დანართი №1

საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგია

I. შესავალი

საქართველოს ხელისუფლება მეორედ აქვეყნებს საქართველოს კიბერუსაფრთხოების ეროვნულ სტრატეგიას. 2008 წლის აგვისტოში რუსეთის ფედერაციის მიერ საქართველოს წინააღმდეგ კიბერსივრცეში განხორციელებული აგრესია და, ასევე საქართველოს მზარდი დამოკიდებულება ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე ნათლად წარმოაჩინს, რომ საქართველოს ეროვნული უსაფრთხოება ვერ შედგება კიბერსივრცის უსაფრთხოების უზრუნველყოფის გარეშე. ამრიგად, კიბერუსაფრთხოების განვითარება წარმოადგენს ეროვნული უსაფრთხოების ინტერესს.

საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგია არის კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი, რომელიც ასახავს სტრატეგიულ მიზნებს, ძირითად პრინციპებს, აყალიბებს ამოცანებს და მათ შესასრულებლად განსაზღვრავს შესაბამის აქტივობებს. ამასთან, მოცემული სტრატეგია ითვალისწინებს რა „საქართველოს საფრთხეების შეფასების 2015-2018 წლების დოკუმენტითა“ და „საქართველოს ეროვნული უსაფრთხოების კონცეფციით“ განსაზღვრულ ეროვნული უსაფრთხოების ძირითად მიმართულებებს, მიზნად ისახავს აღნიშნულ დოკუმენტებში არსებული საფრთხეების აღკვეთასა და შემცირებას, ასევე ემსახურება ქვეყნის თავდაცვისუნარიანობის განმტკიცებასა და გაძლიერებას. საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნულ სტრატეგიაზე დაყრდნობით, საქართველოს ხელისუფლება გაატარებს ღონისძიებებს, რომლებიც ხელს შეუწყობს სახელმწიფო ორგანოების, კერძო სექტორისა და სამოქალაქო საზოგადოების კიბერსივრცეში დაცულად ფუნქციონირებას, ინფორმაციული და საკომუნიკაციო ტექნოლოგიების უსაფრთხო გამოყენებასა და ქვეყანაში ეკონომიკისა და ბიზნესის შეუფერხებლად მოქმედებას.

2013 წლის მაისში მიღებულმა კიბერუსაფრთხოების პირველმა სტრატეგიამ მნიშვნელოვნად შეუწყო ხელი საქართველოს კიბერუსაფრთხოების სისტემის მდგრადობის ამაღლებას, შესრულდა რა ხსენებული დოკუმენტის სამოქმედო გეგმით გათვალისწინებული აქტივობების აბსოლუტური უმრავლესობა. შესაბამისად, წინამდებარე სტრატეგია ორიენტირებულია კიბერუსაფრთხოების სფეროს შემდგომ განვითარებაზე, განსხვავებით პირველი სტრატეგიისგან, რომლის ძირითად მიზანს წარმოადგენდა კიბერუსაფრთხოების სექტორის განვითარების ზოგადი ჩარჩოს შექმნა. ამასთან, ამ სტრატეგიის მნიშვნელოვან სიახლეს წარმოადგენს მასში კიბერთავდაცვის საკითხების ასახვა ამ სფეროს შემდგომი განვითარების მიზნით.

საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგია წარმოადგენს „ეროვნული უსაფრთხოების მიმოხილვის პროცესის ფარგლებში

შექმნილი კონცეპტუალური და სტრატეგიული დოკუმენტების პაკეტის ნაწილს. შესაბამისად, აღნიშნული სტრატეგია ეფუძნება „საქართველოს საფრთხეების შეფასების 2015-2018 წლების დოკუმენტს'' და „საქართველოს ეროვნული უსაფრთხოების კონცეფციას".

წინამდებარე სტრატეგია შემუშავდა სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭოსთან არსებული ეროვნული უსაფრთხოების კონცეპტუალური დოკუმენტების შემუშავების მაკოორდინირებელი მუდმივმოქმედი უწყებათაშორისი კომისიის მიერ.

II. საქართველოს კიბერუსაფრთხოების პოლიტიკის ძირითადი მიზნები და პრინციპები

საქართველოს მიზანია შექმნას და განავითაროს კიბერუსაფრთხოების ისეთი სისტემა, რომელიც ხელს შეუწყობს, ერთი მხრივ, ინფორმაციული ინფრასტრუქტურის დაცულობას კიბერსაფრთხეების წინაშე (სისტემის კონფიდენციალობა, მთლიანობა, ხელმისაწვდომობა) და, მეორე მხრივ, იქნება დამატებითი ფაქტორი ქვეყნის შემდგომი ეკონომიკური და სოციალური განვითარებისათვის. ინფორმაციის უსაფრთხოდ გავრცელება და ამ პროცესში მონაცემთა დაცვა ქვეყნისა და მისი მოქალაქეების ეკონომიკური ინტერესებისა და უსაფრთხოებისთვის აუცილებელი ფაქტორია.

საქართველოს სახელმწიფოსა და მისი ინფორმაციული საზოგადოების განვითარება, თითოეული მოქალაქის სოციალური და ეკონომიკური კეთილდღეობა, ჯანმრთელობა და სიცოცხლე მნიშვნელოვნად დამოკიდებულია ინფორმაციული სისტემებისა და ელექტრონული მომსახურებების უსაფრთხოების უზრუნველყოფაზე. კიბერშეტევები დიდ გავლენას ახდენს ეკონომიკის ყველა სექტორზე, აფერხებს ეკონომიკური სივრცის გამართულ ფუნქციონირებას, ამცირებს ელექტრონული სერვისების მიმართ საზოგადოებრივ ნდობას და საფრთხეს უქმნის ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების გამოყენებით ქვეყნის მდგრადი ეკონომიკური განვითარების მომავალს.

ამასთან, საქართველოს კიბერუსაფრთხოების სისტემის მიზანია კრიტიკული ინფორმაციული სისტემების მდგრადობის ამაღლება კიბერშეტევებისადმი და კიბერინციდენტებით გამოწვეული შედეგების აღმოფხვრა, ასევე ეფექტიანი ღონისძიებების გატარება პოტენციური კიბერინციდენტების პრევენციის უზრუნველსაყოფად.

საქართველო, ასევე მიზნად ისახავს გახდეს კიბერუსაფრთხოების სერვისების რეგიონული პროვაიდერი, ვინაიდან საქართველოს ტერიტორიაზეა განლაგებული რეგიონის ქვეყნების საკომუნიკაციო სისტემების ფუნქციონირებისათვის საჭირო ინფრასტრუქტურა.

ამ მიზნების მიღწევის პროცესში საქართველო ხელმძღვანელობს შემდეგი პრინციპებით:

კიბერუსაფრთხოება როგორც ეროვნული უსაფრთხოების განუყოფელი ნაწილი – საქართველოს კანონმდებლობა და ეროვნული უსაფრთხოების ფუნდამენტური კონცეპტუალური დოკუმენტები კიბერუსაფრთხოებას განსაზღვრავს, როგორც ეროვნული უსაფრთხოების პოლიტიკის შემადგენელ მიმართულებას, რომლის მნიშვნელობაც ტექნოლოგიური პროგრესის პარალელურად განუზომლად იზრდება და მასზეა დამოკიდებული სახელმწიფოს ეფექტური განვითარება.

ადამიანის უფლებათა და ძირითად თავისუფლებათა განუხრელი დაცვა და პატივისცემა – საქართველოს ხელისუფლება ითვალისწინებს ადამიანის უფლებათა განუხრელი დაცვის პრინციპებს ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და განხორციელებს პროცესში. ბუნებრივია აღნიშნული პრინციპი, ასევე მიესადაგება კიბერუსაფრთხოების პოლიტიკის შემუშავებისა და აღსრულების პროცესს, კიბერუსაფრთხოება წარმოადგეს რა ეროვნული უსაფრთხოების განუყოფელ ნაწილს.

