კიბერუსაფრთხოების პოლიტიკა

საქართველოს თავდაცვის სამინისტრო
2014-2016

სარჩევი

შესავალი

ინფორმაციული და კომუნიკაციების ტექნოლოგიების განვითარებამ მნიშვნელოვნად შეუწყო ხელი ქვეყნის კიბერსივრცეში გამოწვევების, რისკების, საფრთხეებისა და მათი წყაროების წარმოქმნას. კიბერუსაფრთხოების მნიშვნელობა, მასთან დაკავშირებული საფრთხეები და გამოწვევები ასახულია საქართველოს სტრატეგიული და უწყებრივი დაგეგმვის შემდეგ დოკუმენტებში: „საქართველოს ეროვნული უსაფრთხოების კონცეფცია“, „საქართველოს საფრთხეების შეფასების 2010-2013 წ.წ. დოკუმენტი“, „თავდაცვის სტრატეგიული მიმოხილვა 2013-2016 წწ.“, „საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013-2015წწ. სამოქმედო გეგმა“, „მინისტრის ხედვა 2013-2014“, „საქართველოს ეროვნული სამხედრო სტრატეგია“, რომელთა დასკვნები და პრინციპები გათვალისწინებულია წინამდებარე დოკუმენტში.

2008-2011 წლებში საქართველოს წინააღმდეგ განხორციელებულმა ფართომასშტაბიანმა კიბერშეტევებმა ნათლად დაგვანახა კიბერუსაფრთხოების პოლიტიკის შემუშავების აუცილებლობა, რათა უზრუნველყოფილ იქნეს კრიტიკული ინფორმაციული სისტემების გამართული და უსაფრთხო ფუნქციონირება. აღნიშნულმა გარემოებამ განაპირობა თავდაცვის სამინისტროს მიერ შემუშავებულიყო კიბერუსაფრთხოების პოლიტიკა 2014-2016 წლებისათვის. წინამდებარე დოკუმენტი კიბერუსაფრთხოების დანერგვისა და შემდგომში მისი განმტკიცებისათვის საჭირო სხვადასხვა სტრატეგიისა და გეგმის საფუძველია, რომელიც განახლებადია კიბერსივრცეში მომხდარი ცვლილებებისა და მათი გავლენით გამოწვეული შედეგების გათვალისწინებით. პოლიტიკა სრულად პასუხობს კიბერსივრცეში გლობალურ გამოწვევებს და თავსებადია ნატოსა და ევროკავშირის ქვეყნების პრინციპებთან კიბერუსაფრთხოების სფეროში.

ქვეყანაში კიბერუსაფრთხოების დანერგვა და განვითარება ნატოსთან ნაკისრი ვალდებულებების ერთ-ერთი შემადგენელი ნაწილია. საქართველოს თავდაცვის სამინისტროს მიერ დასახული მიზნები და გატარებული ღონისძიებები კიბერუსაფრთხოების სფეროში ხელს შეუწყობს საქართველოს ინტეგრაციის პროცესს ევროპულ და ჩრდილო-ატლანტიკურ ორგანიზაციებში.

სახელმწიფოს ინიციატივა - უზრუნველყოს და განავითაროს კიბერუსაფრთხოება, გახლავთ მისი მხრიდან გადადგმული ერთ-ერთი მნიშვნელოვანი ნაბიჯი, რაც უზრუნველყოფს საქართველოს თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემების დაცვასა და გაძლიერებას.

წინამდებარე დოკუმენტი წარმოადგენს საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების უზრუნველყოფისთვის საჭირო მექანიზმების

ეფექტურად დანერგვისა და განვითარების ხედვას, რომელიც პასუხობს ინფორმაციული და კომუნიკაციების ტექნოლოგიების მსოფლიო გამოწვევებს კიბერსივრცეში. „კიბერუსაფრთხოების პოლიტიკა“ განმარტავს საქართველოს თავდაცვის სფეროს მიდგომებსა და პრიორიტეტებს კიბერუსაფრთხოების მიმართულებით და განსაზღვრავს ყველა იმ სტრატეგიულ მიზანს, რომელთა აღსრულებაც განაპირობებს თავდაცვის სფეროს საიმედო, ეფექტურ, სტაბილურ და უსაფრთხო ფუნქციონირებას, რაც თავისთავად ქმნის ეროვნული უსაფრთხოების მყარ საფუძვლებს.

