კიბერუსაფრთხოების განვითარების სამოქმედო გეგმა

სსიპ კიბერუსაფრთხოების ბიურო

2016 - 2017

Cyber Security Development Action Plan

2016 - 2017

Ministry of Defence of Georgia

Cyber Security Bureau

სარჩევი

თავდაცვის სფეროში კიბერუსაფრთხოების განვითარების სამოქმედო გეგმა

თავი I

შესავალი

მუხლი 1.

,,თავდაცვის სფეროში კიბერუსაფრთხოების განვითარების სამოქმედო გეგმა'' (შემდეგში - სამოქმედო გეგმა) წარმოადგენს საქართველოს თავდაცვის სამინისტროს (შემდეგში - სამინისტრო) სისტემაში მოქმედ სსიპ - კიბერუსაფრთხოების ბიუროს (შემდგომში - ბიურო) ძირითად სახელმძღვანელო დოკუმენტს 2016-2017 წლებისათვის კიბერთავდაცვითი შესაძლებლობების შექმნისა და განვითარების შესახებ, რომელშიც აღწერილია პოლიტიკაში გათვალისწინებული კონკრეტული ამოცანების გადასაჭრელად და დასახული მიზნების მისაღწევად საჭირო ქმედებები, რესურსები, მეთოდები და ვადები. სამოქმედო გეგმა ეფუძნება ისეთ სტრატეგიულ და კონცეპტუალურ დოკუმენტებს, როგორიცაა: „საქართველოს ეროვნული უსაფრთხოების კონცეფცია“, „საქართველოს საფრთხეების შეფასების 2010-2013 წწ. დოკუმენტი“, „თავდაცვის სტრატეგიული მიმოხილვა 2013-2016 წწ.“, „საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013-2015 წწ. სამოქმედო გეგმა“, „მინისტრის ხედვა 2013-2014“, „საქართველოს ეროვნული სამხედრო სტრატეგია“ და „მინისტრის ხედვა 2015-2016“. დოკუმენტი პერიოდულ შეფასება/განახლებას ექვემდებარება.

მუხლი 2.

კიბერუსაფრთხოების მნიშვნელობა და აუცილებლობა ქვეყნის და გლობალურ უსაფრთხოებაში ყველა სახელმწიფოს მიერ იქნა აღიარებული. თითოეული ქვეყანა, რომელსაც ტექნოლოგიურად განვითარების სურვილი აქვს, ვალდებულია, დაიცვას საკუთარი კიბერსივრცე, უზრუნველყოს მისი უსაფრთხოება და დინამიკური განვითარება. ამავდროულად, ბიურო უზრუნველყოფს კიბერუსაფრთხოების პოლიტიკით განსაზღვრული ღონისძიებების განხორციელებას, რომელიც მიმართულია ინდივიდუალური და კოლექტიური უსაფრთხოების გასაძლიერებლად, იღებს პასუხისმგებლობას დაიცვას მოქალაქეების პირადი

ცხოვრების უფლებები და პირადი ინფორმაციის კონფედენციალურობა, სხვა ფუნდამენტალურ ღირებულებებთან ერთად.

მუხლი 3.

1. დღეისათვის მსოფლიო აქტიურად იყენებს კიბერსივრცეს პოლიტიკური, გეოპოლიტიკური, სამხედრო და სხვა მიზნების განსახორციელებლად. აღსანიშნავია, რომ რაც უფრო ვითარდება ტექნოლოგიები, მით უფრო რთული ხდება კიბერსივრცეში არსებული საფრთხეების პრევენცია და დაძლევა. თანამედროვე კიბერშეტევები საფრთხეს უქმნიან ქვეყნის უსაფრთხოებას, განვითარებას და ხელს უშლიან საზოგადოების ნორმალურ ფუნქციონირებას. საერთაშორისო სტატისტიკის მიხედვით წარმატებული კიბერინციდენტების რიცხვი ყოველწლიურად მატულობს და შესაბამისად იზრდება კიბერინციდენტებით გამოწვეული ზარალი. შესაბამისად, გლობალური უსაფრთხოების უზრუნველყოფის ერთ-ერთი მთავარი კომპონენტი სწორედ საკუთარი ქვეყნის კიბერთავდაცვაა. რუსეთის მხრიდან საქართველოზე უკანასკნელ წლებში განხორციელებულმა კიბერშეტევებმა ცხადყო, რომ კიბერსივრცის დაცვა ისეთივე მნიშვნელოვანია, როგორც სახმელეთო, საჰაერო და საზღვაო სივრცეებისა.

2. 2014 წლის სექტემბრის ნატოს უელსის სამიტზე კიბერუსაფრთხოება ერთ-ერთ მთავარ პრიორიტეტად განისაზღვრა და აღინიშნა, რომ კიბერსივრცის დაცვა ნატოს ერთიანი თავდაცვის განუყოფელი ნაწილია. საქართველო უერთდება ნატოს წევრი და პარტნიორი ქვეყნების კიბერუსაფრთხოების მნიშვნელობასთან დაკავშირებულ მიდგომებს და აღიარებს, რომ კიბერსაფრთხეები გლობალური გამოწვევაა, რომელიც სცდება ეროვნულ საზღვრებს და თანამშრომლობის საერთაშორისო დონეზე გაძლიერებას საჭიროებს.

3. 2013 წელს საქართველოში ნატოს სამეკავშირეო ოფისის მხარდაჭერით სამინისტროს სამუშაო ჯგუფმა ესტონელი ექსპერტის მონაწილეობით შეისწავლა უწყებაში არსებული სიტუაცია კიბერუსაფრთხოების მიმართულებით. აღნიშნული ღონისძიების შედეგად გამოიკვეთა ძირითადი გამოწვევები და პრობლემები: საქართველოს თავდაცვის სფეროს არ გააჩნდა კიბერსივრცეში არსებული/წარმოქმნილი რისკების მართვის და საფრთხეების მონიტორინგის, ანალიზის, პრევენციის სათანადო საშუალებები და შესაძლებლობები. კვლევის შედეგად შეიქმნა დოკუმენტი „განვითარების გეგმა“ (“Roadmap”), რომელიც გარკვეულწილად, წინამდებარე დოკუმენტის საფუძველი გახდა.

მუხლი 4.

1. საქართველო კონკრეტულ ნაბიჯებს დგამს, რათა საკუთარი ინფორმაციული სისტემები შესაბამისობაში მოიყვანოს ISO 27000 სერიის საერთაშორისო სტანდარტებთან. ამით საქართველო კიდევ უფრო დაუახლოვდება ევროკავშირსა და ნატოს, რომელთა ერთ-ერთი მოთხოვნა ინფორმაციული უსაფრთხოების განმტკიცება და სტანდარტიზაციაა.

2. საქართველოს თავდაცვის სფეროში კიბერუსაფრთხოების პოლიტიკას ახორციელებს ბიურო, რომელსაც „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით განსაზღვრული აქვს ის ვალდებულებები და ამოცანები, რომელთა შესრულებაც უზრუნველყოფს თავდაცვის სფეროს ინფორმაციული და კომუნიკაციების ტექნოლოგიების ერთიანი, ძლიერი და ეფექტური ინფრასტრუქტურის შექმნა/განვითარებას.

მუხლი 5.

სამოქმედო გეგმა შემუშავებულია ,,კიბერუსაფრთხოების პოლიტიკის დამტკიცების შესახებ'' საქართველოს თავდაცვის მინისტრის 2014 წლის 4 ნოემბრის N MOD 7 14 00001575 ბრძანების საფუძველზე, რომელიც პასუხობს მსოფლიო გამოწვევებს კიბერუსაფრთხოების სფეროში და ნატო-საქართველოს თანამშრომლობის ფარგლებში ერთ-ერთი პრიორიტეტული საკითხია.

თავი II

ტერმინთა განმარტება

მუხლი 6.