საქართველოს მთავრობის ერთიანი მიდგომა – საქართველოს მთავრობა დიდ მნიშვნელობას ანიჭებს უსაფრთხოების პოლიტიკის და მისი კომპონენტების განხორციელების მექანიზმების ინსტიტუციონალიზაციას. ამ მხრივ, კიბერუსაფრთხოების უზრუნველსაყოფად მნიშვნელოვანია სახელმწიფო უწყებებს შორის თანამშრომლობის ისეთი მექანიზმის განვითარება, რომელიც კიბერუსაფრთხოების პოლიტიკის დაგეგმვისა და განხორციელებისას ხელს შეუწყობს საქართველოს მთავრობის ერთიან მიდგომას და სხვადასხვა სახელმწიფო უწყებების გამართულ კოორდინირებულ მუშაობას.

თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის – კიბერუსაფრთხოების უზრუნველსაყოფად არანაკლებ მნიშნელოვანია თანამშრომლობის მექანიზმის განვითარება როგორც სახელმწიფო უწყებებს, ასევე სახელმწიფო და კერძო სექტორებს შორისაც. საქართველოს კრიტიკული ინფორმაციული ინფრასტრუქტურის ძირითადი ნაწილი კერძო ბიზნესის ხელშია და ამ სფეროში არსებული გამოცდილება და ცოდნა ძირითადად თავმოყრილია კერძო კომპანიებში. გარდა ბიზნესსექტორთან თანამშრომლობისა, მნიშვნელოვანია არასამთავრობო და აკადემიური წრეების ჩართულობა კიბერუსაფრთხოების პოლიტიკისა დაგეგმვისა და განხორციელების პროცესში. აღნიშნულის გათვალისწინებით, აუცილებელია თანამშრომლობის მექანიზმის შემუშავება, რომელიც ხელს შეუწყობს, ერთი მხრივ, კრიტიკული ინფორმაციული ინფრასტრუქტურის გამართულად მუშაობას, მათ შორის, კრიზისული სიტუაციების დროს და, მეორე მხრივ, დამატებითი მასტიმულირებელი ფაქტორი იქნება ეკონომიკური განვითარებისათვის.

აქტიური საერთაშორისო თანამშრომლობა – საქართველოს მთავრობა აცნობიერებს, რომ შეუძლებელია მხოლოდ საკუთარი რესურსებით უზრუნველყოს კიბერუსაფრთხოების სფეროში არსებულ გამოწვევებთან და საფრთხეებთან გამკლავება. საქართველო წარმოადგენს მსოფლიოს დემოკრატიული საზოგადოების ნაწილს და შესაბამისად მოწყვლადია იმ საფრთხეებისა და გამოწვევების მიმართ, რომლის წინაშეც ეს საზოგადოება დგას. გამომდინარე აქედან, საქართველოს მიზანია აქტიურად ითანამშრომლოს თავის პარტნიორებთან კიბერუსაფრთხოების სფეროში

ორმხრივ და მრავალმხრივ ფორმატებში. ამასთან, კიბერსაფრთხეების ტრანსნაციონალური ბუნებიდან გამომდინარე, საქართველოს წინააღმდეგ მიმართული კიბერინციდენტების ეფექტურად აღკვეთის, პრევენციის ან/და შემცირებისთვის საჭირო მონაცემები ინახება სხვადასხვა ქვეყნის ტერიტორიაზე განლაგებულ ინფრასტრუქტურაში. შესაბამისად, ერთადერთ გზას აღნიშნულ ინციდენტებზე ეფექტური რეაგირების პროცესში წარმოადგენს აქტიური საერთაშორისო თანამშრომლობა.

ინდივიდუალური პასუხისმგებლობა – თითოეული მოქალაქე, საწარმო თუ საჯარო დაწესებულება ვალდებულია ინდივიდუალურად უზრუნველყოს მის მფლობელობასა და განკარგულებაში არსებული ინფორმაციული სისტემების უსაფრთხოება. აღნიშნული სისტემების მფლობელებმა და უშუალო მომხმარებლებმა უნდა მიიღონ ყველა საჭირო ზომა მათი უსაფრთხო ფუნქციონირების უზრუნველსაყოფად.

ადეკვატური ზომები – რისკების ანალიზისა და საერთაშორისო რეკომენდაციების შესაბამისად ისეთი პროპორციული ზომების მიღება, რომლებიც ითვალისწინებს ინფორმაციისადმი თავისუფალი, შეუზღუდავი წვდომის, ადამიანის უფლებებისა და თავისუფლებების, ასევე სხვა დემოკრატიული პრინციპების დაცვას და საჭიროა კიბერუსაფრთხოების უზრუნველსაყოფად.

III. საქართველოს კიბერუსაფრთხოების გარემო

1. არსებული მდგომარეობის მიმოხილვა

2008 წლის რუსეთ-საქართველო ომის შემდგომ, საქართველომ დაიწყო კიბერუსაფრთხოების სფეროს ეტაპობრივი განვითარება, რაც საწყის ფაზაში ძირითადად ფოკუსირებული იყო შესაბამისი ინსტიტუციური ჩარჩოს ჩამოყალიბებასა და მის შემდგომ სრულყოფაში. 2010 წელს ჩამოყალიბდა საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში შემავალი სსიპ – მონაცემთა გაცვლის სააგენტო, რომელსაც დაევალა კრიტიკული ინფორმაციული სისტემების ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა და ინფორმაციული უსაფრთხოების სტანდარტების დანერგვა. სააგენტო, ასევე ახორციელებს ერთიანი სამთავრობო ქსელი მონიტორინგს, ინფორმაციული უსაფრთხოების სფეროში პოლიტიკისა და სტანდარტების განსაზღვრას ინფორმაციული სისტემების აუდიტსა და ტესტირებას. მონაცემთა გაცვლის სააგენტოს დაქვემდებარებაში ფუნქციონირებს კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი, რომელიც საკუთარი კომპეტენციის ფარგლებში პასუხისმგებელია საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვასა და ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ საქმიანობაზე, კიბერინციდენტების გამოვლენასა და მათ აღკვეთაზე. კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი აქტიურად თანამშრომლობს საერთაშორისო პარტნიორებთან და ყოველდღიურ

რეჟიმში იღებს ინფორმაციას მსოფლიოში მიმდინარე მნიშვნელოვანი კიბერინციდენტების თაობაზე.

საქართველოს თავდაცვის სფეროში კიბერუსაფრთხოების უზრუნველყოფის მიზნით, 2014 წელს შეიქმნა თავდაცვის სამინისტროს სისტემაში შემავალი სსიპ – კიბერუსაფრთხოების ბიურო, რომელიც ახორციელებს საქართველოს სამხედრო ინფრასტრუქტურის წინააღმდეგ მიმართული კიბერინციდენტების აღკვეთასა და პრევენციას 24/7 რეჟიმში. აღნიშნულ ფუნქციათა ეფექტური აღსრულების მიზნით, ბიურო უზრუნველყოფს თავდაცვის სფეროში არსებული ინფრასტრუქტურის შესწავლას, უსაფრთხოების მექანიზმების დანერგვასა და განვითარებას.