აღსანიშნავია, რომ კიბერუსაფრთხოების უზრუნველსაყოფად მნიშვნელოვანია თავდაცვის სისტემაში შემავალი სტრუქტურული ერთეულების მჭიდრო თანამშრომლობა, ასევე უწყებათაშორისი ძალისხმევა და კოორდინირებული მუშაობა არასამთავრობო სექტორთან. კიბერუსაფრთხოების სფეროში სახელმწიფოს ერთიანი ძალისხმევის ორგანიზება ხელს შეუწყობს კიბერსივრცეში არსებული საფრთხეების პრევენციასა და კიბერინციდენტების შედეგად მიღებული ზიანის შემცირებას.

კიბერუსაფრთხოების უზრუნველყოფის მნიშვნელობა

კიბერსივრცე ქმნის ერთიან კომპლექსურ გარემოს მასში შემავალი ინფორმაციული და კომუნიკაციების ტექნოლოგიების მოწყობილობებითა და ქსელებით, რაც საშუალებას აძლევს საქართველოს თავდაცვის სამინისტროს სამოქალაქო ოფისს, შეიარაღებული ძალების გენერალური შტაბის სტრუქტურულ ქვედანაყოფებსა და სამინისტროში შემავალ საჯარო სამართლის იურიდიულ პირებს განახორციელონ სხვადასხვა ტიპის კომუნიკაცია, ძალებისა და საშუალებების მართვა.

მომავალში კიბერსივრცე კიდევ უფრო კომპლექსური და მასშტაბური გახდება, გაიზრდება სახელმწიფო სტრუქტურების დამოკიდებულება ინფორმაციულ ტექნოლოგიებზე, რაც განაპირობებს ახალი რისკებისა და საფრთხეების წარმოქმნას. სწორედ აქედან გამომდინარე, აუცილებელია კიბერუსაფრთხოების ისეთი მოქნილი მექანიზმების შექმნა, რომლებიც ეფექტურად უპასუხებენ ახლად წარმოქმნილ გამოწვევებს. კიბერუსაფრთხოების უზრუნველყოფის მნიშვნელოვან ნაწილს, აგრეთვე წარმოადგენს ახალი კიბერშეტევებისადმი ინფორმაციული სისტემების მდგრადობის ამაღლება, პრევენციული ღონისძიებების შემუშავება და გატარება.

კიბერუსაფრთხოება მოიცავს საქართველოს თავდაცვის სამინისტროს საქმიანობის ყველა იმ სფეროს, სადაც გამოიყენება ინფორმაციული ტექნოლოგიები, იქნება ეს სამხედრო/თავდაცვითი ოპერაციების დაგეგმვა, სამხედრო წვრთნების წარმოება, ლოგისტიკური მხარდაჭერა თუ სხვა, რათა უზრუნველყოფილი იქნეს ინფორმაციის მთლიანობა, ხელმისაწვდომობა და დროული გაზიარება.

კიბერსივრცეში ადგილი აქვს მიზანმიმართული, შემთხვევითი, ბუნებრივი ხასიათის ინციდენტებს. ინფორმაციული ტექნოლოგიები შესაძლებელია გამოყენებული იქნეს არამართებული ან/და კანონსაწინააღმდეგო მიზნებისათვის სხვადასხვა წყაროს მიერ. მიზანმიმართულმა კიბერშეტევამ შესაძლოა მნიშვნელოვნად შეაფერხოს კრიტიკული ინფორმაციული სისტემების გამართული ფუნქციონირება, საფრთხე შეუქმნას ქვეყნის თავდაცვისუნარიანობას და უსაფრთხოებას.

