ვლადიმერ სვანაძე

კიბერსივრცის ახალი გამოწვევები და საქართველო

საქართველოს უნივერსიტეტის
გ ა მ ო მ ც ე მ ლ ო ბ ა

წიგნი წარმოადგენს მეორე ქართულენოვან გამოცემას კიბერუსაფრთხოებისა და ინფორმაციული უსაფრთხოების მიმართულებით. მოცემული დარგით დაინტერესებული საზოგადოება წიგნში გაეცნობა კიბერსივრცეში მიმდინარე მნიშვნელოვან მოვლენებსა და არსებულ ახალ გამოწვევებს როგორც საქართველოში, ისე გლობალურ დონეზე. ასევე ინფორმაციას მიიღებს საერთაშორისო დონეზე არსებულ ტერმინთა განმარტების თაობაზე და, ამავდროულად, საშუალება ექნება თავის საქმიანობაში გამოიყენოს წიგნის ბიბლიოგრაფიის ნაწილში მოცემული საკმაოდ მდიდარი ლიტერატურული მასალა.

წიგნი საინტერესო იქნება იმ ადგილობრივი სამეცნიერო წრეების წარმომადგენელთათვის, რომლებიც აპირებენ კიბერუსაფრთხოებისა და ინფორმაციული უსაფრთხოების უფრო სიღრმისეულ შესწავლას. აგრეთვე, შეიძლება გამოყენებულ იქნეს როგორც სახელმძღვანელო საბაკალავრო, სამაგისტრო და სადოქტორო სასწავლო პროგრამების სტუდენტებისთვის.

წიგნი გახდება მოცემული დარგით ქართულ ენაზე საგამომცემლო საქმიანობისა და ტრადიციის დანერგვის ბიძგის მიმცემი, რაც თავს მხრივ საფუძველს ჩაუყრის ქართულ ენაზე კვლევითი მიმართულებისა და სასწავლო პროცესის განვითარებას.

რედაქტორი მარინა ჟღენტი

ყდის დიზაინერი და კომპიუტერული უზრუნველყოფა თათია ქვლივიძე

მისამართი: კოსტავას ქ. 77, თბილისი 0171, საქართველო
ტელ.: 032 2 55 22 22

დაიბეჭდა საქართველოში

ISBN 978-9941-9708-1-8

წიგნი ეძღვნება ჩემი მშობლების ნათელ ხსოვნას.....

სარჩევი

წინასიტყვაობა

წინამდებარე წიგნი მეორე ქართულენოვანი გამოცემაა და მიმაჩნია, რომ ქვეყნის კიბერუსაფრთხოების განვითარებაში ის სათანადო ადგილს დაიკავებს, ისე, როგორც ეს შეძლო ასევე ჩემი თანაავტორობით გამოცემულმა პირველმა ქართულენოვანმა წიგნმა „კიბერ თავდაცვა“: კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები (ნაშრომების და სტატიების კრებული), რომელიც მიჩნეულ იქნა აკადემიურ დონეზე შედგენილ, პირველ სრულყოფილ გამოცემად კიბერსივრცისა და მასთან დაკავშირებილი სირთულეებისა და გამოწვევების შესახებ.

მკითხველი, გარდა იმისა, რომ წიგნში გაეცნობა კიბერსივრცეში მიმდინარე მნიშვნელოვან მოვლენებსა და ახალ გამოწვევებს კიბერუსაფრთხოების მიმართულებით საქართველოში არსებული ვითარებისა და პრობლემების შესახებ, ასევე ინფორმაციას მიიღებს საერთაშორისო დონეზე არსებულ ტერმინთა განმარტების თაობაზე და, ამავდროულად, საშუალება ექნება თავის საქმიანობაში გამოიყენოს წიგნის ბიბლიოგრაფიის ნაწილში მოცემული საკმაოდ მდიდარი ლიტერატურული მასალა.

პირველი ქართულენოვანი წიგნის გამოცემის შემდეგ დაახლოებით შვიდი წელი გავიდა. მოცემულ პერიოდში კიბერუსაფრთხოებამ საკმაოდ დიდი ცვლილებები განიცადა, გაჩნდა ახალი რეალიები და საფრთხეები, კიბერსივრცე დადგა სრულიად ახალი გამოწვევების წინაშე, როგორც გლობალურ, ისე რეგიონალურ და ეროვნულ დონეზე. ეს მოვლენები პირდაპირ კავშირშია ინფორმაციული ტექნოლოგიების, ინტერნეტისა და ინტერნეტ ტექნოლოგიების სწრაფ განვითარებასთან, ხოლო პანდემიამ ეს პროცესი კიდევ უფრო დააჩქარა. სწრაფად მიმდინარე პროცესებს შეიძლება დავაბრალოთ ასევე ის გარემოებაც, რომ წინამდებარე წიგნში შეიძლება ვერ მოხვდა კიბერსივრცეში მიმდინარე ის სიახლეები და მოვლენები, რომლებსაც წიგნზე მუშაობის დროს ჰქონდა ადგილი.