იმის გათვალისწინებით, რომ კიბერინციდენტებთან ბრძოლის პროცესში უდიდესი მნიშვნელობა ენიჭება ეფექტურ სამართალდაცვით საქმიანობას, 2012 წლის დეკემბერში საქართველოს შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა სპეციალიზირებული დანაყოფი – კიბერდანაშაულთან ბრძოლის სამმართველო, რომელიც ახორციელებს კიბერდინციდენტების გამოძიებას მთელი ქვეყნის მასშტაბით. სამმართველო, ასევე წარმოადგენს 24/7 საერთაშორისო საკონტაქტო პუნქტს, რომელიც ასრულებს საერთაშორისო სამართალდამცავ თანამშრომლობასთან დაკავშირებულ ფუნქციებს „კიბერდანაშაულის შესახებ“ ევროპის საბჭოს კონვენციის შესაბამისად.

2015 წელს განხორციელდა შინაგან საქმეთა სამინისტროს რეფორმირება, რომელსაც გამოეყო ეროვნული უსაფრთხოების ბლოკი და ჩამოყალიბდა დამოუკიდებელ უწყებად – სახელმწიფო უსაფრთხოების სამსახურად. აღნიშნული ორგანო პასუხისმგებელია ეროვნული უსაფრთხოების წინააღმდეგ კიბერსივრცეში განხორციელებული აქტივობების გამოვლენაზე, პრევენციასა და აღკვეთაზე. ამასთან, მოქმედი კანონმდებლობით სახელმწიფო უსაფრთხოების სამსახური წარმოადგენს ორგანოს, რომელსაც გაჩნია კიბერსივრცეში ფარული საგამოძიებო საქმიანობის განხორციელების ექსკლუზიური უფლებამოსილება.

2013 წელს ახალი კონსტიტუციური მოდელის ამოქმედებასთან დაკავშირებით, ეროვნულ უსაფრთხოებასთან დაკავშირებული უფლებამოსილებების დიდი ნაწილი გადავიდა საქართველოს მთავრობის დაქვემდებარებაში. საქართველოს მთავრობის კომპეტენციას მიეკუთვნა აგრეთვე კიბერუსაფრთხოების საკითხები. აღნიშნულ ფუნქციათა განხორციელების ხელშეწყობის მიზნით საქართველოს პრემიერ-მინისტრის დაქვემდებარებაში 2014 წელს შეიქმნა სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო, რომელიც უზრუნველყოფს კიბერუსაფრთხოების პოლიტიკის ძირითადი ჩარჩოს შემუშავებას და კიბერუსაფრთხოების სისტემის განვითარების თაობაზე შესაბამისი რეკომენდაციების წარდგენას საქართველოს მთავრობისთვის. ამასთან, საბჭო კოორდინაციას უწევს შესაბამის უწყებებს კიბერსაფრთხეების გამოვლენის პროცესში და, ასევე შეიმუშავებს სათანადო ზომებს ხსენებულ საფრთხეთა ნეიტრალიზაციისა და შემცირების მიზნით, ასევე აღნიშნულ საფრთხეთა რეალიზების შედეგების აღმოსაფხვრელად რეკომენდაციები წარედგინება საქართველოს მთავრობას. ამასთან, საბჭო მართავს

კიბერუსაფრთხოებასთან დაკავშირებული ეროვნული მასშტაბის ნებისმიერ კრიზისულ სიტუაციას.

ინსტიტუციური განვითარების პარალელურად, საქართველოს ხელისუფლება რეგულარულად ახორციელებს ტრეინინგებს, კურსებს და სხვა სახის შესაძლებლობათა ამაღლების პროექტებს, რომელიც მიზნად ისახავს კიბერუსაფრთხოების საკითხებზე მომუშავე პერსონალის პროფესიული უნარ-ჩვევების განვითარებას.

მიუხედავად მიღწეული პროგრესისა, საქართველოს კიბერუსაფრთხოების ორგანოების საქმიანობაში არსებობს რიგი ნაკლოვანებებისა, რომელთა ეფექტური აღმოფხვრა ვერ განხორციელდება მხოლოდ წინამდებარე სტრატეგიის სამოქმედო გეგმით გათვალისწინებული აქტივობების ფორმალური შესრულებით. საჭიროა, რომ ამავე სამოქმედო გეგმით გათვალისწინებული ორგანოები შიდაუწყებრივ დონეზე ავტონომიურ რეჟიმში ავითარებდნენ საკუთარ შესაძლებლობებს, რომელიც ბუნებრივია უნდა შეესაბამებოდეს საქართველოს კიბერუსაფრთხოების პოლიტიკის სტრატეგიულ მიმართულებებს.

2. საქართველოს წინაშე მდგარი კიბერსაფრთხეები

ელექტრონული მმართველობის პრინციპის დამკვიდრებასთან ერთად იზრდება საქართველოს კრიტიკული ინფორმაციული ინფრასტრუქტურის წინაშე არსებული საფრთხეები და გამოწვევები. ამასთან, ინფორმაციული სისტემის კრიტიკულობისა და კიბერუსაფრთხოებისადმი მდგრადობა განისაზღვრება ისეთი კრიტერიუმებით, როგორიცაა მოსალოდნელი ზიანის სიმძიმე და მასშტაბი, ინფორმაციული სისტემის აუცილებლობა სახელმწიფოსა და საზოგადოების ნორმალური ფუნქციონირებისათვის, სისტემის მომხმარებელთა რაოდენობა და კიბერუსაფრთხოების სათანადო დონის უზრუნველსაყოფად საჭირო რესურსები.

აღნიშნულ ეტაპზე საქართველოს კიბერუსაფრთხოების სისტემის წინაშე არსებულ მთავარ საფრთხეს წარმოადგენს რუსეთის ფედერაციის მიერ ორგანიზებული კიბერშეტევები და კიბერსაშუალებებით ჩადენილი სხვა დანაშაულები. რუსეთის ფედერაცია იყენებს კიბერსაშუალებებს ევროატლანტიკური სივრცის წინააღმდეგ წარმოებულ საინფორმაციო ომში და შესაბამისად, კიბერსივრცის მეშვეობით რუსეთის ფედერაცია აქტიურად ეწევა საინფორმაციო კამპანიას, რომელიც მიზნად ისახავს საქართველოს ევროატლანტიკურ ოჯახში ინტეგრაციის შეფერხებას და, ასევე საქართველოს მოსახლეობაში ევროატლანტიკური ღირებულებების დისკრედიტაციას.

დღეს არსებული მდგომარეობით საქართველოს კიბერუსაფრთხოების წინააღმდეგ რუსეთის ფედერაციიდან მომდინარე საფრთხე რეალურია და მისი დონე მომატებულია 2008 წელთან შედარებით შემდეგ გარემოებათა გამო:

- რუსეთის ფედერაციას არ შეუცვლია საკუთარი აგრესიული პოლიტიკა კიბერდომეინში;

- რუსეთის ფედერაციამ უკანასკნელ წლებში მნიშვნელოვნად აამაღლა საკუთარი კიბერშეტევითი შესაძლებლობები;
- რუსეთის ფედერაციამ მნიშვნელოვნად დახვეწა კიბერსაშუალებების გამოყენების სპეციფიკა მის მიერვე წარმოებულ ფსიქოლოგიური გავლენის ოპერაციებში;
- 2008 წელთან შედარებით მნიშვნელოვნად არის გაზრდილი საქართველოს დამოკიდებულება ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე, რაც პოტენციური კიბერთავდასხმების შემთხვევაში, თავის მხრივ, ზრდის მოსალოდნელი ზიანის მასშტაბებს.