კიბერუსაფრთხოების პოლიტიკის ძირითადი პრიორიტეტები

კიბერუსაფრთხოების პოლიტიკა მოიცავს რამდენიმე მნიშვნელოვან პრიორიტეტს, რომელთა განხორციელება აუცილებელია ამ დოკუმენტით გათვალისწინებული მიზნების მისაღწევად.

კიბერუსაფრთხოების პოლიტიკის პირველი პრიორიტეტული ამოცანაა, განსაზღვროს კიბერსივრცის უსაფრთხოების უზრუნველყოფასთან დაკავშირებული სტრატეგია. პოლიტიკა აღწერს იმ პრინციპებს, რომლებიც განაპირობებენ ინფრასტრუქტურის უსაფრთხოების უზრუნველყოფას და იმ სტანდარტების დანერგვას, რომელთა გამოყენება მყარ საფუძველს შეუქმნის ინფორმაციული სისტემებისა და ქსელების ეფექტურ დაცვას თავდაცვის სფეროში. პოლიტიკა ხაზს უსვამს კიბერუსაფრთხოების წარმატებული და ოპერატიული დაცვის მიზნით ადგილობრივი სტრუქტურების მჭიდრო და აქტიურ კოორდინაციასა და მათი ჩართულობის აუცილებლობას.

პოლიტიკის მეორე პრიორიტეტული ამოცანაა საქართველოს შეიარაღებული ძალების ინფორმაციული სისტემების დაცვა პოტენციური კიბერშეტევებისგან, დაზვერვის და რადიო-ელექტრონული ბრძოლის ხერხების და საშუალებების, ფსიქოლოგიური ოპერაციების აქტიური წინააღმდეგობის საშუალებებისა და მეთოდების განვითარება.

კიბერშეტევების მზარდი რაოდენობიდან გამომდინარე, საქართველოს თავდაცვის სამინისტროს პრიორიტეტია უსაფრთხო და ადეკვატური ინფორმაციული გარემოს შექმნა, რაც სტაბილური ფუნქციონირებისა და მოქმედების საწინდარია. საქართველოს თავდაცვის სამინისტრო მზადყოფნას აცხადებს განახორციელოს ყველა საჭირო ღონისძიება კიბერუსაფრთხოების სფეროში გამოწვევების წინააღმდეგ და შექმნას მყარი პლატფორმა კიბერუსაფრთხოების შემდგომი განვითარებისათვის. კიბერსივრცის დინამიკური და სპეციფიკური ხასიათიდან გამომდინარე, ქვეყანაში დადგა საჭიროება თავდაცვის სფეროში კიბერსივრცესთან დაკავშირებული ყველა საკითხი განხილულ იქნეს თავდაცვის სამინისტროს კიბერუსაფრთხოების პოლიტიკის ჭრილში, რაც ითვალისწინებს ინტეგრირებულ ხედვასა და სტრატეგიის კოორდინირებულ განხორციელებას.

სტრატეგიული მიზნები და ამოცანები

ხედვა: საქართველოს თავდაცვის სამინისტროს სამოქალაქო ოფისის, შეიარაღებული ძალების გენერალური შტაბის სტრუქტურული ქვედანაყოფებისა და სამინისტროში შემავალი საჯარო სამართლის იურიდიული პირებისათვის ინფორმაციული და კომუნიკაციების ტექნოლოგიების სტაბილური, ეფექტური და უსაფრთხო სისტემების შექმნა და გაძლიერება, რაც მნიშვნელოვან როლს შეასრულებს ეროვნულ კიბერუსაფრთხოებაში.

მისია: შეიქმნას კიბერსაფრთხეების პრევენციისა და მათზე რეაგირების შესაძლებლობები, შემცირდეს სისუსტეები და კიბერინციდენტებით გამოწვეული ზიანი, დაცული იქნეს თავდაცვის სფეროს ინფორმაციული სისტემები.