სამოქმედო გეგმაში გამოყენებულ ტერმინებს აქვთ შემდეგი მნიშვნელობა:

ა) **კიბერუსაფრთხოება** - ინფორმაციული და კომუნიკაციების სისტემების მდგომარეობა, რომელიც კიბერსივრცეში არსებული/წარმოქმნილი საფრთხეებისგან მონაცემთა კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დაცვის შესაძლებლობას იძლევა;

ბ) **ინფორმაციული უსაფრთხოება** - საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების კონფიდენციალურობის, ერთიანობის, წვდომის, ავთენტიფიკაციის და განგრძობადი მუშაობის დაცვას;

გ) კიბერსივრცე - სივრცე, რომლის განმასხვავებელი ნიშანია ელექტრონული მოწყობილობებისა და ელექტრომაგნიტური სპექტრის გამოყენება ქსელით დაკავშირებული სისტემებისა და დამხმარე ფიზიკური ინფრასტრუქტურის მეშვეობით მონაცემთა შენახვის, შეცვლის ან გაცვლისთვის; პროგრამული უზრუნველყოფის, ტექნიკური საშუალებების და მათი ურთიერთკავშირის საშუალებით შექმნილი ვირტუალური სივრცე;

დ) კიბერინციდენტი - კიბერუსაფრთხოების ინციდენტი, რომლის დროსაც ინფორმაციული სისტემების კონფიდენციალურობის, ხელმისაწვდომობის და მთლიანობის ხელყოფა ხდება;

ე) ინფორმაციული სისტემა - ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადაწყვეტილების მიღებას;

ვ) კრიტიკული ინფორმაციული სისტემა - ინფორმაციული სისტემა, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის;

ზ) კრიტიკული ინფორმაციული სისტემის სუბიექტი - სახელმწიფო ორგანო ან იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის;

თ) ინფორმაციული და კომუნიკაციების ტექნოლოგიების უსაფრთხოება-იმ ელექტრონული და ინფორმაციული ქსელებისა და სისტემების დაცულობა, რომლებიც ერთმანეთთან კომუნიკაციასა და მონაცემთა დამუშავებას ან გენერირებას ახდენენ;

ი) ინფრასტრუქტურა - ძირითადი სტრუქტურები და სისტემები (ადმინისტრაციულ და ორგანიზაციულ ქმედებებთან დაკავშირებული ტექნიკური აღჭურვილობისა და მოწყობილობების ერთობლიობა), რომლებიც საჭიროა ორგანიზაციების ფუნქციონირებისთვის;

კ) კიბერთავდაცვა - საკუთარი კიბერსივრცის დაცვის მიზნით განხორციელებული ღონისძიებების და საშუალებების ერთობლიობა, რომელიც სამხედრო-სტრატეგიულ მიზანს ემსახურება;

ლ) კიბერსაფრთხე - კიბერსივრცეში არსებული/წარმოქმნილი საფრთხე, რომელმაც შეიძლება გამოიწვიოს ინფორმაციული და კომუნიკაციების სისტემების კონფიდენციალურობის, ხელმისაწვდომობის და მთლიანობის დარღვევა;

მ) **კიბერკრიზისი** - ვითარება, რომლის დროსაც სახელმწიფოს ნორმალური ფუნქციონირებისთვის აუცილებელი ინფორმაციული სისტემების, სერვისების ან საკომუნიკაციო ქსელების უსაფრთხოება კრიტიკული საფრთხის წინაშეა.

თავი III

სტრატეგიული მიზნები და ამოცანები

მუხლი 7.

ბიუროს მიზანია, სამინისტროს სამოქალაქო ოფისის, საქართველოს შეიარაღებული ძალების გენერალური შტაბის (შემდეგში - გენერალური შტაბი) სტრუქტურული ქვედანაყოფებისა და სამინისტროს სისტემაში მოქმედი საჯარო სამართლის იურიდიული პირებისათვის ინფორმაციული და კომუნიკაციების ტექნოლოგიების სტაბილური, ეფექტური და უსაფრთხო სისტემების დანერგვა და განვითარება.

მუხლი 8.

კიბერუსაფრთხოების უზრუნველყოფის ერთ-ერთი მნიშვნელოვანი ნაწილია სამინისტროს ინფორმაციული და კომუნიკაციების ტექნოლოგიების სისტემების დაგეგმვის, შექმნის, ექსპლუატაციის, მოდერნიზაციის და გაფართოების ეტაპებზე მიღებული საერთაშორისო სტანდარტების და ნორმების დაცვა. ახალი სისტემების და სერვისების დანერგვისას მათი წინასწარი ტესტირება და უსაფრთხოების მოთხოვნების გათვალისწინება. ამ მიმართულებით ბიუროს ამოცანაა, გაუწიოს კონსულტაცია სამინისტროს კრიტიკული ინფორმაციული სისტემების სუბიექტებს, აღმოუჩინოს მხარდაჭერა ახალი სისტემების და სერვისების დანერგვაში. აქტიური მონაწილეობა მიიღოს ინფორმაციული ტექნოლოგიების სფეროში დაგეგმილი პროექტების განხილვასა და განხორციელებაში კომპეტენციის ფარგლებში.

მუხლი 9.

თავდაცვის სფეროში ინფორმაციული და კომუნიკაციების ტექნოლოგიების უსაფრთხო სისტემების დანერგვა და განვითარება ემყარება კიბერსივრცეში საფრთხეებისა და რისკების

სწრაფ იდენტიფიცირებას, მათზე რეაგირებას, პრევენციული ზომების გატარებასა და საჭიროების შემთხვევაში, კრიზისების მართვას პროგნოზირებადი, პრევენციული, დაცვითი, აღდგენითი მექანიზმების საშუალებით. აღნიშნული ღონისძიებები ხორციელდება სტანდარტიზებულად კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის მიერ, რომლის სამუშაო ციკლი შექმნილია მსოფლიოში არსებული საუკეთესო პრაქტიკის გათვალისწინებით და მოიცავს ყველა იმ აუცილებელ ქმედებას, რომელიც ხელს შეუწყობს ინციდენტების დროულ იდენტიფიცირებასა და აღმოფხვრას. შესაბამისად, ბიუროს ერთ-ერთ პრიორიტეტულ მიმართულებას წარმოადგენს კომპიუტერულ ინციდენტებზე დახმარების 24/7 მექანიზმების დახვეწა და განვითარება.

მუხლი 10.

წინამდებარე დოკუმენტში ორწლიანი გეგმით დასახული მიზნების შესასრულებლად და კონკრეტული ამოცანების წარმატებულად გადასაჭრელად ბიურო აქტიურად ითანამშრომლებს სამინისტროსთან და მის სისტემაში მოქმედ საჯარო სამართლის იურიდიულ პირებთან და უზრუნველყოფს **2016-2017** წლების ბიუჯეტის სწორ ფოკუსირებას ბიუროს სტრატეგიულ მიმართულებებზე (ადამიანური რესურსების პროფესიული განვითარება, ცნობიერების ამაღლება, ლიცენზირებული პროგრამები და ა.შ.) ბიუჯეტის ეფექტურად აღსრულებასა და მონიტორინგს; საჭიროების შემთხვევაში, დამატებითი ფინანსური რესურსების მოზიდვას; ლოგისტიკური უზრუნველყოფისათვის შესაბამისი მოთხოვნების სწორად განსაზღვრასა და საჭირო მექანიზმების განვითარებას; ლოგისტიკის საქმიანობის დაახლოვებას სამხედრო ლოგისტიკურ სტანდარტებთან; შესყიდვების სისტემის გაუმჯობესებას.

მუხლი 11.

1. წინამდებარე დოკუმენტით გათვალისწინებული თითოეული ამოცანის შესასრულებლად უაღრესად მნიშვნელოვანია შემდგომი საკითხების უზრუნველყოფა:

ა) საკმარისი ფინანსური რესურსების მოძიება;

ბ) ახალი საფრთხეების და რისკების იდენტიფიცირება;

გ) კვალიფიციური კადრების მოზიდვა/შენარჩუნება, კვალიფიკაციის ამაღლების მიზნით პროფესიული განვითარების პროგრამებით უზრუნველყოფა;

დ) საზოგადოების ცნობიერების ამაღლება კიბერუსაფრთხოების სფეროში;

ე) საქართველოს კანონმდებლობის ჰარმონიზაცია საერთაშორისო ნორმებთან კიბერუსაფრთხოების კუთხით;

ვ) სამთავრობო სტრუქტურებთან მჭიდრო თანამშრომლობა;

ზ) კრიტიკული სერვისების იდენტიფიკაცია, ნუსხის შემუშავება და მათი საერთაშორისო სტანდარტებთან ჰარმონიზაცია.