აღნიშნულ ეტაპზე საქართველოს წინააღმდეგ მიმართული კიბერსაფრთხეებიდან განსაკუთრებული აღსანიშნავია შემდეგი:

კიბეროომი – 2008 წელს რუსეთის ფედერაციამ საქართველოს წინააღმდეგ აგრესია, სამხედრო თავდასხმის პარალელურად, კიბერსივრცეშიც განახორციელა, რომელიც საკუთარი მასშტაბებით, ზიანის ხარისხითა და აქტიურ საბრძოლო მოქმედებებთან მჭიდრო კოორდინაციით სავსებით აკმაყოფილებს კიბეროომის დეფინიციას. რუსეთის ფედერაციამ უკანასკნელ პერიოდში კიდევ უფრო განავითარა კიბერსივრცეში საკუთარი სამხედრო შესაძლებლობები, რაც დასტურდება უკრაინის წინააღმდეგ მიმდინარე სამხედრო მოქმედებების მხარდამჭერი კიბეროპერაციებითაც.

კიბერტერორიზმი – კრიტიკულ ინფორმაციულ ინფრასტრუქტურაზე, საქართველოს სახელმწიფო მართვის და ბიზნესის მნიშვნელოვანი სფეროების მზარდ დამოკიდებულებასთან ერთად იზრდება კიბერტერორიზმის საფრთხეები და, ასევე მოსალოდნელი ზიანის მასშტაბები. თანამედროვე პერიოდში ტერორისტულ დაჯგუფებებს გააჩნიათ მნიშვნელოვანი რესურსები და ინფორმაციული და საკომუნიკაციო ტექნოლოგიების ცოდნა, რომლებსაც აქტიურად იყენებენ საკუთარი საქმიანობის მხარდაჭერის მიზნით. აღნიშნულის ნათელი დადასტურებაა ტერორისტული ორგანიზაციის „ისლამური სახელმწიფო“, რომელიც რეგულარულად ახორციელებს კიბერშეტევებს ანტიტერორისტული კოალიციის წევრი სახელმწიფოების კრიტიკული ინფორმაციული სისტემების წინააღმდეგ. ამასთან, „ისლამური სახელმწიფო“ სხვადასხვა ქვეყნაში ტერორისტული აქტების დაგეგმვას ახორციელებს დისტანციურად, თანამედროვე ტექნოლოგიების გამოყენებით, ხოლო სოციალური ქსელებისა და სხვა საკომუნიკაციო პლატფორმის მეშვეობით კი ეწევა ორგანიზაციაში გაწევრიანების მიზნით ახალგაზრდების მასობრივ გადაბირებას.

უკანასკნელ პერიოდში სულ უფრო აქტუალური ხდება მიზანმიმართულ საფრთხეთა ჯგუფების (Advanced Persistent Threat Groups -APTs) კიბერსივრცეში საქმიანობა, რაც არსებით საფრთხეს უქმნის ეროვნული უსაფრთხოების ინტერესებს იმის გათვალისწინებით, რომ მოცემულ ჯგუფებს გააჩნიათ ძლიერი კიბერშეტევითი შესაძლებლობები და, ასევე შეუძლიათ საკუთარი აქტივობების კომპლექსურად შენიღბვა. APTs შესაძლოა იყვნენ როგორც დამოუკიდებლად მოქმედი არასახელმწიფო აქტორები, ასევე იმართებოდნენ უცხო ქვეყნების სპეციალური სამსახურების მიერ.

ტერორისტული ორგანიზაციებისა და სხვა არასახელმწიფო აქტორებიდან მომდინარე კიბერტერორისტული საფრთხესთან ერთად, მნიშვნელოვანია ცალკეულ სახელმწიფოთა მიერ ორგანიზებული მიზნობრივი კიბერშეტევები იმდენად რამდენადაც ეს უკანასკნელნი ფლობენ და მუდმივად ავითარებენ მნიშვნელოვან კიბერშეტევით შესაძლებლობებს. ამ კუთხით აღსანიშნავია რუსეთის ფედერაცია, რომელიც ფლობს შესაბამის საშუალებებს და, ასევე მზად არის მისთვის არასასურველი ქვეყნების მიმართ კიბერსივრცეში გამოიყენოს ტერორისტული მეთოდები აღნიშნულ სახელმწიფოთა მოსახლეობაზე ან ხელისუფლებაზე ზემოქმედების მიზნით. რუსეთის ფედერაციის კიბერტერორისტული საქმიანობის განსაკუთრებულად საშიში ხასიათი დასტურდება როგორც 2008 წლის აგვისტოს ომის მაგალითზე, ასევე 2007 წელს ესტონეთის კრიტიკული ინფორმაციული ინფრასტრუქტურის წინააღმდეგ განხორციელებული შეტევებით.

კიბერსადაზვერვო საქმიანობა – ტექნოლოგიური პროგრესის პირობებში ინფორმაციის დამუშავება ძირითადად ხორციელდება ინფორმაციული ტექნოლოგიების საშუალებებით, რომელთა უსაფრთხოების უზრუნველყოფაც საქართველოს მსგავსი მცირე რესურსების მქონე ქვეყნისათვის საკმაოდ რთულ ამოცანას წარმოადგენს იმის გათვალისწინებით, რომ კიბერსადაზვერვო საქმიანობას ეწევა ორგანიზებული ძალა, რომლის უკანაც ხშირ შემთხვევაში დგას უცხო ქვეყნის სპეციალური სამსახურები. ამ მიმართებაშიც საქართველოს ძირითადი საფრთხე ემუქრება რუსეთის სპეციალური სამსახურებისგან, რომლებიც რეგულარულად ახორციელებენ კიბერსადაზვერო საქმიანობას როგორც სახელმწიფო საიდუმლოების შემცველი, ასევე სხვა სახის დახურული ინფორმაციის მოპოვების მიზნით. 2011 წელს საქართველოს შესაბამისი სამსახურების მიერ გამოვლენილ იქნა საკმაოდ დიდი მასშტაბის კიბერსადაზვერვო ოპერაცია – GEORBOT, რომელიც მიზნად ისახავდა სამხედრო სფეროს და, ასევე საქართველოს ხელისუფლებასა და ნატო-ს შორის არსებული ურთიერთობების თაობაზე ინფორმაციის მოპოვებას. სადაზვერვო ოპერაციის მთავარ სამიზნე ობიექტებს წარმოადგენდნენ საქართველოს მაღალი თანამდებობის პირების სამსახურებრივი გამოყენების ელექტრონული რესურსები, სადაც დისტანციურად განხორციელდა ჯაშუშური პროგრამული უზრუნველყოფის საშუალებათა ინსტალაცია, რომლის მეშვეობითაც მუდმივად ხორციელდებოდა სხვადასხვა კატეგორიის ინფორმაციის გადინება. გატარებული ღონისძიებების შედეგად დადგინდა, რომ ხსენებულ ოპერაციას ახორციელებდნენ რუსეთის ფედერაციის ფედერალური უშიშროების სამსახურთან დაკავშირებული პირები.

კიბერსივრცის მეშვეობით საქართველოს წინააღმდეგ მიმართული სხვა საქმიანობა – საქართველოს უსაფრთხოების გამოწვევაა კიბერსივრცის გამოყენებით ჩადენილი დანაშაულთა ის სახეები, რომელიც მიმართულია საქართველოსთვის კრიტიკული სერვისების მომწოდებელი კერძო და საჯარო ინფრასტრუქტურის წინააღმდეგ. უკანასკნელ პერიოდში სულ უფრო საშიშ ხასიათს იღებს საფინანსო და საკომუნიკაციო სერვისების მომწოდებლების წინააღმდეგ განხორციელებული შეტევები იმის გათვალისწინებით, რომ ხსენებულ სერვისებზეა დამოკიდებული

ქვეყნისთვის კრიტიკული მნიშვნელობის ყველა სუბიექტი. შესაბამისად, ფინანსურ და საკომუნიკაციო სექტორის ფუნქციონირების მოშლა, ასევე ახდენს სხვა კრიტიკული მნიშვნელობის სუბიექტების ნორმალური ოპერირების პარალიზებას.