ამოცანები:

- შეიქმნას უსაფრთხო კიბერსისტემა თავდაცვის სფეროში, მოხდეს ნდობის გენერირება ინფორმაციული ტექნოლოგიების სფეროში, შესაბამისად, გაძლიერდეს ინფრასტრუქტურული შესაძლებლობები თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტებისათვის;
- ჩამოყალიბდეს ისეთი სისტემა, რომელიც უზრუნველყოფს უსაფრთხოების განხორციელებისათვის საჭირო კონცეპტუალური დოკუმენტების შემუშავებას. აღნიშნული სისტემა შემდგომში ხელს შეუწყობს ამ დოკუმენტების გლობალური უსაფრთხოების სტანდარტებთან და საუკეთესო პრაქტიკასთან შესაბამისობაში მოყვანას;
- დაინერგოს და განვითარდეს ინფორმაციული ტექნოლოგიების უსაფრთხოების ინციდენტებზე რეაგირების 24/7 მექანიზმები, რომლებიც უზრუნველყოფენ ინფორმაციული და კომუნიკაციების ტექნოლოგიების ინფრასტრუქტურის დაცვას, მოახდენენ საფრთხეებისა და რისკების სწრაფ იდენტიფიცირებას, მათზე რეაგირებას, პრევენციული ზომების გატარებას და საჭიროების შემთხვევაში, კრიზისების მართვას პროგნოზირებადი, პრევენციული, დაცვითი, აღდგენითი მექანიზმების საშუალებით;
- გაძლიერდეს თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტების კრიტიკული ინფრასტრუქტურის დაცვა და გამართული ფუნქციონირების უზრუნველყოფა 24/7 მოქმედი მექანიზმების მიერ ინფორმაციული რესურსების შექმნის, დაუფლების, განვითარების, ოპერირების საუკეთესო პრაქტიკის გამოყენებით;
- რეგულარულად განხორციელდეს კიბერსივრცეში არსებული და პოტენციური საფრთხეების, რისკებისა და გამოწვევების კვლევა და ანალიზი. საფრთხეების გაცნობიერება და მათი პოტენციური ზემოქმედების შეფასება ხელს შეუწყობს უსაფრთხოების ზომების გაძლიერებას. საფრთხეების ანალიზისა და რისკების

კვლევის შედეგების საფუძველზე მოხდეს პრევენციული ზომების შემუშავება და გატარება თანამედროვე გამოწვევების დაძლევის მიზნით;

- პროფესიული უნარ-ჩვევების განვითარების მიზნით საგანმანათლებლო პროგრამებისა და ტრენინგების საშუალებით შეიქმნას კიბერუსაფრთხოების სფეროში სპეციალიზებული ჯგუფი;
- შეიქმნას და დამკვიდრდეს კიბერუსაფრთხოებისა და კონფიდენციალობის კულტურა, რაც საშუალებას მისცემს მომხმარებელს, იმოქმედოს ეფექტურად წინასწარ განსაზღვრული წესებით;
- ხელი შეეწყოს თანამშრომლებს, მონაწილეობა მიიღონ კიბერუსაფრთხოების სფეროსთან დაკავშირებულ სხვადასხვა საგანმანათლებლო ტრენინგებსა და პროგრამებში;
- დამყარდეს მჭიდრო თანამშრომლობა ადგილობრივ და საერთაშორისო ორგანიზაციებთან, ხელი შეეწყოს ორმხრივი და მრავალმხრივი ურთიერთობების განვითარებას;
- 2014-2016 წლების პოლიტიკის განხორციელებისათვის საქართველოს თავდაცვის სამინისტროს მიერ შემუშავებული იქნეს სახელმძღვანელო დოკუმენტები, რომლებიც მნიშვნელოვნად შეუწყობენ ხელს კიბერუსაფრთხოების უზრუნველყოფისათვის საჭირო ინფრასტრუქტურის ეფექტურად დანერგვასა და განვითარებას.