2. აღნიშნული ამოცანების შესრულება უზრუნველყოფს საერთაშორისო სტანდარტებთან თავსებადობას, კიბერელემენტების სამხედრო ოპერაციებში ინტეგრაციას და მტკიცე და მყარი კიბერუსაფრთხოების სისტემის შექმნას. აღნიშნული განაპირობებს თავდაცვის სფეროს საიმედო, ეფექტურ, სტაბილურ და უსაფრთხო ფუნქციონირებას, რაც თავისთავად ქმნის ეროვნული უსაფრთხოების მყარ საფუძვლებს.

თავი IV

სტრატეგიული მიზნების განსახორციელებელი ამოცანები

მუხლი 12.

სტრატეგია და გარემო

ა) **ამოცანა 1** - „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ საქართველოს თავდაცვის მინისტრის 2014 წლის 7 აპრილის N26 ბრძანების შესაბამისად, კონცეპტუალური დოკუმენტების ბაზის ჩამოყალიბება, რომელიც პასუხობს გლობალური უსაფრთხოების ნორმებსა და მსოფლიოში აღიარებულ სტანდარტებს;

ა.ა) **ღონისძიებები:**

ა.ა.ა) ინფორმაციული უსაფრთხოების მართვის სისტემის პოლიტიკის დოკუმენტის შემუშავება, დანერგვა და იმპლემენტაცია. დოკუმენტში ასახული იქნება თავდაცვის სფეროში აღნიშნული სისტემის დანერგვის, ფუნქციონირებისა და მონიტორინგის საჭირო ფაზები, ორგანიზაციის ინფორმაციული უსაფრთხოების მართვის სისტემის მიზნები, ძირითადი მიმართულებები, პრინციპები და შედეგები;

ა.ა.ბ) თავდაცვის სისტემაში ინფორმაციული უსაფრთხოების მართვის სისტემების გავრცელების სფეროს განსაზღვრა და დოკუმენტურად წარმოდგენა ორგანიზაციის სტრუქტურის, საქმიანობის, აქტივებისა და ტექნოლოგიების ჭრილში;

ა.ა.გ) ბიუროში არსებული აქტივების (მატერიალური და არამატერიალური) გამოვლენის, აღწერის, კლასიფიცირების, შეცვლისა და განადგურების წესების შემუშავება და განხორციელება;

ა.ა.დ) რისკებთან მოპყრობის გეგმის შემუშავება, დანერგვა და განხორციელება. აღნიშნული გეგმა გულისხმობს ინფორმაციული უსაფრთხოების რისკების მართვისთვის საჭირო ქმედებების, რესურსების, პასუხისმგებლობების, პრიორიტეტების, რისკების გავლენით გამოწვეული შედეგების შეფასების კრიტერიუმების განსაზღვრას და ანალიზის განხორციელებას თავდაცვის სფეროში;

ა.ა.ე) საჭირო წესების, სტანდარტების, ნორმებისა და მიდგომების შემუშავება;

ა.ბ) შედეგი: ამოცანის წარმატებულად განხორციელება ხელს შეუწყობს ინფორმაციული უსაფრთხოების რისკების ეფექტურ მართვას, ინფორმაციული და კომუნიკაციების ტექნოლოგიების უსაფრთხოების ინციდენტების სწრაფ იდენტიფიცირებას, მართვას, მონიტორინგს, ანალიზსა და პრევენციას, ინფორმაციული და კომუნიკაციების ტექნოლოგიების ინფრასტრუქტურის დაცვასა და განვითარებას;

ა.გ) ვადა: 2016 წ.;

ა.დ) მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები: სამინისტროს საინფორმაციო ტექნოლოგიების დეპარტამენტი, სამინისტროს თავდაცვის პოლიტიკისა და დაგეგმვის დეპარტამენტი, სამინისტროს გენერალური ინსპექცია;

ბ) ამოცანა 2 - „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ საქართველოს თავდაცვის მინისტრის 2014 წლის 7 აპრილის N26 ბრძანების შესაბამისად, სამინისტროში ინფორმაციული უსაფრთხოების საბჭოს შექმნა.

ბ.ა) ღონისძიებები - სამინისტროში ინფორმაციული უსაფრთხოების საბჭოს შექმნის შესახებ საქართველოს თავდაცვის მინისტრის ინდივიდუალური ადმინისტრაციულ-სამართლებრივი აქტის მომზადება;

ბ.ბ) შედეგი: აღნიშნული ამოცანის წარმატებულად გადაჭრა ხელს შეუწყობს თავდაცვის სფეროში ინფორმაციული უსაფრთხოების ეფექტურ მართვას;

ბ.გ) ვადა: 2016 წ.;

გ.დ) მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები: სამინისტროს ადმინისტრაციის სამართლებრივი უზრუნველყოფის სამმართველო;

გ) ამოცანა 3 - საქართველოს თავდაცვის სფეროს კიბერსივრცეში პოტენციური და არსებული/წარმოქმნილი საფრთხეებისა და გამოწვევების კვლევისა და ანალიზის რეგულარული განხორციელება;

გ.ა) ღონისძიებები:

გ.ა.ა) ბიუროში ანალიტიკური მუშაობის ინტენსიფიკაცია;

გ.ა.ბ) კიბერსივრცეში არსებული/წარმოქმნილი საფრთხეების ანალიზი და რისკების კვლევა;

გ.ა.გ) ღია წყაროების გამოყენებით ინფორმაციული ტექნოლოგიების სფეროში, მსოფლიოში მიმდინარე პროცესების მონიტორინგი, ანალიზი და რეკომენდაციების შემუშავება არსებული/წარმოქმნილი საფრთხეებიის პრევენციის, რისკების მინიმიზაციის და ინფორმაციული უსაფრთხოების სფეროში ცნობიერების ამაღლების მიზნით;

გ.ა.დ) რეკომენდაციებისა და კვლევების საფუძველზე პრევენციული ზომების შემუშავება და გატარება;

გ.ბ) შედეგი: კიბერუსაფრთხოების სფეროს განვითარების ხელშეწყობის მიზნით კიბერსივრცეში არსებული და მოსალოდნელი ვითარების, გამოწვევებისა და საფრთხეების ანალიზი, მათ შესახებ წინადადებების მომზადება, კიბერსაფრთხეების სტატისტიკის წარმოება, რისკების შეფასება, განხილვა და შესაბამისი რეკომენდაციების შემუშავება;

გ.გ) ვადა*:* 2016-2017 წწ.;

გ.დ) მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები: გენერალური შტაბის სამხედრო დაზვერვის დეპარტამენტი, გენერალური შტაბის J-6 კავშირგაბმულობის და ინფორმაციული სისტემების დეპარტამენტი, გენერალური შტაბის J-2 დაზვერვის დეპარტამენტი, სამინისტროს საინფორმაციო ტექნოლოგიების დეპარტამენტი, სამინისტროს ანალიტიკური დეპარტამენტი.

მუხლი 13.

ოპერაციული მოთხოვნები

ა) **ამოცანა 4** - ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ საქართველოს თავდაცვის მინისტრის 2014 წლის 7 აპრილის N26 ბრძანების შესაბამისად, ინფორმაციული უსაფრთხოების მართვის სისტემის მონიტორინგი და ინფორმაციული უსაფრთხოების ინციდენტებზე რეაგირება;

ა.ა) **ღონისძიებები:**

ა.ა.ა) პროცედურებისა და კონტროლის მექანიზმების დანერგვა, მონიტორინგის წარმოება, მონიტორინგის შედეგების გაანალიზება და საჭიროების შემთხვევაში, გაუმჯობესებისათვის აუცილებელი გზების განსაზღვრა, ინფორმაციული უსაფრთხოების სისტემების ფუნქციონირების ეფექტურობის პერიოდული შემოწმება, რისკების შეფასების გადახედვა;

ა.ა.ბ) ინფორმაციული უსაფრთხოების მართვის სისტემების აუდიტი და პერიოდული მიმოხილვა;

ა.ბ) შედეგი: აღნიშნული ამოცანის შესრულება ხელს შეუწყობს ბიუროს, სწორად განსაზღვროს ინფორმაციული უსაფრთხოების სისტემების ფუნქციონირებისათვის საჭირო კონტროლის მექანიზმები, მონიტორინგის შედეგების გათვალისწინებით დასახოს ინფორმაციული უსაფრთხოების ღონისძიებების განხორციელებისთვის აუცილებელი გეგმები და შეიმუშაოს მართვის სისტემების გაუმჯობესების ეფექტური გზები;

ა.გ) ვადა: 2016-2017 წწ.;

ა.დ) მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები: სამინისტროს საინფორმაციო ტექნოლოგიების დეპარტამენტი, სამინისტროს გენერალური ინსპექცია, გენერალური შტაბის J-6 კავშირგაბმულობის და ინფორმაციული სისტემების დეპარტამენტი.