IV. საქართველოს კიბერუსაფრთხოების პოლიტიკის ძირითადი მიმართულებები

საქართველოს კიბერუსაფრთხოების პოლიტიკის ძირითადი მიმართულებები წარმოადგენს ქვეყნის წინაშე არსებული კიბერსაფრთხეებზე და გამოწვევებზე ეფექტიანი რეაგირების ღონისძიებათა კომპლექსს.

საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიის ძირითადი მიმართულებებია:

კვლევა და ანალიზი;

სამართლებრივი ბაზის შემუშავება და სრულყოფა;

კიბერუსაფრთხოების სფეროში შესაძლებლობათა ამაღლება;

საზოგადოებრივი ცნობიერების ამაღლება და საგანმანათლებლო ბაზის ჩამოყალიბება;

საერთაშორისო თანამშრომლობა.

1. კვლევა და ანალიზი

მნიშვნელოვანია, რომ კიბერუსაფრთხოების სფეროში საქართველოს მიერ განხორციელებული აქტივობები ემყარებოდეს კვლევასა და ანალიზს, რომელიც უზრუნველყოფს კიბერუსაფრთხოების პოლიტიკის ეფექტიანობას და, ასევე ითვალისწინებდეს კიბერუსაფრთხოების ისეთ პრიორიტეტულ საფრთხეებს, რომელიც ემუქრება ადამიანთა სიცოცხლესა და ჯანმრთელობას, სახელმწიფო ინტერესებს, ქვეყნის თავდაცვისუნარიანობას, ფინანსურ უსაფრთხოებას, კერძო საკუთრების უფლებას და ზოგადად საფრთხეს უქმნის კრიტიკული ინფორმაციული სისტემის ნორმალურ ფუნქციონირებას. შესაბამისად, მიზანშეწონილია, რომ კვლევა და ანალიზის მიმართულება არ შემოიფარგლებოდეს მხოლოდ თეორიული მიდგომებით და იგი ფოკუსირებული იყოს კიბერუსაფრთხოების პრაქტიკულ საკითხებზე იმის გათვალისწინებით, რომ სწორედ რეალობასთან დაახლოებული პრაქტიკული სავარაუდოები წარმოადგენს კრიტიკულ სიტუაციებზე რეაგირების საუკეთესო ფორმატს. სწორედ აღნიშნული გარემოებებიდან გამომდინარე, წინამდებარე სტრატეგიის ფარგლებში, განხორციელდება ინტერნეტზე წვდომის არარსებობის შემთხვევაში, სახელმწიფო და კრიტიკული სისტემების მუშაობის შესაძლებლობების შეფასება, რომელზე დაყრდნობითაც მომზადდება სათანადო ანგარიშები და რეკომენდაციები. მოცემული აქტივობა კრიზისულ რეალობასთან მაქსიმალურად დაახლოებულ სიტუაციურ სცენარში შეამოწმებს ამ სიტუაციებზე რეაგირების გეგმებსა და საქართველოს შესაბამისი სამსახურების საქმიანობას კრიტიკულ ვითარებაში, ასევე წარმოაჩენს აღნიშნული ორგანოების ოპერირების

ნაკლოვან მხარეებს, რომელთა აღმოფხვრისთვის გატარდება შესაბამისი ღონისძიებები.

გარდა ამისა, კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განხორციელებისათვის აუცილებელია კვლევა და ანალიზი შემდეგი მიმართულებებითაც:

სხვა ქვეყნების საუკეთესო პრაქტიკის შესწავლა და გამოცდილების გაზიარება;

კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტების იდენტიფიცირების კრიტერიუმებისა და სტანდარტების კვლევა;

კრიტიკული ინფორმაციული ინფრასტრუქტურის მდგრადობის ანალიზი;

კიბერუსაფრთხოების სფეროში რეგიონში არსებული პრობლემატიკის შესწავლა;

კიბერუსაფრთხოების განმსაზღვრელი სტანდარტების შემუშავება მათი შემდგომი დანერგვის მიზნით;

საქართველოს კიბერსივრცის წინაშე მდგარი საფრთხეების და რისკების გამოვლენაზე წინადადებების პერიოდულად მომზადება.

2. სამართლებრივი ბაზის შემუშავება და სრულყოფა

2010 წლიდან დღემდე საქართველომ შეიმუშავა კიბერუსაფრთხოების უზრუნველმყოფი ძირითადი სამართლებრივი ჩარჩო, რომელიც მიზნად ისახავს ამ სფეროში უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, განსაზღვრავს საჯარო და კერძო სექტორების უფლება-მოვალეობებს ინფორმაციული უსაფრთხოების დაცვის სფეროში, არეგულირებს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმებს. გარდა ჩარჩო საკანონმდებლო აქტებისა, ინფორმაციული და კიბერუსაფრთხოების დეტალური იმპლემენტაციის მიზნით შემუშავებულია კანონქვემდებარე ნორმატიული აქტები, რომლებიც კრიტიკული ინფორმაციული სისტემის სუბიექტებისთვის კიბერუსაფრთხოების უზრუნველყოფის პროცესში სახელმძღვანელო ნორმების შემცველია, ამასთანავე შემუშავებულია კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფის საქმიანობის სამართლებრივი საფუძვლები და, ზოგადად, განსაზღვრულია სხვა უფლებამოსილი უწყებების კომპეტენციისა და საქმიანობის სამართლებრივი არეალი.

მიუხედავად ზემოაღნიშნულისა, საქართველოს კიბერუსაფრთხოების უზრუნველმყოფი სამართლებრივი ჩარჩო საჭიროებს გაცილებით ფართო და სპეციალურ გადამუშავებასა და შეფასებას, იმისათვის რათა აღმოიფხვრას ყველა შესაძლო იურიდიული ხარვეზი და შეივსოს ამ სფეროში არსებული სამართლებრივი ვაკუუმი. შედეგად, მივიღებთ კიბერუსაფრთხოების დახვეწილ და თანამედროვე კიბერგამოწვევებთან ბრძოლის პროცესში ხელშემწყობ სამართლებრივ ბერკეტს.

ზემოაღნიშნული მიზეზების გამო, სათანადო რეგულირების მიღმაა დარჩენილი ინფორმაციული აქტივების კლასიფიცირების საკითხი, რომელიც ქვეყნის კიბერუსაფრთხოების ინტერესებს მნიშვნელოვან საფრთხეებს უქმნის.

ამასთან, სახელმწიფო უსაფრთხოების ინტერესებისთვის განსაკუთრებულ მნიშვნელობას ატარებს კერძო კრიტიკული ინფორმაციული სისტემების ბაზარზე ოპერირების მექანიზმების დახვეწა, ვინაიდან საქართველოს მოწინააღმდეგეების მიერ აღნიშნული სისტემების დაუფლება ქვეყნის საკომუნიკაციო სივრცეს აბსოლუტურად დაუცველს ტოვებს. ამრიგად, საჭიროა კიბერუსაფრთხოების სფეროში ისეთი რეგულაციების მიღება, რაც ხელს შეუწყობს კიბერუსაფრთხოების დაცვის ქმედითი და ეფექტიანი მექანიზმების შექმნას.