კიბერუსაფრთხოების დანერგვისათვის აუცილებელი ნაბიჯები

თავდაცვის სფეროში კიბერუსაფრთხოების პოლიტიკის წარმატებული დანერგვისთვის საჭიროა, როგორც უცხო ქვეყნების საუკეთესო პრაქტიკის გაზიარება, ასევე, შესაბამისი პროცედურული ღონისძიებების გატარება. აქედან გამომდინარე, საქართველოს თავდაცვის სამინისტროს სამოქალაქო ოფისმა, შეიარაღებული ძალების გენერალური შტაბის სტრუქტურულმა ქვედანაყოფებმა და სამინისტროს სისტემაში შემავალმა საჯარო სამართლის იურიდიულმა პირებმა უნდა გადადგან შემდეგი აუცილებელი ნაბიჯები:

- აღასრულონ აღნიშნული პოლიტიკისა და მასთან დაკავშირებული სტრატეგიებისა და პროცედურების განხორციელება. ეს პროცედურები მოიცავს იმ სტანდარტებსა და მექანიზმებს, რომლებიც უნდა დაინერგოს ინფორმაციული ინფრასტრუქტურის უსაფრთხოების უზრუნველსაყოფად;
- განსაზღვრონ ბიუჯეტი კიბერუსაფრთხოების ინიციატივებსა და კიბერინციდენტებზე საჭირო რეაგირებისთვის;
- მოახდინონ ინფორმაციული აქტივების იდენტიფიცირება და კლასიფიცირება შესაბამისი უსაფრთხოების ზომების განხორციელების მიზნით;
- ხელი შეუწყონ საუკეთესო პრაქტიკაზე დაფუძნებული უსაფრთხო აპლიკაციების/პროგრამული უზრუნველყოფის დანერგვის პროცესებს;
- შექმნან პერიოდული შეფასების სისტემა კიბერუსაფრთხოების სფეროსთან დაკავშირებული საუკეთესო პრაქტიკის, სტანდარტებისა და ინსტრუქციების საფუძველზე სხვადასხვა ცვლილების განხორციელების მიზნით;
- ხელი შეუწყონ ინფორმაციული ტექნოლოგიების სისტემებსა და ქსელებში განხორციელებულ პერიოდულ ტესტირებებს ტექნიკური და ოპერაციული უსაფრთხოების კონტროლის ზომების ადეკვატურობისა და ეფექტურობის შეფასების მიზნით;
- კომპეტენციის ფარგლებში ხელი შეუწყონ ქვეყანაში კიბერუსაფრთხოების სფეროსთან დაკავშირებული საკითხების კოორდინაციას;
- ჩამოაყალიბონ ინფორმაციის გაზიარების, კიბერინციდენტების იდენტიფიცირებისა და რეაგირების ქმედითი მექანიზმები;
- მოახდინონ არსებული მატერიალური აქტივების შესწავლა, „კიბერუსაფრთხოების პოლიტიკის“ დოკუმენტითა და „კიბერუსაფრთხოების განვითარების სტრატეგიით“ გათვალისწინებული ამოცანების შესრულებისათვის საჭირო ტექნოლოგიებისა და მატერიალური აქტივების დაგეგმვა, შეძენა, განკარგვა და მართვა.

კიბერსაფრთხეების პრევენცია და მათზე დროული რეაგირება

კიბერინციდენტების თავიდან აცილებისა და მათზე ეფექტური რეაგირებისთვის აუცილებელია ადრეული გამაფრთხილებელი სიგნალების, სისუსტეების მართვისა და საფრთხეებზე რეაგირების მექანიზმების დანერგვა. ამისათვის საჭიროა შემდეგი ღონისძიებების გატარება:

- არსებული და პოტენციური კიბერსაფრთხეების პრევენციისთვის საჭირო სიტუაციური შემთხვევების გენერირება და ინფორმაციის დროული გაზიარება აქტიური, პრევენციული, თავდაცვითი ქმედებების განხორციელების მეშვეობით;
- კიბერინციდენტებზე რეაგირება და კრიზისების მართვის კოორდინაცია კომპიუტერულ ინციდენტებზე 24/7 რეაგირების ჯგუფების მიერ;
- კრიზისების მართვის სამოქმედო გეგმის შემუშავება, რომელიც ითვალისწინებს იმ კიბერინციდენტების მართვას, რომლებიც ზეგავლენას ახდენენ კრიტიკულ ინფრასტრუქტურებზე, საფრთხეს უქმნიან საზოგადოებრივ უსაფრთხოებას ან ქვეყნის ეროვნულ უსაფრთხოებას. აღნიშნული ღონისძიება ხორციელდება კარგად კოორდინირებული მრავალდისციპლინური სტანდარტებით;
- კიბერსივრცეში არსებული ინციდენტების მართვის სიმულაციების ხელშეწყობა და მათი რეგულარული განხორციელება.