ბ) ამოცანა 5 - თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტების ინფრასტრუქტურის დაცვის გაძლიერება და გამართულად ფუნქციონირების უზრუნველყოფა. ქსელური ინფრასტრუქტურის განვითარებისა და გაძლიერების ადეკვატურად ბიუროსთვის დამატებითი ტექნიკური შესაძლებლობების შექმნა, უსაფრთხოების კონტროლის დამატებითი მექანიზმების დანერგვა, ამოქმედება და განვითარება, რაც განაპირობებს ბიუროს მატერიალურ-ტექნიკურ და ადამიანური რესურსების ზრდის მოთხოვნილებას, უსაფრთხოების წესების, სტანდარტების, ნორმების განსაზღვრასა და შემუშავებას;

ბ.ა) ღონისძიებები:

ბ.ა.ა) თავდაცვის სისტემაში არსებული ინფორმაციული და კომუნიკაციების ტექნოლოგიების ინფრასტრუქტურის შესწავლა, ინფორმაციული უსაფრთხოების პერიოდული აუდიტის განხორციელება: სამინისტროს ინფორმაციული და კომუნიკაციების ტექნოლოგიების სისტემების უსაფრთხოების ხარისხისა და შეღწევადობის შესწავლა-შეფასება, რაც გულისხმობს ინფორმაციული ტექნოლოგიების სისტემაში გათვალისწინებული ან/და გაუთვალისწინებელი სისუსტეებისა და ხარვეზების გამოვლენასა და განსაზღვრას; ინფორმაციული ტექნოლოგიებისა და ინფორმაციული სისტემების უსაფრთხოების ხარისხის გაზრდისა და მოდერნიზაციის მიზნით რეკომენდაციების შემუშავება მიღებული ინფორმაციის საფუძველზე; ინფორმაციული ტექნოლოგიებისა და ინფორმაციული სისტემების განვითარების მოკლე და გრძელვადიანი გეგმების დასახვა კიბერუსაფრთხოების განხრით;

ბ.ა.ბ) ინფორმაციული და კომუნიკაციების ტექნოლოგიების სფეროში არსებული მსოფლიო გამოწვევების შესაბამისად თანამედროვე ტექნოლოგიებით აღჭურვის უზრუნველყოფაში ხელშეწყობა და საერთაშორისო პროგრამებში/პროექტებში მონაწილეობის მიღება;ბ.ა.გ) კიბერუსაფრთხოების სისტემის ინტეგრაცია სამხედრო სფეროსთან. კიბერუსაფრთხოების სფეროში არსებული საფრთხეების დასაძლევად მუდმივი მზადყოფნის მიზნით კრიზისული სიტუაციებისათვის სამოქმედო გეგმის შემუშავება, კიბერსივრცეში პოტენციური ინციდენტებისა და მათზე რეაგირებისათვის საჭირო ქმედებების სიმულაციების დოკუმენტურად შემუშავება და შემდგომში რეგულარული განხორციელება. ამ მიმართულებით მნიშვნელოვანია:

- აქტიური მონაწილეობის მიღება სამინისტროს მიერ ყოველწლიურად განხორციელებულ შესაბამის სამხედრო წვრთნებში;
- ბიუროს მიერ კიბერწვრთნების ორგანიზება და ჩატარება, რაც, როგორც ტექნიკურ, ასევე ოპერატიულ ასპექტებსა და სტრატეგიული გადაწყვეტილებების მიღების პროცედურებს მოიცავს;
- საერთაშორისო ტექნიკურ სავარჯიშოებსა და კიბერწვრთნებში მონაწილეობის მიღება;
- ინფრასტრუქტურის განვითარების შედეგად წარმოქმნილი ახალი კიბერრისკებისა და კიბერსაფრთხეების შესწავლა, შეფასება, ანალიზი;
- ინფრასტრუქტურის განვითარების შედეგად ბიუროს საჭიროებების განსაზღვრა;

ბ.ბ) შედეგი: ოცდამეერთე საუკუნეში დამკვიდრებული ცნების „ჰიბრიდული ომის“ აუცილებელი ატრიბუტია ოპერაციები კიბერსივრცეში. სამხედრო წვრთნებში კიბერუსაფრთხოების კომპონენტის შეტანა აამაღლებს როგორც ბიუროს, ასევე სამინისტროს შესაბამისი სტრუქტურული ერთეულების მზადყოფნის დონეს კიბერსივრცეში არსებული საფრთხეების წინაშე, შექმნის კიბერკრიზისების მართვის გაუმჯობესებისათვის აუცილებელ მექანიზმებს, ხელს შეუწყობს უწყებათაშორისი თანამშრომლობის გაღრმავებას, ბიუროსა და

სამინისტროს სტრუქტურულ ერთეულებს შორის მომავალში შეთანხმებულ მოქმედებას. აღნიშნული მექანიზმები უზრუნველყოფენ თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტების ინფრასტრუქტურის ეფექტურ დაცვას, გაძლიერებასა და გამართულად ფუნქციონირებას. აღნიშნული ამოცანის წარმატებულად შესრულებით გაძლიერდება თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტების ინფრასტრუქტურის დაცვა და უზრუნველყოფილი იქნება მისი გამართულად ფუნქციონირება;

ბ.გ) ვადა: 2016-2017 წწ.;

ბ.დ) მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები: გენერალური შტაბის J-6 კავშირგაბმულობის და ინფორმაციული სისტემების დეპარტამენტი, გენერალური შტაბის სამხედრო დაზვერვის დეპარტამენტი, გენერალური შტაბის J-3 ოპერატიული დაგეგმვის დეპარტამენტი, გენერალური შტაბის J-4/8 ლოგისტიკისა და რესურსების დაგეგმვის დეპარტამენტი, გენერალური შტაბის J-2 დაზვერვის დეპარტამენტი, გენერალური შტაბის ჯარების ლოგისტიკური უზრუნველყოფის სარდლობა, გენერალური შტაბის ეროვნული გვარდია, სამინისტროს საინფორმაციო ტექნოლოგიების დეპარტამენტი, სამინისტროს ანალიტიკური დეპარტამენტი;

გ) ამოცანა 6 - ბიუროში საკადრო პოლიტიკის გატარება და ეფექტური მეთოდების შემუშავება; პერსონალის პროფესიული განვითარება, მათი კომპეტენციის ამაღლება და კვალიფიციური კადრების შენარჩუნება;

გ.ა) ღონისძიებები:

გ.ა.ა) ადამიანური რესურსების მართვისა და პროფესიული განვითარების მიზნით კონცეპტუალური დოკუმენტების შემუშავება:

გ.ა.ბ) ბიუროს ადამიანური რესურსების მართვისა და პროფესიული განვითარების კონცეფციის შემუშავება და დამტკიცება;

გ.ა.გ) ბიუროს პერსონალის მართვის სისტემის განვითარების 2016-2017 წლების სტრატეგიის შემუშავება და დამტკიცება;

გ.ა.დ) ბიუროს გენდერული თანასწორობის სტრატეგიის შემუშავება და დამტკიცება;

გ.ა.ე) პროფესიული განვითარების პროგრამების დაგეგმვის, მონაწილეთა შერჩევისა და მათი ეფექტიანობის შეფასების რეგულაციის სრულყოფის მიზნით შემდეგი ღონისძიების

განხორციელებაა პერსონალის პროფესიული განვითარების პროგრამების დაგეგმვისა და პროგრამებისათვის კანდიდატთა შერჩევის საბჭოს შექმნა;