კიბერუსაფრთხოების სფეროში სამართლებრივი ბაზის სრულყოფისათვის აუცილებელია შემდეგი ღონისძიებების გატარება:

კრიტიკული ინფორმაციული ინფრასტრუქტურის განმსაზღვრელი და მისი კიბერუსაფრთხოების უზრუნველმყოფი ნორმატიული ბაზის შემდგომი დახვეწა, განვითარება;

კრიტიკული ინფორმაციული სისტემების კიბერუსაფრთხოების უზრუნველმყოფი სამართლებრივი ბაზის განახლება;

კრიტიკული ინფორმაციული სისტემების სუბიექტების საქმიანობისთვის საჭირო პროგრამული და ტექნიკური აღჭურვილობის მომწოდებლებთან თანამშრომლობის მექანიზმების დახვეწა;

ინფორმაციული უსაფრთხოების მარეგულირებელი კანონმდებლობით გათვალისწინებული ვალდებულებების აღსრულების მექანიზმების შემუშავება;

ევროპის საბჭოს 2001 წლის ,,კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირების შედეგად აღებული ვალდებულებების შესრულების გაგრძელება;

საგანგებო, საომარი და სხვა სახის კრიზისული სიტუაციების დროს კიბერინციდენტებთან დაკავშირებულ მოვლენათა სავარაუდო განვითარების სცენარების დამუშავება და შესაბამისი მოქმედების სარეზერვო გეგმების და პროცედურების გაწერა.

საქართველოს მთავრობის 2017 წლის 29 მარტის დადგენილება №159 - ვებგვერდი, 30.03.2017წ.

3. კიბერუსაფრთხოების სფეროში შესაძლებლობათა ამაღლება

კიბერუსაფრთხოების უზრუნველსაყოფად განსაკუთრებული მნიშვნელობა ენიჭება აღნიშნული პროცესში ჩართული უწყებების შესაძლებლობათა ამაღლებას როგორც ტექნიკურ, ასევე ადამიანურ დონეზე. ტექნიკურ დონეზე განსაკუთრებით მნიშვნელოვანია კიბერკვლევითი ლაბორატორიის ჩამოყალიბება, რომლის საქმიანობაც დაკავშირებული იქნება კიბერუსაფრთხოების კომპლექსურ საკითხებზე სხვადასხვა ინოვაციური გადაწყვეტილებების შემუშავებასთან. ამასთან, ლაბორატორია უზრუნველყოფს საქართველოს შესაბამისი სამსახურების

თანამედროვე ცოდნით აღჭურვას, რაც, ასევე სასიცოცხლოდ მნიშვნელოვანია ეროვნული უსაფრთხოების ინტერესებისთვის იმის გათვალისწინებით, რომ თანამედროვე ტექნოლოგიები პროგრესირებს სწრაფი ტემპებით და უსაფრთხოების ორგანოებს რეგულარულ რეჟიმში ესაჭიროებათ ტექნოლოგიურ პროგრესის შესატყვისი უნარ-ჩვევების განვითარება.

ადამიანურ დონეზე საქართველოს კიბერუსაფრთხოებას მნიშვნელოვნად გააძლიერებს კიბერრეზერვის პროგრამა, რომლის დანერგვაც იგეგმება მოცემული სტრატეგიის სამოქმედო პერიოდში. იმის გათვალისწინებით, რომ საქართველოს კვლავ დგას 2008 წლის აგვისტოში განხორციელებული კიბერომის მასშტაბის საფრთხის წინაშე, ხოლო სახელმწიფოს ორგანოების ხელთ არსებული რესურსები არასაკმარისია, მნიშვნელოვანია სხვადასხვა სექტორში არსებული ცოდნისა და გამოცდილების გაერთიანება საქართველოს წინააღმდეგ მიმართული საფრთხეების აღკვეთისა და შემცირების მიზნით. სწორედ აღნიშნული მიზნების მიღწევას ემსახურება კიბერრეზერვის სისტემის ჩამოყალიბება, რომელიც იძლევა საშუალებას კრიზისული სიტუაციების დროს მოახდინოს ქვეყანაში არსებული რესურსების სწორი მობილიზაცია და კოორდინირებული მართვა.

მნიშვნელოვანია, სახელმწიფოს გააჩნდეს კერძო სექტორთან თანამშრომლობის ეფექტური მექანიზმები კიბერსაფრთხეებსა და გამოწვევებზე დროული რეაგირების მიზნით, ვინაიდან სწორედ კერძო სექტორი ფლობს კრიტიკული ინფორმაციული ინფრასტრუქტურის დიდ ნაწილს და, ასევე ამ სფეროში არსებულ ცოდნასა და გამოცდილებას. კიბერუსაფრთხოების სფეროში კერძო სექტორთან თანამშრომლობა მოიცავს არა მხოლოდ ბიზნეს წრეებთან ურთიერთობებს. იგი, ასევე გულისხმობს შესაბამისი მიმართულების არასამთავრობო სექტორისა და აკადემიური წრეების ჩართულობას ამ პროცესში იმის გათვალისწინებით, რომ აღნიშნული ორგანიზაციები ატარებენ სიღრმისეულ კვლევებს კიბერუსაფრთხოების სფეროში და ამასთან შეიმუშავებენ მნიშვნელოვან ინოვაციურ მიდგომებს, რომელთა რეალიზების პროცესს ხშირ შემთხვევაში ესაჭიროება სახელმწიფოს მხრიდან ხელშეწყობა. ამრიგად, საქართველოს მთავრობა გამოთქვამს მზადყოფნას შესაძლებლობის ფარგლებში მაქსიმალურად უზრუნველყოს კერძო სექტორის მიერ წარმოდგენილი ინოვაციური ინიციატივების მხარდაჭერა.

ამასთან, საქართველოს ხელისუფლება მიზნად ისახავს კერძო სექტორთან თანამშრომლობის გზით განახორციელოს კიბერუსაფრთხოების სფეროში სტანდარტების დანერგვა და შესაბამისი მარეგულირებელი სამართლებრივი ჩარჩოს დახვეწა. აუცილებელია, რომ სახელმწიფოსთან თანამშრომლობის ფორმატი კერძო სექტორს საშუალებას აძლევდეს ხელისუფლებას გაუზიაროს საკუთარი ხედვები აღნიშნულ საკითხებზე და, ასევე შესთავაზოს ალტერნატიული წინადადებები.

დღეს არსებული სიტუაციით, საქართველოს აქვს კერძო სექტორთან თანამშრომლობის წარმატებული პრაქტიკა, რომელიც ძირითადად დაგროვდა საქართველოს კიბერუსაფრთხოების ფორუმის ფარგლებში, სადაც წარმოდგენილია საქართველოს სატელეკომუნიკაციო ბაზარზე მოქმედი თითქმის ყველა მთავარი

მოთამაშე კიბერუსაფრთხოების სფეროში ჩართულ სახელმწიფო ორგანოებთან ერთად. თანამშრომლობის ამ ფორმატმა როგორც სახელმწიფო, ისე კერძო სექტორს საშუალება მისცა გაეზიარებინათ საკუთარი ხედვები კიბერუსაფრთხოების მნიშვნელოვან საკითხებზე და, ასევე ხელი შეუწყო ერთობლივი ინიციატივების განხორციელებას. საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიის სამოქმედო პერიოდის განმავლობაში იგეგმება კიბერუსაფრთხოების ფორუმის ინსტიტუციონალიზაცია და, ასევე მისი ფუნქციებისა და შემადგენლობის გაფართოვება. აღნიშნული ხელს შეუწყობს კერძო სექტორის კიდევ უფრო აქტიურ და ნაყოფიერ მონაწილეობას კიბერუსაფრთხოების პოლიტიკის დაგეგმვისა და განხორციელების პროცესში.

გარდა ამისა, როგორც წარსული პრაქტიკა ადასტურებს, მნიშვნელოვანია სახელმწიფო და კერძო სექტორის კოორდინირებული ურთიერთქმედება კრიზისული სიტუაციების დროს, როდესაც სახელმწიფო ორგანოები მოკლებულნი არიან შესაძლებლობას ეფექტურად გაუმკლავდნენ საქართველოს კიბერუსაფრთხოების წინაშე არსებულ მყისიერ საფრთხეებს. შესაბამისად, მიზანშეწონილია, რომ თანამშრომლობის ფარგლებში განისაზღვროს კრიზისული სიტუაციების რეაგირების სახელმწიფო და კერძო სექტორის კოორდინირებული მუშაობის მექანიზმები, რომლის ეფექტურობის ამაღლება უნდა მოხდეს შესაბამის რეალურ ვითარებაზე მორგებული სიტუაციური სცენარების გამოყენებით.