კრიტიკული ინფრასტრუქტურის დაცვა და მდგრადობა

საქართველოს თავდაცვის სამინისტროს კრიტიკული ინფრასტრუქტურის ჯეროვანი დაცვისა და მათი ქმედითი ფუნქციონირებისთვის აუცილებელია შემდეგი მნიშვნელოვანი ნაბიჯების გადადგმა:

- კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის გეგმის (ინფორმაციის ნაკადის უსაფრთხოების მარეგულირებელი მექანიზმები, ინსტრუქციები და სტანდარტები, კრიზისების მართვის გეგმა, ა.შ.) შემუშავება;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვა ცენტრალური სისტემის - კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფების 24/7 ფუნქციონირების საშუალებით;
- ფისკალური სქემებისა და წამახალისებელი მექანიზმების უზრუნველყოფა იმისათვის, რომ საქართველოს თავდაცვის სამინისტროს სამოქალაქო ოფისმა, შეიარაღებული ძალების გენერალური შტაბის სტრუქტურულმა ქვედანაყოფებმა და სამინისტროს სისტემაში შემავალმა საჯარო სამართლის იურიდიულმა პირებმა დანერგონ, გააძლიერონ და განაახლონ ინფორმაციული ინფრასტრუქტურა კიბერუსაფრთხოების ნორმების შესაბამისად;
- ინფორმაციული ტექნოლოგიების ვალიდური და სერტიფიცირებული პროდუქტების გამოყენების ხელშეწყობა;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის უსაფრთხოების აუდიტის პერიოდული განხორციელება;
- ინფრასტრუქტურის შექმნა ინფორმაციული უსაფრთხოების შესაბამისი სტანდარტების მიხედვით (ISO 27000, IS სისტემების აუდიტი, შეღწევადობის ტესტი, სისუსტეების შეფასება, აპლიკაციების უსაფრთხოების ტესტი, ვებუსაფრთხოების ტესტი).

საკანონმდებლო ინიციატივების მნიშვნელობა

წინამდებარე პოლიტიკის აღსრულებისა და განხორციელებისათვის საჭირო კომპონენტია საკანონმდებლო ბაზის დახვეწა. ინფორმაციული ტექნოლოგიების სფეროში საქართველოს თავდაცვის სამინისტრომ უნდა განსაზღვროს შესაბამისი ნორმატიული აქტების შემუშავების საჭიროება, უზრუნველყოს არსებული კანონმდებლობის საერთაშორისო ნორმებთან შესაბამისობაში მოყვანა და ამით განავითაროს და გააძლიეროს სამართლებრივი ჩარჩოები. ასევე, წინამდებარე პოლიტიკის გათვალისწინებით, საჭიროა განხილულ იქნეს საქართველოს კანონმდებლობაში, მათ შორის „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილებების შეტანის საკითხი.

საქართველოს თავდაცვის სამინისტრო აცნობიერებს ამ ღონისძიებების პრიორიტეტულობას და ხაზს უსვამს ისეთი ინიციატივების საჭიროებას, რომლებიც ქმნიან მყარ სამართლებრივ საფუძვლებს პოლიტიკის განხორციელებისა და თავდაცვის სამინისტროს კიბერუსაფრთხოების უზრუნველყოფისთვის.

კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების, ტრენინგებისა და საგანმანათლებლო პროგრამების მნიშვნელობა

საქართველოს თავდაცვის სამინისტრო აცნობიერებს, რომ კიბერუსაფრთხოების უზრუნველყოფისთვის სტრატეგიულ ნაწილს წარმოადგენს ამ სფეროში ცნობიერების ამაღლება, საგანმანათლებლო პროგრამების შექმნა და განხორციელება. ამ მიმართულებით გატარებული ღონისძიებები ხელს შეუწყობს ადამიანური რესურსების პროფესიულ განვითარებას, ახალი უნარ-ჩვევების დაუფლებას და უზრუნველყოფს საქართველოს თავდაცვის სფეროში კიბერუსაფრთხოების მიმართულებით დასახული სტრატეგიული მიზნებისა და ამოცანების ეფექტურად შესრულებას. თავდაცვის სამინისტრომ საერთაშორისო ურთიერთობების დამყარებით ხელი უნდა შეუწყოს სემინარების, ტრენინგებისა და სერტიფიცირების პროგრამების განხორციელებას, რომლის მთავარ მიზანსაც წარმოადგენს კიბერუსაფრთხოების სფეროში დასაქმებული თითოეული ადამიანის მაღალი კვალიფიკაცია.

კიბერუსაფრთხოება უნდა გახდეს საქართველოს თავდაცვის სამინისტროს მიერ ორგანიზებული სამხედრო წვრთნების შემადგენელი კომპონენტი. ძალზე მნიშვნელოვანია კიბერუსაფრთხოების წვრთნების რეგულარულად ორგანიზება და წარმოება, რაც მოიცავს, როგორც ტექნიკურ, ასევე ოპერატიულ ასპექტებსა და სტრატეგიული გადაწყვეტილებების მიღების პროცედურებს. აღნიშნული წვრთნების სისტემატურად განხორციელება უზრუნველყოფს არსებული და პოტენციური საფრთხეების დასაძლევად მზადყოფნის შეფასებას.

ურთიერთობები საერთაშორისო და ადგილობრივ დონეზე

შეუძლებელია კიბერუსაფრთხოების უზრუნველყოფა და განვითარება იზოლირებულად განხორციელდეს. დასახული ამოცანის ეფექტურად შესრულება შესაძლებელია მხოლოდ იმ შემთხვევაში, თუკი უზრუნველყოფილი იქნება მჭიდრო კოლაბორაცია საერთაშორისო და ადგილობრივ დონეზე. აქედან გამომდინარე, სახელმწიფომ უნდა განავითაროს ორმხრივი და მრავალმხრივი ურთიერთობები და აქტიურად დაუჭიროს მხარი ევროპული და ჩრდილო-ატლანტიკური ხელშეკრულების ორგანიზაციების რეკომენდაციებს, რაც ხელს შეუწყობს კიბერუსაფრთხოების უზრუნველყოფისათვის საჭირო ამოცანების შესრულებას. საქართველოს თავდაცვის სამინისტრომ ხელი უნდა შეუწყოს ინფორმაციული ტექნოლოგიების უსაფრთხოების

ინციდენტებზე რეაგირების ადგილობრივ ჯგუფებს, დაამყარონ ურთიერთობა უცხო ქვეყნების კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფებთან, რათა მოხდეს ახალი სტანდარტების, მიდგომებისა და პრინციპების ადგილობრივ დონეზე დანერგვა საქართველოს კანონმდებლობის შესაბამისად. აგრეთვე, მნიშვნელოვანია თანამშრომლობის გაღრმავება საერთაშორისო ორგანიზაციებთან სამართლებრივი კუთხით. კიბერუსაფრთხოება დინამიკური სფეროა, იცვლება შეტევების ტიპი, თავდამსხმელთა მიზნები და მოტივები, და ხშირ შემთხვევაში, ძალიან რთული ხდება, განისაზღვროს, რომელი სამართლებრივი ნორმა არეგულირებს კიბერინციდენტის კონკრეტულ შემთხვევას.

კიბერუსაფრთხოების უზრუნველყოფის უმნიშვნელოვანესი ასპექტია საერთო მხარდაჭერა - უწყებათაშორისი თანამშრომლობა და აქტიური კოორდინაცია სხვადასხვა სამინისტროებთან და კერძო სექტორთან. მსოფლიო პრაქტიკიდან გამომდინარე, არცერთ უწყებას არ შეუძლია საკუთარი ინფორმაციული და კომუნიკაციების ტექნოლოგიების სისტემების დაცვა სხვა უწყებების დახმარების გარეშე. კიბერუსაფრთხოების სფეროში აქტიური ურთიერთობების განვითარება ხელს შეუწყობს ინფორმაციის დროულ გაცვლას, გამოცდილების გაზიარებას, საერთაშორისო პრაქტიკის შესწავლასა და დანერგვას.