გ.ა.ვ) ბიუროს კვალიფიციური ადამიანური რესურსებით უზრუნველყოფის და შემდგომში მათ მიერ შესრულებული სამუშაოს შეფასების სისტემების ჩამოყალიბების, ასევე კარიერის დაგეგმვისა და მართვის მიზნით შემდეგი ღონისძიებების გატარება:
- ერთიანი საკვალიფიკაციო მოთხოვნების შემუშავება;
- თანამდებობრივი კომპეტენციების ნუსხის შემუშავება;
- სამუშაოთა კლასიფიკაციის სისტემის შემუშავება;
- სამუშაოს შესრულების ხარისხის მართვისა და შეფასების სისტემის შემუშავება;

გ.ა.ზ) პერსონალის ცოდნის, გამოცდილების, უნარ-ჩვევებისა და კვალიფიკაციის განსაზღვრის მიზნით, ფაქტობრივი და შედარებითი ანალიზის შემუშავება (GAP Analysis);

გ.ა.თ) სერთიფიცირებული ტრეინინგების, ბიუროს პერსონალის პროფესიულ განვითარებაზე ორიენტირებული პროექტებისა და საგანმანათლებლო პროგრამების უზრუნველყოფა, რაც საკადრო პოლიტიკის ერთ-ერთი ძირითადი კომპონენტია. საკადრო რესურსის უწყვეტი პროფესიული ზრდისა და განვითარებისათვის მნიშვნელოვანია ბიუროს პერსონალის ჩართვა მსოფლიოში აპრობირებულ და სერთიფიცირებულ ისეთ ტრეინინგებსა და პროგრამებში, რომლებიც პასუხობენ კიბერუსაფრთხოების სფეროში არსებულ მოთხოვნებს, ბიუროს თანამშრომლებისთვის უზრუნველყოფენ თანამედროვე მიდგომებსა და ტექნოლოგიებს;

გ.ა.ი) ბიუროს ორგანიზაციული განვითარებისა და გაძლიერებისათვის პრიორიტეტულ მიმართულებების განსაზღვრა, რასაც წარმოადგენს კიბერთავდაცვითი წვრთნები, ინციდენტების მართვა, კვლევა, ანალიზი და გამოძიება; ინფორმაციული უსაფრთხოების სისტემების მართვა, აუდიტი და მონიტორინგი, პრევენციის მეთოდები, და ა.შ.;

გ.ა.კ) არსებული კანონმდებლობის საერთაშორისო ნორმებთან შესაბამისობაში მოყვანა, ადმინისტრაციული პროცედურების, საერთაშორისო ურთიერთობების, სახელმწიფო შესყიდვების უზრუნველყოფა, საქმიანი დოკუმენტების მომზადება და აღრიცხვიანობა, ლოგისტიკური უზრუნველყოფისა და ფინანსური რესურსების მენეჯმენტი და ა. შ.;

გ.ა.ლ) საერთაშორისო და ადგილობრივ კიბერწვრთნებში, ტექნიკურ სავარჯიშოებში, სემინარებში, კონფერენციებსა და სიმპოზიუმებში მონაწილეობის მიღებაში ხელშეწყობა კიბერუსაფრთხოების სფეროში;

გ.ა.მ) მდგრადი საკადრო პოლიტიკის დანერგვისათვის აუცილებელი მექანიზმების შემუშავება და გატარება, კერძოდ, ორგანიზაციული კულტურის შექმნა, რაც ბიუროს პერსონალს საკუთარი

ცოდნის, შესაძლებლობების უკეთ გამოყენებისა და გამოვლენის საშუალებას მისცემს; შეუქმნის სათანადო სამუშაო პირობებსა და გარემოს; მინიმუმამდე დაიყვანს კვალიფიციური პერსონალის გადინების პროცესს; საჭიროების შემთხვევაში, ბიუროს ძირითად დანაყოფებში სამხედრო კომპონენტის ჩართვა, კიბერშესაძლებლობების ინტეგრირება სამხედრო ძალებთან და შესაბამისი ღონისძიებების განხორციელება;

გ.ა.ნ) კიბერუსაფრთხოების სფეროში ინფორმაციული ტექნოლოგიების, ინოვაციების დანერგვაში ხელშეწყობა, ასევე სხვადასხვა ინტელექტუალური პროდუქტის შექმნა. კიბერუსაფრთხოების სფეროში ტერმინოლოგიის განსაზღვრა სხვადასხვა დოკუმენტის შინაარსის სწორად აღქმის, ინტერპრეტაციისა და ზოგადად, ნებისმიერი კომუნიკაციური უზუსტობის თავიდან აცილების მიზნით;

გ.ა.ო) სამინისტროს სისტემაში არსებულ საგანმანათლებლო სივრცეში კიბერუსაფრთხოების კურსის დანერგვა და სასწავლო პროგრამების შემუშავებაში ხელშეწყობა;

გ.ა.პ) 2016 წელს ნატოს კიბერწვრთნებში მონაწილეობის მიღების მიზნით, სამხედრო კონტინგენტის მომზადება;

გ.ბ) შედეგი: ადამიანური რესურსების სწორად მართვა და განვითარება ხელს შეუწყობს თავდაცვის სისტემაში კიბერუსაფრთხოების მიმართულებით დასახული სტრატეგიული მიზნებისა და ამოცანების ეფექტურად შესრულებას. ბიუროს საგანმანათლებლო პოლიტიკა ორიენტირებულია მსოფლიოში წამყვანი ინსტიტუციების სერთიფიცირებულ პროგრამებზე (ნატოს კოოპერაციული კიბერთავდაცვის სასწავლო ცენტრები, SANS, ISACA, ENISA, FIRST და ა. შ);

გ.გ) ვადა: 2016-2017 წწ.;

გ.დ) მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები: სამინისტროს ადამიანური რესურსების მართვისა და პროფესიული განვითარების დეპარტამენტი, სამინისტროს ადმინისტრაციის ნატოს კლასიფიცირებული ინფორმაციის უსაფრთხოების სამსახური, სამინისტროს საერთაშორისო ურთიერთობებისა და ევროატლანტიკური ინტეგრაციის დეპარტამენტი, სამინისტროს ადმინისტრაციის მასმედიასთან ურთიერთობის სამმართველო, სამინისტროს პარლამენტთან ურთიერთობისა და სამართლებრივ საკითხთა დეპარტამენტი, გენერალური შტაბის წვრთნებისა და სამხედრო განათლების სარდლობა, სსიპ დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემიის პროფესიული განვითარების ცენტრი (PDC), აშშ-ს თავდაცვის გამოყენებითი ჯგუფი (CUBIC), საქართველოს

წარმომადგენლობა ნატოში, საქართველოში ნატოს სამეკავშირეო ოფისი (NLO), ნატო-საქართველოს პროფესიული განვითარების პროგრამა (PDP);

დ) ამოცანა 7 - ბიუროს მიერ კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების 24/7 მექანიზმების დანერგვა, ამოქმედება და განვითარება;

დ.ა) ღონისძიებები:

დ.ა.ა) კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის (CERT) ინფორმაციული და კომუნიკაციების ტექნოლოგიების მაღალკვალიფიციური და მოტივირებული სპეციალისტებით დაკომპლექტება;

დ.ა.ბ) კომპიუტერულ ინციდენტებზე დახმარების 24/7 ჯგუფების შესაძლებლობების მუდმივი განვითარება და მათთვის სტანდარტული საოპერაციო პროცედურების თანახმად შესაბამისი ინსტრუქციებისა და პროცედურების შემუშავება;

დ.ა.გ) კვალიფიკაციის ამაღლებისა და პროფესიული ზრდის ხელშეწყობის მიზნით ბიუროს პერსონალის მონაწილეობა საერთაშორისო სერთიფიცირების პროგრამებში. აღნიშნული ინიციატივა მოიცავს საინფორმაციო სისტემების აუდიტორის, ინფორმაციული უსაფრთხოების მენეჯერის, საინფორმაციო სისტემების რისკებისა და კონტროლის მართვისა და სხვა სერთიფიცირების პროგრამებს. აღნიშნული სერთიფიცირება ხელს შეუწყობს ბიუროში დასაქმებულ პირებს, მოიპოვონ მსოფლიოში აღიარებული ინფორმაციული ტექნოლოგიების აუდიტის სერთიფიკატები, რაც ბიუროს აუდიტორული საქმიანობის შესაძლებლობებს შეუქმნის;

დ.ა.დ) ნატოსა და ევროკავშირის ქვეყნების კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფებთან მჭიდრო ურთიერთობების დამყარება და განვითარება;