პირადად მე დიდ მნიშვნელობას ვანიჭებ კიბერუსაფრთხოების მიმართულებით ქართულ ენაზე საგამომცემლო საქმიანობის წარმოებასა და მის განვითარებას. მიმაჩნია, რომ ამით საფუძველი ეყრება საქართველოში მოცემული დარგით დაინტერესებული უფრო ფართო მასებისთვის ხელმისაწვდომობასა და სამეცნიერო დონეზე ქვეყნისთვის მნიშვნელოვან კიბერუსაფრთხოების განვითარების აუცილებელ პროცესს, რაც საშუალებას იძლევა გაიზარდოს აკადემიური ხარისხი.

წიგნი განკუთვნილია როგორც მოცემული დარგის სპეციალისტებისთვის, ისე იმ დაინტერესებული პირებისთვის, რომლებსაც სურთ ამ მიმართულებით შეიძინონ გარკვეული ცოდნა და მიიღონ ინფორმაცია. წიგნი შეიძლება გამოყენებულ იქნას როგორც სასწავლო სახელმძღვანელო უმაღლესი განათლების ყველა საფეხურის (ბაკალავრიატი, მაგისტრატურა, დოქტორანტურა) სტუდენტებისთვის სასწავლო პროცესში, ასევე ცალკეული მეცნიერ - მკვლევარების მიერ სამეცნიერო საქმიანობაში. აგრეთვე, თავისი ინფორმაციული დატვირთულობიდან გამომდინარე, წიგნი ასევე სასარგებლო და გამოსადეგი იქნება როგორც საკანონმდებლო და აღმასრულებელი ხელისუფლების, ისე კერძო, სამოქალაქო სექტორისა და აკადემიური წრეების წარმომადგენლებისთვის.

და ბოლოს, დიდი მადლობა მინდა გადავუხადო საქართველოს უნივერსიტეტს მხარდაჭერისთვის.

ავტორისგან

შესავალი

ბოლო ორ ათწლეულში მსოფლიოში საინფორმაციო ტექნოლოგიების განვითარებისა და მოხმარების არნახული ზრდა შეინიშნება, რასაც „ინფორმაციული აფეთქება“ უწოდეს. პრაქტიკულად არავის შეუძლია გვერდი აუაროს ინფორმაციულ ქსელებში ჩართვასა და მათ გამოყენებას, როგორც პირად, საყოფაცხოვრებო, ისე პროფესიულ გარემოში. ინტერნეტი, რომელიც სამეცნიერო მონაცემების გაცვლის მიზნით შეიქმნა, ამჟამად მსოფლიო ეკონომიკის მხარდამჭერ ერთ - ერთ ძირითად საშუალებას წარმოადგენს. თუმცა, გლობალური ქსელების განვითარების პოზიტიურ ასპექტებს თან ახლავს მათი უსაფრთხოების უზრუნველყოფის პრობლემაც. თუ ადრე საზოგადოებრივი კეთილდღეობა და ეკონომიკური სტაბილურობა გადაცემის ქსელების მონაცემებისა და გამოთვლითი მომსახურების გამართულ მუშაობას ეყრდნობოდა, რომლის სანდოობის მაჩვენებელი საკმაოდ დიდი იყო, დღეს ის ინტერნეტის გლობალური ქსელის გამართულ, სტაბილურ და უსაფრთხო მუშაობაზეა დამოკიდებული, რაც სხვადასხვა რისკებს შეიცავს.