კიბერუსაფრთხოების მიმართულებით მრავალმხრივ ფორმატში თანამშრომლობა გაზრდის ინფორმაციული და კომუნიკაციების ტექნოლოგიების სტაბილური და უსაფრთხო სისტემის შექმნის, განვითარების და ქვეყანაში მისი ამოქმედების შესაძლებლობებს.

პოლიტიკის განხორციელება

2014-2016 წლების პოლიტიკის განხორციელებისათვის აუცილებელია, საქართველოს თავდაცვის სამინისტროს მიერ შემუშავებული იქნეს სხვადასხვა სპეციფიკური პროცედურა და სახელმძღვანელო დოკუმენტი, რაც მნიშვნელოვნად შეუწყობს ხელს კიბერუსაფრთხოების უზრუნველყოფისათვის საჭირო ინფრასტრუქტურის ეფექტურად დანერგვასა და განვითარებას. კერძოდ, პოლიტიკის დოკუმენტის მიღების შემდგომ, საქართველოს თავდაცვის სამინისტროს მიერ შემუშავდება „კიბერუსაფრთხოების განვითარების სტრატეგია“, რომელიც იქნება წინამდებარე პოლიტიკაში დასახული ამოცანებისა და მიზნების უახლოეს ორ წელიწადში რეალიზების დეტალური გეგმა. პერიოდულად მოხდება აღნიშნული დოკუმენტის განხილვა და კორექტივების შეტანა მიმდინარე პროგრესის მიხედვით.

კიბერუსაფრთხოების განვითარება ინფორმაციული ტექნოლოგიების განვითარების პირდაპირპროპორციულია, რაც გულისხმობს ახალი ტექნოლოგიებისა და მექანიზმების დანერგვას. ამ დოკუმენტით გათვალისწინებული პრიორიტეტების სისრულეში მოყვანა შეუძლებელია სახელმწიფო სტრუქტურებთან კოორდინირებული

მუშაობის, საერთაშორისო ორგანიზაციებთან მჭიდრო თანამშრომლობისა და შესაბამისი ფინანსური უზრუნველყოფის გარეშე.

პოლიტიკით განსაზღვრული ვალდებულებების შესრულება მნიშვნელოვან წვლილს შეიტანს თავდაცვის სფეროს კიბერუსაფრთხოების განვითარებისა და განმტკიცების საქმეში, რაც ქვეყნის ეროვნული უსაფრთხოების საწინდარია.

დასკვნა

კიბერუსაფრთხოების პოლიტიკა ფუნდამენტური დოკუმენტია, რომელიც ითვალისწინებს ქვეყნისთვის კიბერუსაფრთხოების შექმნის მნიშვნელობას, მის ძირითად პრიორიტეტებს, სტრატეგიულ მიზნებსა და ამოცანებს. აღნიშნული დოკუმენტი გახდება თავდაცვის სფეროში კიბერუსაფრთხოების განვითარების საფუძველი და გააერთიანებს სამთავრობო სტრუქტურებს კიბერსივრცეში არსებული რისკებისა და საფრთხეების წინააღმდეგ ბრძოლაში.

კიბერუსაფრთხოების პოლიტიკის დოკუმენტი შემუშავებულია საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს მიერ და ეფუძნება წამყვან ქვეყნებში კიბერუსაფრთხოების შესაძლებლობების შექმნისა და განვითარების მოდელს. დოკუმენტი ითვალისწინებს „ნატოს კიბერუსაფრთხოების ეროვნული სტრატეგიის სახელმძღვანელოს", ესტონეთის კიბერუსაფრთხოების ექსპერტების მიერ მომზადებული „განვითარების გეგმისა" და კიბერუსაფრთხოების სფეროში ევროკავშირის ქვეყნების პრინციპებსა და მიდგომებს.