დ.ა.ე) კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფების საერთაშორისო გაერთიანებებსა და ფორუმებში გაწევრიანება;

დ.ა.ვ) საერთაშორისო და ადგილობრივ დონეზე კონფერენციებსა და სიმპოზიუმებში მონაწილეობის მიღება;

დ.ა.ზ) სამთავრობო და არასამთავრობო სექტორთან ერთად სხვადასხვა აქტივობისა და ერთობლივი პროექტების დაგეგმვა და განხორციელება კიბერუსაფრთხოების სფეროში;

დ.ბ) შედეგი: აღნიშნული ღონისძიებების გატარებით კომპიუტერულ ინციდენტებზე დახმარების ჯგუფებს ექნებათ გამოცდილებისა და საუკეთესო პრაქტიკის გაზიარების, თანამედროვე მიდგომების, მეთოდების გაცნობისა და მათი ადგილობრივ დონეზე დანერგვის

შესაძლებლობა, უსაფრთხოების წესების, სტანდარტების, პროცედურებისა და სტრატეგიების ერთობლივად შემუშავებისა და განვითარების საშუალება, რაც უზრუნველყოფს სამინისტროს ინფორმაციული და კომუნიკაციების ტექნოლოგიების ინფრასტრუქტურის დაცვას, საფრთხეებისა და რისკების სწრაფ იდენტიფიცირებას, მათზე რეაგირებას, პრევენციული ზომების გატარებას და საჭიროების შემთხვევაში, კრიზისების მართვას პროგნოზირებადი, პრევენციული, დაცვითი, აღდგენითი მექანიზმების საშუალებით;

დ.გ) ვადა: 2016 წ.;

დ.დ) მხარდამჭერი სტრუქტურული ერთეულები - გენერალური შტაბის J-6 კავშირგაბმულობის და ინფორმაციული სისტემების დეპარტამენტი, სამინისტროს ადამიანური რესურსების მართვისა და პროფესიული განვითარების დეპარტამენტი, სამინისტროს საერთაშორისო ურთიერთობებისა და ევროატლანტიკური ინტეგრაციის დეპარტამენტი, სამინისტროს საინფორმაციო ტექნოლოგიების დეპარტამენტი, სამინისტროს თავდაცვის ატაშეებისა და სამინისტროს წარმომადგენლების ოფისი, სსიპ დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემიის პროფესიული განვითარების ცენტრი (PDC), საქართველოში ნატოს სამეკავშირეო ოფისი (NLO);

ე) ამოცანა 8 - გენერალური შტაბის ეროვნულ გვარდიასთან ერთად მოხალისეთა კავშირი - კიბერრაზმის ჩამოყალიბება და კიბერრეზერვისტთა მომზადება. აღნიშნული ამოცანის მიზანია კიბერშესაძლებლობების განვითარებისა და გაძლიერების ხელშეწყობა, რაც, საბოლოო ჯამში, ქვეყნის საერთო თავდაცვისუნარიანობას აამაღლებს;

ე.ა) ღონისძიებები:

ე.ა.ა) სამართლებრივი ბაზის შექმნა, რის საფუძველზეც ჩამოყალიბდება მოხალისეთა კავშირი - კიბერრაზმი;

ე.ა.ბ) გასაწვევი კონტინგენტის საკვალიფიკაციო მოთხოვნების განსაზღვრა;

ე.ა.გ) კიბერრეზერვისტთა მონაცემთა ბაზის შექმნა;

ე.ა.დ) სასწავლო პროგრამის შემუშავება;

ე.ა.ე) ინსტრუქტორების შერჩევა;

ე.ა.ვ) გაწვევის პერიოდის განსაზღვრა;

ე.ა.ზ) კიბერრეზერვის მომზადება;

ე.ბ) შედეგი: მოხალისეთა კავშირი - კიბერრაზმი დაეხმარება კიბერუსაფრთხოების სფეროში მოქმედ აქტორებს, უზრუნველყონ კიბერსივრცის ეფექტური დაცვა. მოხალისეთა კავშირი - კიბერრაზმის მიზანია თავისუფალ ნებაზე და ინიციატივებზე დაყრდნობით განავითაროს და

გააძლიეროს ქვეყნის კიბერშესაძლებლობები, რაც მოიცავს შემდეგი ქმედებების განხორციელებას:

ე.ბ.ა) საჯარო და კერძო სექტორს შორის თანამშრომლობა ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის დაცვის კუთხით;
ე.ბ.ბ) მუდმივ რეჟიმში მექანიზმების შემუშავების ინიცირება, რაც უზრუნველყოფს კიბერსაფრთხეებისა და კიბერრისკების წინაშე მდგრადობის გაძლიერებასა და შენარჩუნებას;

ე.ბ.გ) გაერთიანების ფოკუსირება მშვიდობიან და კრიზისულ სიტუაციებში სამოქმედო მხარდამჭერი შესაძლებლობების განსაზღვრაზე სამოქალაქო სექტორის დახმარების მიზნით;

ე.ბ.დ) საომარი, კრიზისული ან/და საგანგებო მდგომარეობის დროს ან ეროვნული უსაფრთხოების ინტერესებიდან გამომდინარე შესაბამისი ამოცანების შესრულება;

ე.ბ.ე) ცოდნისა და გამოცდილების გაზიარება კიბერუსაფრთხოების სფეროში;

ე.ბ.ვ) საჯარო და კერძო სექტორში ინფორმაციული უსაფრთხოების მიმართულებით მოღვაწე სპეციალისტების გაერთიანება. ამ ტიპის საზოგადოება უზრუნველყოფს ეროვნული თავდაცვის პრობლემების კერძო ორგანიზაციების ინტერესებთან გაერთიანების დამატებით შესაძლებლობებს, ასევე დახმარებას კრიტიკული ინფრასტრუქტურის დაცვაში და მშვიდობიან და კრიზისულ სიტუაციებში მომსახურებას;

ე.ბ.ზ) მოხალისეთა კავშირი - კიბერრაზმის ინფორმაციული უსაფრთხოების სპეციალისტებისთვის სამხედრო წვრთნების ორგანიზება და ზედამხედველობა; საჭირო ტრეინინგების, კურსებისა და პრაქტიკული გარემოს უზრუნველყოფა. მიღებული გამოცდილებითა და ცოდნით ისინი დამატებით პროფესიულ უნარ-ჩვევებს შეიძენენ;

ე.გ) ვადა*:* 2016-2017 წწ.;

ე.დ) მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები: სამინისტრო, გენერალური შტაბის ეროვნული გვარდია, გენერალური შტაბის J-3 ოპერატიული დაგეგმვის დეპარტამენტი, საქართველოს იუსტიციის სამინისტროს სსიპ - მონაცემთა გაცვლის სააგენტო.

მუხლი 14.

ცნობიერების ამაღლება, განათლება და თანამშრომლობა;

ა) **ამოცანა 9** - ,,კიბერუსაფრთხოების პოლიტიკის დამტკიცების შესახებ'' საქართველოს თავდაცვის მინისტრის 2014 წლის 4 ნოემბრის N MOD 7 14 00001575 ბრძანების შესაბამისად, მჭიდრო ინსტიტუციური კოორდინაცია კიბერუსაფრთხოების უზრუნველყოფის მიმართულებით; კიბერუსაფრთხოების უზრუნველყოფის უმნიშვნელოვანესი ასპექტია საერთო მხარდაჭერა - უწყებათაშორისი თანამშრომლობა და აქტიური კოორდინაცია სახელმწიფო უწყებებთან, ინფორმაციული უსაფრთხოების სფეროს კერძო კომპანიებთან, ინტერნეტ-სერვის პროვაიდერებთან, IT სფეროთი დაინტერესებულ არასამთავრობო ორგანიზაციებთან. მსოფლიო პრაქტიკიდან გამომდინარე, სახელმწიფო უწყებას, როგორც წესი, არ შეუძლია საკუთარი ინფორმაციული და კომუნიკაციების ტექნოლოგიების სისტემების დაცვა დამოუკიდებლად;

ა.ა) **ღონისძიებები:**

ა.ა.ა) მჭიდრო თანამშრომლობა სამთავრობო უწყებებთან ხელს შეუწყობს თანამედროვე და განვითარებადი საფრთხეების, ინციდენტებისა და მათი პრევენციის საშუალებების შესახებ ინფორმაციის დროულ გაცვლას, გამოცდილების გაზიარებასა და კოორდინირებულ მუშაობას კიბერუსაფრთხოების სფეროში;

