციულ უსაფრთხოებაზე პასუხისმგებელი პირები ჩაერთონ კომპიუტერული უსაფრთხოების ინციდენტებთან დაკავშირებულ ინფორმაციის გაცვლის საერთაშორისო პლატფორმებში, როგორიცაა FIRST, NATO MISP, Trusted Introducer… საერთაშორისო თანამშრომლობა უნდა გაღრმავდეს ნატოსა და ევროკავშირთან;

11. მიზანშეწონილია ინფორმაციის გაცვლის ეროვნული პლატფორმის შექმნა, რომელშიც ჩართულნი იქნებიან კრიტიკული ინფორმაციული სისტემის სუბიექტები როგორც საჯარო, ასევე კერძო სექტორიდან. ის შეიძლება განხილული იყოს კერძო-საჯარო პარტნიორობის კუთხით და გათვალისწინებული უნდა იყოს ევროპული გამოცდილება, მაგ.: ENISA-ს მოდელი;
12. კიბერშპიონაჟის რისკის თავიდან ასარიდებლად, მიზანშეწონილია კონტროლის მექანიზმების დანერგვა, რომელმაც ჰპოვა საერთაშორისო აღიარება და ასახულია Verizon-ის ხსენებულ კვლევაში;
13. იმის გათვალისწინებით, რომ სფეროს ყველაზე მაღალკვალიფიციური სპეციალისტები, მიჩნეულია, რომ დასაქმებულნი არიან კერძო სექტორში, საჭიროებისამებრ, მოძიებული უნდა იქნეს შეღწევადობის ტესტირების მომსახურების შესაძლებლობა საჯარო დაწესებულებისთვის. აქ გათვალისწინებული და თავიდან არიდებული უნდა იყოს ინფორმაციის კონფიდენციალურობის კომპრომეტირების შემთხვევები;
14. საჭიროების შემთხვევაში, ხარჯ-ეფექტიანობის საფუძველზე, საჯარო დაწესებულებებმა შეიძლება განიხილონ ინფორმაციული უსაფრთხოების აუთსორსინგი. გათვალისწინებული უნდა იყოს ამგვარი მომსახურების სარგებელი და მომსახურების მიღებამდე უნდა მოხდეს სტრატეგიული საკითხების შეთანხმება, დადასტურდეს მომსახურე კომპანიის მონიტორინგის შესაძლებლობა, პასუხისმგებელი პირების კვალიფიკაცია და სწორად განისაზღვროს ხელშეკრულების თანხა;
15. ინფორმაციულ უსაფრთხოებასთან დაკავშირებული უმთავრესი გადაწყვეტილებები უნდა იყოს მიღებული მმართველი რგოლის მიერ, რომელსაც, თავის მხრივ, უნდა ესმოდეს იუმს-ის არსი, დანიშნულება და საჭირო რესურსების გამოყოფის მნიშვნელობა;
16. ინფორმაციული უსაფრთხოების მართვისთვის საუკეთესო პრაქტიკაა საერთაშორისო სტანდარტების გამოყენება და უნდა მოხდეს სწორი მეთოდოლოგიისა და საშუალებების არჩევა. თუმცა, მხოლოდ ორგანიზაციაზეა დამოკიდებული ის, თუ რომელ კონკრეტულ შეარჩევს

თავისი ამოცანების, საჭიროებების, საქმიანობის სფეროს და შესაძლებლობების მიხედვით. აგრეთვე საჭიროა პერსონალის ჩართვა, რომელიც არ შემოიფარგლება ინფორმაციული უსაფრთხოების მენეჯერით;

17. მეტი ყურადღება უნდა დაეთმოს კიბერდაზღვევის იდეას. მიუხედავად იმისა, რომ კიბერდაზღვევის გადაწყვეტა ინფორმაციის გაჟონვის შემთხვევაში, ვერ შეძლებს ამგვარი მავნე შედეგის მინიმიზებას, ის დაეხმარება ორგანიზაციას სისტემების აღდგენასთან დაკავშირებული ხარჯების დაფარვაში;
18. სახელმწიფომ და აკადემიურმა დაწესებულებებმა უნდა წაახალისონ ინდუსტრია 4.0-ის უახლესი ტექნოლოგიების კვლევა, ვინაიდან ეჭვებს ამგვარი ტექნოლოგიების რისკებთან დაკავშირებით, აქვს რეალური საფუძველი;
19. ხელოვნური ინტელექტი და სხვა ციფრული ტექნოლოგიები, ასევე მათთან დაკავშირებული ეჭვები და მათგან მომდინარე საფრთხეები (ასეთის არსებობის შემთხვევაში) გათვალისწინებული უნდა იყოს ეროვნული კანონმდებლობის და უსაფრთხოების სტრატეგიების შედგენა-გაახლების დროს. ამის მიზანია როგორც ინფორმაციის დაცვა, ასევე გამჭვირვალობის უზრუნველყოფა და ხელოვნური ინტელექტის მიერ მოგროვებული ინფორმაციის არამიზნობრივი გამოყენება;
20. უახლესი ტექნოლოგიების დანერგვისას სახელმწიფო სისტემებში უნდა გავითვალისწინოთ რისკების შემცირების ისეთი საშუალებები, როგორიცაა ძლიერი დაშიფვრა, საიმედო პაროლების გამოყენება, წვდომის კონტროლი, საფრთხეების შეფასება, მოწყვლადი ადგილების გამოვლენა და დაცვა. აქვე უდიდესი მნიშვნელობა უნდა მიენიჭოს ტრენინგსა და განათლებას;
21. და ბოლოს, აუცილებელია, რომ თანამედროვე სამყაროში ქვეყნებმა, თუნდაც თანამშრომლობის შედეგად, ინფორმაციული უსაფრთხოების რისკებთან ბრძოლისთვის სფეროს სპეციალისტებისთვის შექმნან შესაძლებლობა და უზრუნველყონ მათი მხარდაჭერა, რომ მივიღოთ