ამასთან, კიბერუსაფრთხოების სფეროში შესაძლებლობათა ამაღლებისათვის აუცილებელია შემდეგი ღონისძიებების გატარება:

კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფის შესაძლებლობების შემდგომი განვითარება;

კომპიუტერული მონაცემების საექსპერტო კვლევის შესაძლებლობების შემდგომი განვითარება;

სახელმწიფო საიდუმლოების შემცველი ინფორმაციის მიმოცვლის დაშიფრული სისტემის შექმნა და განვითარება;

კიბერუსაფრთხოების ინციდენტებიდან გამოწვეული სიტუაციური სცენარებზე მორგებული ტრენინგებისა და კიბერსავარჯიშოების ჩატარება.

4. საზოგადოებრივი ცნობიერების ამაღლება და საგანმანათლებლო ბაზის ჩამოყალიბება

საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიის მნიშვნელოვან ნაწილს ამ სფეროში საზოგადოებრივი ცნობიერების და შესაბამისი სპეციალისტების პროფესიული დონის ამაღლება წარმოადგენს. არსებული მდგომარეობით, მიუხედავად ამ მიზნით სახელმწიფო ორგანოების მიერ განხორციელებული და მიმდინარე მრავალი ინიციატივისა, საქართველოში კიბერუსაფრთხოების საკითხებზე საზოგადოებრივი ცნობიერება კვლავ საკმაოდ დაბალია. ცნობიერების ამაღლება, ასევე გამოწვევად რჩება სახელმწიფო

სექტორისთვისაც, სადაც დასაქმებული მოხლეების საკმაოდ დიდი ნაწილი არ ფლობს კიბერუსაფრთხოების ბაზისური ნორმების ცოდნას. საწყის ეტაპზე მიზანშეწონილი იქნება იმ სახელმწიფო მოხელეთა მომზადება-გადამზადება, რომელთაც აქვთ დაშვება სახელმწიფო საიდუმლოებასთან და საკუთარი საქმიანობით უკავშირდებიან ქვეყნისთვის კრიტიკული მნიშვნელობის მქონე სფეროებს.

ამასთან ერთად, კიბერუსაფრთხოების საკითხებზე სპეციალიზებული ადამიანური რესურსების მომზადების უწყვეტობა დიდ მნიშვნელობას ატარებს სახელმწიფოსთვის იმის გათვალისწინებით, რომ შრომის ბაზარზე არსებული მოთხოვნის გამო ამ კატეგორიის საკადრო რესურსი რეგულარულად გაედინება არა მხოლოდ საჯარო სექტორიდან კერძო სექტორში, არამედ ქვეყნიდან – მაღალი ფინანსური ანაზღაურების სანაცვლოდ. შესაბამისად, ქვეყანას უნდა გააჩნდეს ინსტიტუციონალიზებული საგანმანთლებლო ბაზა და აკადემიური პროგრამები, რომელიც უზრუნველყოფს საკადრო რესურსის მომზადების უწყვეტობას, ხოლო აღნიშნული კი წარმოადგენს კიბერუსაფრთხოების ორგანოების სტაბილური ფუნქციონირების მნიშვნელოვან გარანტიას.

საზოგადოებრივი ცნობიერების ამაღლებისა და საგანმანათლებლო ბაზის ჩამოყალიბების მიზნით საჭიროა შემდეგი ღონისძიებების გატარება:

კიბერუსაფრთხოების სფეროში საზოგადოებრივი ცნობიერების ამაღლებისა და საგანმანათლებლო პროგრამების შექმნა;

კიბერდა ინფორმაციული უსაფრთხოების მიმართულებით უმაღლესი განათლების სისტემის შესაძლებლობების განვითარება;

კრიტიკული ინფორმაციული ინფრასტრუქტურის სუბიექტების და სხვა დაინტერესებული ორგანიზაციების კადრებისა და ტექნიკური პერსონალის გადამზადება ინფორმაციული უსაფრთხოების საერთაშორისო და ეროვნული სტანდარტების შესწავლისათვის;

საქართველოს ეროვნული უსაფრთხოების წინააღმდეგ მიმართული კიბერინციდენტების გამოძიების სპეციალიზებული ტრენინგები;

კიბერუსაფრთხოების სფეროში სამეცნიერო-კვლევითი პროექტების ხელშეწყობა;

5. საერთაშორისო თანამშრომლობა

კიბერუსაფრთხოების უზრუნველყოფა შეუძლებელია მხოლოდ საკუთარი ძალებით, ვინაიდან კიბერინციდენტები ატარებს ტრანსნაციონალურ ხასიათს და, შესაბამისად, აღნიშნულ საფრთხეების აღკვეთა-შემცირების პროცესში საერთაშორისო თანამშრომლობა გარდაუვალ აუცილებლობას წარმოადგენს. აღნიშნულ გარემოებას, ასევე ადასტურებს არაერთი საერთაშორისო ორგანიზაციის ეგიდით მიღებული რეზოლუცია თუ სხვა სახის სამართლებრივი აქტები, რომელთა შემუშავების

ძირითად მოტივაციას წარმოადგენდა სწორედ საერთაშორისო თანამშრომლობის ხელშეწყობა.

ამასთან, კიბერინციდენტებზე ეფექტური რეაგირების მიზნით, არსებული მონაცემები, რომლებიც აღნიშნული ინციდენტების ტრანსნაციონალური ხასიათიდან გამომდინარე შესაძლოა ინახებოდეს სხვადასხვა ქვეყნის ტერიტორიაზე განლაგებულ ინფრასტრუქტურაში, წარმოადგენს მოწყვლად ინფორმაციას და მისი უსაფრთხო და დროული მოპოვება წარმოადგენს მოცემულ ინციდენტებზე ეფექტური რეაგირების აუცილებელ პირობას. აღნიშნული კი მიიღწევა მხოლოდ ეფექტიანი საერთაშორისო თანამშრომლობის არხებით და ფორმატებით.

ასევე გასათვალისწინებელია ის გარემოება, რომ საქართველოს, მიუხედავად უკანასკნელ წლებში კიბერუსაფრთხოების სფეროში მიღწეული შესამჩნევი პროგრესისა, არ გააჩნია კომპლექსური ცოდნა და ინსტიტუციური შესაძლებლობა, რათა ავტონომიურ რეჟიმში მოახდინოს საკუთარი კიბერშესაძლებლობების განვითარება. უნდა აღინიშნოს აგრეთვე ისიც, რომ უკანასკნელ პერიოდში კიბერუსაფრთხოების სფეროში პროგრესი სწორედ საერთაშორისო თანამშრომლობის შედეგად იქნა მიღწეული.

საქართველოს ევროატლანტიკური ინტეგრაციის პროცესში განსაკუთრებული მნიშნელობა ენიჭება NATO-სა და ევროკავშირთან კიბერუსაფრთხოების საკითხებზე თანამშრომლობას, იმის გათვალისწინებით, რომ აღნიშნული სფერო უკანასკნელ პერიოდში გახდა მოცემული ორგანიზაციების უსაფრთხოების არქიტექტურის განუყოფელი ნაწილი.