ინფორმაციული სისტემების ფუნქციონირებას საფრთხე შეიძლება შეუქმნას ინტერნეტზე შეტევამ, ფიზიკური ზემოქმედების შედეგად მიყენებულმა დარღვევებმა, პროგრამული და აპარატული უზრუნველყოფის მწყობრიდან გამოსვლამ, ადამიანის, როგორც მომხმარებლის მიერ მუშაობის პროცესში დაშვებულმა შეცდომებმა. ჩამოთვლილი ფაქტორები ნათლად აჩვენებს იმ გარემოებას, თუ რამდენად რთულია კიბერუსაფრთხოების შენარჩუნება. ინტერნეტის შემქმნელები ვერასდროს წარმოიდგენდნენ, რომ ინტერნეტ ტექნოლოგიების მზარდი განვითარება წარმოშობდა ისეთ მასშტაბურ სისტემათა ერთობლიობას, რომლის უსაფრთხოება ესოდენ მნიშვნელოვან გამოწვევად გადაიქცეოდა. ამ ახალმა მეცნიერულმა მიღწევამ ბევრ სიკეთესთან ერთად, ასევე წარმოშვა ახალი საფრთხეები და საბრძოლო სივრცის ახალი ველი. ყოველდღიურად ხდება კიბერდანაშაული ინდივიდების, სხვადასხვა ბიზნესისა თუ მთავრობების წინააღმდეგ. დღეს, კიბერთავდასხმები წარმოადგენს საფრთხეს, რომლის წინააღმდეგაც ეროვნული უსაფრთხოების ექსპერტები ეძებენ უფრო ეფექტურ, თანმიმდევრულ კიბერპოლიტიკას, ქმნიან სტრატეგიულ დოკუმენტებს და თავდაცვის მეთოდებს. მოცემულ აქტივობაში მონაწილეობს კიბერსივრცეში ჩართული ყველა დაინტერესებული მხარე, ე. წ. „სტეიქჰოლდერები“ - საჯარო და კერძო სექტორები, სამოქალაქო საზოგა-

დოება და აკადემიური წრეები, ასევე ტექნიკური საზოგადოება.

გლობალური ქსელური ინფრასტრუქტურის რეფორმირებისა და უსაფრთხოების უზრუნველყოფის ძალისხმევა ჩამორჩება ინტერნეტის კონსტრუქციული თუ დესტრუქციული მიზნებით გამოყენებისა და მისი ფუნქციონირების სულ უფრო სწრაფად მზარდ პროცესს. კიბერუსაფრთხოება მოიცავს საკითხის გადაჭრის გლობალურ მასშტაბს, მაშინ, როდესაც ამ მიმართულებით ღონისძიებების დიდი ნაწილი ცალკეული ქვეყნებისა და მათი ეროვნული უსაფრთხოების პოლიტიკის ფარგლებში ხორციელდება, რაც არ არის საკმარისი, საკითხი მოითხოვს როგორც საერთაშორისო, ისე რეგიონალურ და ეროვნულ მიდგომას.

ვინაიდან ცალკეული ქვეყნები კიბერუსაფრთხოების უზრუნველყოფას დამოუკიდებლად ცდილობენ, მათ მიერ გატარებული ღონისძიებები ხშირ შემთხვევაში არ არის საკმარისი. ქვეყნები სირთულეებს აწყდებიან როგორც კიბერუსაფრთხოების კონცეპტუალურ გააზრებაში, ისე სახელმწიფო პოლიტიკასა და ტექნოლოგიურ შესაძლებლობებში, რომლებიც აუცილებელია მოცემული საკითხების გადასაჭრელად.

კიბერუსაფრთხოება ხშირად განიხილება როგორც სახელმწიფო მნიშვნელობის სტრატეგიული პრობლემა, რომელიც ეხება საზოგადოების ყველა ფენას. ამის დასტურია კიბერუსაფრთხოების გერმანული სტრატეგია, რომლის მიხედვით, „კიბერსივრცეზე დაშვების უზრუნველყოფა, ასევე კიბერსივრცეში ინფორმაციის კონფიდენციალობა და სანდოობა 21 - ე საუკუნის ერთ - ერთი მნიშვნელოვანი პრობლემა გახდა. ამიტომ კიბერსივრცის დაცვა ხდება მთავარი ამოცანა სახელმწიფოს, ეკონომიკისა და საზოგადოების, როგორც ქვეყნის, ისე საერთაშორისო დონეზე“ (გერმანიის კიბერ უსაფრთხოების სტრატეგია, 2011). ამერიკის შეერთებულ შტატებში კიბერუსაფრთხოების სახელმწიფო პოლიტიკა (NCSS - National Cyber Security Strategy) არის საშუალება, რომელიც ემსახურება სახელმწიფოს ინფორმაციული სისტემებისა და მთლიანად ინფრასტრუქტურის უსაფრთხოებისა და სანდოობის გაზრდის შესაძლებლობას. სტრატეგია ამავდროულად ხელს უწყობს კიბერსივრცეში არსებული რისკების მაქსიმალურ შემცირებას.

ზოგადად, კიბერუსაფრთხოების სტრატეგია გულისხმობს პრობლემისადმი საფუძვლიან, სტრატეგიულ მიდგომებს. კერძოდ, ხდება სახელმწიფოს მთელი რიგი მიზნების, ამოცანებისა და პრიორიტეტების იდენტიფიცირება, რომელთა მიღწევა აუცილებელია მოცემული დროის