კიბერსაფრთხეებთან ბრძოლის ახალი, ინოვაციური, ტექნიკური და არატექნიკური გზები. მოცემული გზები უნდა წარმოადგენდეს გადაწყვეტას კიბერშეტევების ჩამოთვლილ ტიპებთა ფართო სპექტრისთვის, ვინაიდან კიბერშეტევების ახალი საშუალებები, პროგრამული თუ არაპროგრამული სახით, ძალიან დიდი სისწრაფით აღმოცენდება და ჩვენ არ გვაქვს იმის ფუფუნება, რომ საფრთხეს ვებრძოლოთ უმძიმესი შედეგის დადგომის შემდეგ.

დისერტაციის თემაზე გამოქვეყნებული სტატიები:

1. შეყელაძე ა. კიბერუსაფრთხოება, როგორც ეროვნული უსაფრთხოების ქვაკუთხედი XXI საუკუნეში და მისი გამოწვევები. „მეცნიერება და ტექნოლოგიები“, 2022, №3(740), გვ.7-18;

2. Shekeladze A. Georgian experience of developing cyber capabilities in the defence field. Journal of Defense Resources Management, 2022, №13:2, pp.25-34;

3. შეყელაძე ა. ინფორმაციული უსაფრთხოების რისკების მართვა: სტანდარტები და გამოწვევები. Scientific&practical cyber security journal, 2022, №3, გვ.25-34;

4. შეყელაძე ა. კიბერშპიონაჟის მიზნები, ტაქტიკა და მისი საფრთხის მართვის საშუალებები საქართველოს საჯარო ადმინისტრირების სისტემაში. სტუ-ის შრომები, 2022, №3(525), გვ.186-198.

Abstract

The Ph.D. thesis "Information Security Challenges in Public Administration and Innovative Ways of Response" consists of 4 parts – introduction, literature review, results research and judgment, conclusions.

Literature review covers analysed Georgian and foreign publications, books and the research content. They became the basis to assess the research level of information security management. Due to the specificity of the sphere, the attention is drawn on the newest research, statistics presented by experts and scientific papers.

Introduction defines the relevancy of the research topic, research goals and tasks, its scientific novelty, research methodology, theoretical and practical significance and information about the approbation of work.

The main part of the paper is presented with 5 chapters, which are divided into sub-chapters. The first chapter defines the role of information in the digital universe, information security pyramid, its parameters and the inevitability to defend them. Based on the trustworthy statistics, the future trends are demonstrated, which highlights the necessity to bolster cyber security not only in Georgia, but also throughout the world, especially within Industry 4.0 revolution and emerging breaking technologies. The review of the western efforts towards the concept of collective defence will also be found here.

The Georgian information security system is covered in the second chapter. Georgian law on Information Security is analysed here along with the critics around it, as well as the national cyber security strategy and the subjects responsible for cyber security. The international methodology for assessing the countries in the sphere of information security is presented here together with the existing challenges. Here we also refer to the efforts which the country makes to minimize security risks.

The third chapter is about the biggest and most famous cyber attacks against countries, including Georgia. Attention is drawn on the software and technical potential, which is alarming, now, in the modern cyber sphere and which is the biggest risk for the Georgian public administration information system. The consequences are analysed not only on the information systems, but also on the physical infrastructure. Based on analysis, the possible studied and innovative ways are mentioned to avoid the threats.

The fourth chapter covers cyber espionage, which, based on the recent cases, was demonstrated to be the major cyber threat for the states. Attention is drawn on the aims of cyber espionage, methods and means, which the perpetrators use to achieve malicious goals. When demonstrating aims, we present relevant statistics and information about the tactics of the malicious actors. The most famous examples and the consequences of cyber espionage is also covered here, along with case against Georgia, one of the first ever. Based on discussion, we present the list of possible methods, useful to stay away from such cases and minimize harmful consequences.

Information security risk management necessity is discussed in the fifth chapter, together with its benefits, process of management based on the approved international standards and the challenges coming up in this way in Georgian context. Here, the best practice and innovative ways are demonstrated to optimize management and minimize risks. In the last subchapter, we cover the risks associated with the latest, innovative technologies and present the view, based on which they should be regarded as the opportunity to establish the enhanced automated systems of security, rather than the threat.

In the final part of work, based on the performed researched, studied literature, personal experience, exchanged information via international conferences and cyber exercise, the conclusions and recommendations are summarized, which will be practically valuable to manage information security. Each of these solutions, the major part of which has never been examined in the Georgian public administration system, is explained, strengthened with international research and/or experience and supported with specific benefits. The possible existing obstacles are also envisaged.

On each step of discussing the research topic, we take into consideration its use from the management perspective. Therefore, the attention is drawn not on the technical solutions, but on the best practice to administer the information security.

To provide clarity, tables and drawing are introduced, part of which is made by me and others are referenced from recent researches and reports drafted by acknowledged experts of the sphere.

While performing research, Georgian, European and American experience is foreseen. I had discussions on possible ways of overcoming the existing information security challenges with experts on international workshops in Czech Republic and Romania, on the international conferences in Tbilisi and Tallinn, also when participating in the cyber exercise in Atlanta, USA.

The piece of work will be beneficial for representatives from both government and private sectors, as the innovative ways of managing information security can be implemented in each sector. Additionally, the mechanisms for public-private partnership is studied and the opportunity of implementing in the Georgian reality is offered. The research will be no less interesting for the academic sphere representatives.