საქართველო ხელისუფლება უმნიშვნელოვანესად მიიჩნევს NATO-ს 2016 წლის ვარშავის სამიტზე მიღებულ გადაწყვეტილებას, რომლის ფარგლებშიც კიბერსივრცე განისაზღვრა ორგანიზაციის სამოქმედო დომეინად. NATO-ს წევრ სახელმწიფოებს შორის 2014 წელს მიღწეული შეთანხმების გათვალისწინებით, რომლის თანახმადაც კიბერთავდაცვა იქცა კოლექტიური თავდაცვის განუყოფელ ნაწილად, მოცემული გადაწყვეტილება ემსახურება შეკავებისა და თავდაცვის ამოცანების უზრუნველყოფას და, ასევე მიზნად ისახავს სხვადასხვა მიმართულებით ალიანსის ოპერაციების მხარდაჭერას.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, ორგანიზაციის 2016 წლის ვარშავის სამიტზე დამტკიცდა კიბერთავდაცვის განაცხადი (Cyber Defense Pledge), რომლის მიზანია წევრი სახელმწიფოების ეროვნული ინფორმაციული ინფრასტრუქტურის დაცვის გაძლიერება. აღნიშნული, თავის მხრივ, წარმოადგენს ალიანსის უსაფრთხოების მთელი სისტემის მდგრადობის მნიშვნელოვან წინაპირობას.

საქართველოს მთავრობა გააგრძელებს NATO-საქართველოს არსებით ღონისძიებათა პაკეტის იმპლემენტაციას, ასევე გამოთქვას მზადყოფნას კიდევ უფრო გააღრმავოს თანამშრომლობა ალიანსთან და ხელი შეუწყოს ეროვნული კიბერთავდაცვის სისტემის თავსებადობის ამაღლებას NATO-ს მოთხოვნებთან.

მზარდი კიბერსაფრთხეების პრევენციისა და შემცირების მიზნით, მნიშვნელოვანი აქტივობები განხორციელდა, ასევე ევროკავშირის მხრიდან, რომლის გლობალური უსაფრთხოების სტრატეგიის განუყოფელ ნაწილად იქცა კიბერუსაფრთხოება. ამ კუთხით განსაკუთრებით აღსანიშნავია 2013 წელს მიღებული კიბერუსაფრთხოების სტრატეგია და 2016 წლის დირექტივა „ქსელებისა და ინფორმაციული სისტემების უსაფრთხოების შესახებ“ იმის გათვალისიწინებით რომ მოცემული დოკუმენტები თვისობრივად ახლებურად აყალიბებენ ევროპის კავშირის მთლიან ინფორმაციული უსაფრთხოების სისტემას. საქართველოს მთავრობა გააძლიერებს ევროკავშირთან კიბერუსაფრთხოების საკითხებზე თანამშრომლობას და ამასთან, ქვეყნის კიბერუსაფრთხოების სფეროს განვითარების პროცესში მხედველობაში მიიღებს ზემოაღნიშნული დოკუმენტებით გათვალისწინებულ პრიორიტეტებსა და სამოქმედო გეგმებს.

კიბერუსაფრთხოების უზრუნველყოფის მიზნით საერთაშორისო თანამშრომლობის განვითარებისათვის საქართველო, ასევე ატარებს შემდეგ ღონისძიებებს:

კიბერუსაფრთხოების საკითხებზე საერთაშორისო ურთიერთობების განმტკიცება ამ სფეროში მომუშავე საერთაშორისო ორგანიზაციებთან (OECD, OSCE, CoE, UN, ITU და სხვა) და სახელმწიფო ორგანოებთან;

კიბერუსაფრთხოების სფეროში საერთაშორისო ინიციატივებში აქტიური მონაწილეობის მიღება და ამ ინიციატივების რეგიონის მასშტაბით მხარდაჭერა;

სხვა ქვეყნების CERT-ებთან კიბერუსაფრთხოების სფეროში ორმხრივ და მრავალმხრივ ფორმატებში თანამშრომლობის ინიციირება;

კიბერუსაფრთხოების კვლევებისა და სწავლების რეგიონული ცენტრის შექმნა და განვითარება.

V. საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიის განხორციელების მექანიზმები და ვადები

წინამდებარე სტრატეგიის იმპლემენტაციის მთავარ მექანიზმს წარმოადგენს თანდართული სამოქმედო გეგმა, რომელიც „ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ“ საქართველოს კანონის მე-15 მუხლის მე-4 პუნქტის შესაბამისად, კონკრეტული ამოცანების შესასრულებლად განსაზღვრავს დროს, საშუალებებსა და პასუხისმგებელ უწყებებს.

სტრატეგიის განხორციელების ვადებია 2017-2018 წლები. აღნიშნული სტრატეგიის შესრულებაზე პასუხისმგებელი უწყებები შესაბამის სფეროში შიდაუწყებრივი პოლიტიკის განხორციელებისას ითვალისწინებენ ამ სტრატეგიის მოთხოვნების შესრულებისათვის საჭირო ღონისძიებებს.

წინამდებარე სტრატეგიის შესრულებისათვის საჭირო რესურსები უზრუნველყოფილი იქნება სამოქმედო გეგმით განსაზღვრული ცალკეული

აქტივობის შესრულებაზე პასუხისმგებელი უწყებებისთვის გამოყოფილი ასიგნებების ფარგლებში. ამასთან, შესაძლებელია საერთაშორისო დონორებისგან დამატებითი ფინანსური სახსრების მოძიება სამოქმედო გეგმით გათვალისწინებული საჭიროების შემთხვევაში.

მოცემული სტრატეგიის სამოქმედო გეგმის განხორციელებაზე პასუხისმგებლები არიან კონკრეტული აქტივობის შესრულებაზე თავად სამოქმედო გეგმით ასეთად განსაზღვრული უწყებები. სამოქმედო გეგმით გათვალისწინებული კონკრეტული აქტივობის შესრულებაზე რამდენიმე პასუხისმგებელი უწყების განსაზღვრის შემთხვევაში, მთავარ პასუხისმგებელ უწყებას წარმოადგენს შესაბამის ჩამონათვალში პირველ ადგილზე მითითებული უწყება. დამხმარე უწყებები საკუთარი კომპეტენციის ფარგლებში ახორციელებენ პასუხისმგებელი სახელმწიფო ორგანოების საქმიანობის ხელშეწყობას კომპეტენციის იმ ფარგლებში, რასაც მოქმედი კანონმდებლობა აღნიშნულ უწყებებს სამოქმედო გეგმით გათვალისწინებულ საკითხებთან მიმართებაში ანიჭებს.

„ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის შესახებ“ საქართველოს კანონის თანახმად, საქართველოს კიბერუსაფრთხოების 2017-2018 წლების სტრატეგიის სამოქმედო გეგმით განსაზღვრულ პასუხისმგებელ უწყებებს ევალებათ შეიმუშავონ შიდაუწყებრივი სამოქმედო გეგმები, რომლებიც განსაზღრავს ამავე სამოქმედო გეგმით მათზე დაკისრებული ვალდებულებების შესრულების მექანიზმებსა და ეტაპებს.

საქართველოს კიბერუსაფრთხოების 2017-2018 წლების სტრატეგიის შესრულების შედეგები ყოველწლიურად შეფასდება და შეფასების ყოველწლიური ანგარიში წარედგინება სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭოს აპარატს, რომელიც სტრატეგიის შესრულების მდგომარეობას აცნობს სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭოსთან არსებულ საქართველოს ეროვნული უსაფრთხოების კონცეპტუალური დოკუმენტების შემუშავების მაკოორდინირებელ მუდმივმოქმედ უწყებათაშორის კომისიასა და საქართველოს მთავრობას. ამასთან, სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭოს აპარატი უფლებამოსილია, დადგენილ ვადაზე ადრე, შესაბამისი სახელმწიფო უწყებ(ებ)იდან მოცემული სტრატეგიის სამოქმედო გეგმით განსაზღვრულ ცალკეულ აქტივობებზე გამოითხოვოს ინფორმაცია, რომელიც წარედგინება კომისიას.