ა.ა.ბ) აქტიური თანამშრომლობა კიბერუსაფრთხოების სფეროთი დაინტერესებულ არასამთავრობო სექტორთან, რომლის ფარგლებშიც გაიმართება სამუშაო შეხვედრები, კონსულტაციები კონცეპტუალური დოკუმენტების, კიბერსივრცეში თანამედროვე გამოწვევებისა და კიბერუსაფრთხოების სფეროში სხვადასხვა აქტუალური საკითხის განხილვისა და ამ სფეროში რეკომენდაციების შემუშავების/წარმოდგენის მიზნით. არასამთავრობო ორგანიზაციების ჩართულობა კიბერუსაფრთხოების სფეროში ხელს შეუწყობს ამ მიმართულებით მიმდინარე პროცესების გამჭვირვალობის ამაღლებას;

ა.ა.გ) საჯარო და კერძო სექტორებს შორის თანამშრომლობის პლატფორმის შექმნა (PPP-Public Private Partnership) და განვითარება ხელს შეუწყობს კიბერშესაძლებლობების გაძლიერებას, ნდობის ამაღლებას, კიბერუსაფრთხოების მიმართულებით მუდმივ რეჟიმში ინფორმაციის გაცვლას;

ა.ბ) შედეგი: აღნიშნული ამოცანის განხორციელება ხელს შეუწყობს კოორდინირებული ინსტიტუციური რგოლის შექმნას კიბერუსაფრთხოების სფეროში, რაც, თავის მხრივ ქვეყნის კიბერთავდაცვითი მექანიზმების გაძლიერებას ითვალისწინებს;

ა.გ) **ვადა:** 2016-2017 წწ.;

ა.დ) **მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები:** სამინისტროს თავდაცვის პოლიტიკისა და დაგეგმვის დეპარტამენტი, სსიპ - დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემიის პროფესიული განვითარების ცენტრი (PDC), სამინისტროს ადმინისტრაციის მასმედიასთან ურთიერთობის სამმართველო, სამინისტროს ადმინისტრაციის პროტოკოლის სამსახური;

ბ) **ამოცანა 10** - ეროვნული კონცეპტუალური დოკუმენტების (მათ შორის საქართველოს საფრთხეების შეფასების დოკუმენტი), ასევე სხვა, როგორც ეროვნული, ისე უწყებრივი დოკუმენტების შემუშავების პროცესში მონაწილეობის მიღება კომპეტენციის ფარგლებში;

ბ.ა) **ღონისძიებები** - სამხედრო სფეროში კიბერსაფრთხეებისა და კიბერრისკების იდენტიფიცირება, კლასიფიცირება, მათზე რეაგირებისა და შესაძლო სცენარების, მოვლენების განვითარებისა და სავარაუდო ანალიზის შედეგების შემუშავება;

ბ.ბ) **შედეგი:** აღნიშნული ქმედებები ხელს შეუწყობს საქართველოს თავდაცვის სფეროში არსებული კიბერგამოწვევების დაძლევასა და კიბერსაფრთხეების პრევენციას, სახელმწიფო უსაფრთხოების უზრუნველყოფასა და ქვეყნის თავდაცვისუნარიანობის ამაღლებას;

ბ.გ) **ვადა**: 2016-2017 წწ.;

ბ.დ) **მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები:** გენერალური შტაბის სამხედრო დაზვერვის დეპარტამენტი, გენერალური შტაბის J-6 კავშირგაბმულობის და ინფორმაციული სისტემების დეპარტამენტი, გენერალური შტაბის J-2 დაზვერვის დეპარტამენტი, სამინისტროს საინფორმაციო ტექნოლოგიების დეპარტამენტი, სამინისტროს ანალიტიკური დეპარტამენტი;

გ) **ამოცანა 11** - „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ საქართველოს თავდაცვის მინისტრის 2014 წლის 7 აპრილის N26 ბრძანებისა და „კიბერუსაფრთხოების პოლიტიკის დამტკიცების შესახებ“ საქართველოს თავდაცვის მინისტრის 2014 წლის 4 ნოემბრის N MOD 7 14 00001575 ბრძანების თანახმად, კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლება. კიბერუსაფრთხოების უზრუნველყოფის ერთ-ერთი სტრატეგიული ნაწილი „კიბერუსაფრთხოების კულტურის” (Cyber Security Culture) დანერგვა და განვითარებაა, რაც გულისხმობს ცნობიერების ამაღლებას კიბერუსაფრთხოების სფეროში. კიბერუსაფრთხოება, არა მარტო რიგითი მოქალაქეებისთვის, არამედ აკადემიური წრეებისთვისაც შედარებით ახალი ტერმინია მსოფლიოში. კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლება ხელს შეუწყობს საზოგადოებას, უკეთ

აღიქვას კიბერუსაფრთხოების მნიშვნელობა, მისი როლი და გააცნობიეროს კიბერშეტევებით გამოწვეული შესაძლო შედეგები;

გ.ა) ღონისძიებები - კიბერუსაფრთხოების საინფორმაციო დღეების, სემინარებისა და კონფერენციების ორგანიზება, საგანმანათლებლო პროგრამების შემუშავება, მათი რეგულარული განხორციელება სამინისტროს სამოქალაქო ოფისის, საქართველოს შეიარაღებული ძალების ქვედანაყოფების, სამინისტროში შემავალი საჯარო სამართლის იურიდიული პირების თანამშრომლებისათვის, საქართველოში აკრედიტებული უმაღლესი სასწავლებლების სტუდენტებისათვის, სპეციალური სამიზნე ჯგუფებისათვის;

გ.ბ) შედეგი: აღნიშნული ღონისძიებების რეგულარულად განხორციელება ხელს შეუწყობს თითოეულ მომხმარებელს, თავიდან აიცილოს მინიმალური რისკები, გაეცნოს განახლებულ ინფორმაციას კომპიუტერულ, მობილურ, სხვადასხვა კომუნიკაციურ მოწყობილობაზე, ისწავლოს ელექტრონული ფოსტის უსაფრთხოდ გამოყენება და ა. შ., მიიღოს ინფორმაცია იმ საჭირო მექანიზმების შესახებ, რაც დაეხმარება მათ უსაფრთხოდ ფუნქციონირებაში. კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლება შექმნის ბიუროსა და სხვადასხვა უწყებას შორის მჭიდრო და კოორდინირებული თანამშრომლობის მყარ საფუძვლებს;

გ.გ) ვადები*:* 2016-2017 წწ.;

გ.დ) მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები: სამინისტროს ადამიანური რესურსების მართვისა და პროფესიული განვითარების დეპარტამენტი, სამინისტროს ადმინისტრაციის მასმედიასთან ურთიერთობის სამმართველო, სამინისტროს საინფორმაციო ტექნოლოგიების დეპარტამენტი, სამინისტროს სტრატეგიული კომუნიკაციების დეპარტამენტი, გენერალური შტაბის წვრთნებისა და სამხედრო განათლების სარდლობა, გენერალური შტაბის J-6 კავშირგაბმულობის და ინფორმაციული სისტემების დეპარტამენტი, სსიპ დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემიის პროფესიული განვითარების ცენტრი (PDC), საქართველოში ნატოს სამეკავშირეო ოფისი (NLO), ნატო-საქართველოს პროფესიული განვითარების პროგრამა (PDP);

დ) ამოცანა 12 - ,,კიბერუსაფრთხოების პოლიტიკის დამტკიცების შესახებ'' საქართველოს თავდაცვის მინისტრის 2014 წლის 4 ნოემბრის N MOD 7 14 00001575 ბრძანების თანახმად, საქართველოს კანონმდებლობის საერთაშორისო სამართლებრივ ნორმებთან ჰარმონიზაციის უზრუნველყოფა საქართველოს თავდაცვის სფეროში;

დ.ა) ღონისძიებები:

დ.ა.ა) ადგილობრივი კანონმდებლობის საერთაშორისო სტანდარტებთან და ნორმებთან შესაბამისობაში მოყვანა;

დ.ა.ბ) ინფორმაციული ტექნოლოგიების სფეროში შესაბამისი ნორმატიული აქტების შემუშავება;

დ.ა.გ) სპეციალიზებული კანონმდებლობის ფორმირება სამართლებრივი რეგულაციების, საკანონმდებლო და კანონქვემდებარე აქტების საშუალებით კიბერუსაფრთხოების სფეროში;

დ.ა.დ) კანონმდებლობით დადგენილი წესის შესაბამისად აქტივების გამოვლენის, აღწერის, კლასიფიცირების, შეცვლისა და განადგურების წესების შემუშავება და გამოცემა;

დ.ა.ე) ,,სსიპ - კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ'' საქართველოს თავდაცვის მინისტრის 2014 წლის წლის 7 აპრილის N27 ბრძანებით შექმნილი დახმარების ჯგუფის საქმიანობის უზრუნველყოფის მიზნით, მისთვის სამართლებრივი მხარდაჭერის აღმოჩენა, კომპეტენციის ფარგლებში სათანადო დოკუმენტაციის მომზადება და სამართლებრივი კონსულტირება;

დ.ა.ვ) ბიუროში 24/7 პრინციპით კიბერსამართლებრივი კონსულტაციების გაწევის დანერგვა;

დ.ა.ზ) ,,კიბერდანაშაულის შესახებ“ 2001 წლის ევროპის საბჭოს კონვენციის 35-ე მუხლის შესრულება - 24/7 ცხელი ხაზის შექმნა და ამოქმედება თავდაცვის სფეროს კიბერუსაფრთხოების მიმართულებით;

დ.ბ) შედეგი: საკანონმდებლო ბაზის დახვეწა კიბერუსაფრთხოების სფეროში ხელს შეუწყობს სამინისტროს კიბერუსაფრთხოების სისტემის სრულფასოვნად ჩამოყალიბებას, კიბერუსაფრთხოების დაცვის ქმედითი და ეფექტური მექანიზმების შექმნას, სამართლებრივი ჩარჩოების განვითარებას და გაძლიერებას, კიბერუსაფრთხოების სფეროში ქვეყნების ერთობლივად მუშაობას გარკვეული მიზნების მისაღწევად და გადაწყვეტილებების მისაღებად;

დ.გ) ვადა: 2016-2017 წწ.;

დ.დ) მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები: სამინისტროს პარლამენტთან ურთიერთობისა და სამართლებრივ საკითხთა დეპარტამენტი, სამინისტროს თავდაცვის პოლიტიკისა და დაგეგმვის დეპარტამენტი, სამინისტროს ადმინისტრაციის სამართლებრივი უზრუნველყოფის სამმართველო;

ე) ამოცანა 13 - კიბერუსაფრთხოების უზრუნველყოფისათვის საერთაშორისო თანამშრომლობის განვითარება და განმტკიცება;

ე.ა) ღონისძიებები:

ე.ა.ა) კიბერუსაფრთხოების საკითხებთან დაკავშირებით საერთაშორისო მექანიზმების ამოქმედება, ორმხრივი და მრავალმხრივი ურთიერთობების დამყარება და განვითარება NATO-სა და ევროკავშირის ქვეყნების კიბერდანაყოფებთან;

ე.ა.ბ) ევროკავშირის საგარეო ქმედებათა სამსახურის (EEAS) კიბერუსაფრთხოების დირექტორატთან (Directorate K) და ასევე, ევროკავშირის შესაბამის სტრუქტურებთან ურთიერთობების დამყარება და განვითარება; კიბერუსაფრთხოების პოლიტიკის მიდგომებისა და გამოცდილების გაზიარება;

ე.ა.გ) თანამშრომლობის ჩამოყალიბება და განმტკიცება საერთაშორისო ორგანიზაციების კიბერუსაფრთხოების სფეროსთან დაკავშირებულ ქვესტრუქტურებთან და მათი ეგიდით ორგანიზებულ საგანმანათლებლო პროგრამებში, ტრეინინგებში, კიბერწვრთნებში, სემინარებსა და კონფერენციებში მონაწილეობის მიღება (EU-ENISA, NATO-CCD COE, OSCE, SEDM ა. შ.);

ე.ა.დ) სტრატეგიული პარტნიორობის ფარგლებში, ქვეყნის უმთავრეს სტრატეგიულ პარტნიორთან ამერიკის შეერთებულ შტატებთან თანამშრომლობის გაღრმავება კიბერუსაფრთხოების მიმართულებით;

ე.ა.ე) ესტონეთთან, როგორც კიბერუსაფრთხოების სფეროში ერთ-ერთ წამყვან ქვეყანასთან, თანამშრომლობის გაღრმავება კიბერუსაფრთხოების მიმართულებით;

ე.ა.ვ) ნატო-საქართველოს თანამშრომლობის ფორმატში ყოველწლიური ეროვნული პროგრამისა (ANP) და დაგეგმვისა და მიმოხილვის პროცესის (PARP) ფარგლებში აღებული ვალდებულებების დროულად და ეფექტურად შესრულება;

ე.ა.ზ) ნატო-საქართველოს არსებითი პაკეტის (SNGP) ფარგლებში კიბერუსაფრთხოების შესაძლებლობების განვითარება ნატოს შესაბამის სტრუქტურებთან და წევრ ქვეყნებთან თანამშრომლობით;

ე.ა.თ) მჭიდრო თანამშრომლობა საქართველოში აკრედიტებულ უცხო ქვეყნებისა და საზღვარგარეთ საქართველოს თავდაცვის ატაშეებთან კიბერუსაფრთხოების მიმართულებით;

ე.ა.ი) კიბერუსაფრთხოების სფეროში რეგიონული თანამშრომლობის ფორმატის შექმნა და განვითარება;

ე.ბ) შედეგი: აღნიშნული ამოცანის წარმატებულად განხორციელება ხელს შეუწყობს საგანმანათლებლო პროგრამებში, ტრეინინგებში, საერთაშორისო კიბერწვრთნებში მონაწილეობის შესაძლებლობების შექმნას, ინფორმაციის გაცვლას თანამედროვე და განვითარებადი კიბერსაფრთხეების, ახალი ინციდენტებისა და მათი პრევენციის საშუალებების შესახებ, საუკეთესო გამოცდილებისა და პრაქტიკის გაზიარებას, მსოფლიოში აღიარებული სტანდარტების გაცნობასა და მათ ადგილობრივ დონეზე დანერგვას კიბერუსაფრთხოების სფეროში. საერთაშორისო თანამშრომლობა თავდაცვის სფეროში კიბერუსაფრთხოების უზრუნველყოფისათვის საჭირო ეფექტურ კიბერშესაძლებლობებს განავითარებს და შესაბამისად გააძლიერებს ინფორმაციული და კომუნიკაციების ტექნოლოგიების უსაფრთხო სისტემის დანერგვისა და ქვეყანაში მისი ამოქმედების მექანიზმებს;

ე.გ) ვადა: 2016-2017 წწ.;

ე.დ) მხარდამჭერი სტრუქტურული ერთეულები/ორგანიზაციები: სამინისტროს საერთაშორისო ურთიერთობებისა და ევროატლანტიკური ინტეგრაციის დეპარტამენტი, სამინისტროს ადმინისტრაციის ნატოს კლასიფიცირებული ინფორმაციის უსაფრთხოების სამსახური, სამინისტროს თავდაცვის ატაშეებისა და სამინისტროს წარმომადგენლების ოფისი, სსიპ დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემიის პროფესიული განვითარების ცენტრი (PDC), გენერალური შტაბის წვრთნებისა და სამხედრო განათლების სარდლობა, აშშ-ს თავდაცვის გამოყენებითი ჯგუფი (CUBIC), საქართველოს წარმომადგენლობა ნატოში, სამინისტროს სამოქალაქო წარმომადგენლის აპარატი ნატოსა და ევროკავშირში.

თავი V

დასკვნითი ნაწილი

მუხლი 15.

1. წინამდებარე დოკუმენტი მიმოიხილავს იმ ამოცანებს, რომლებიც განსხვავდებიან ერთმანეთისაგან, თუმცა მჭიდროდ არიან ერთმანეთთან დაკავშირებული და მხოლოდ ერთობლივად უზრუნველყოფენ თავდაცვის სფეროს ინფორმაციული და კომუნიკაციების ტექნოლოგიების სტაბილურ, ეფექტურ და უსაფრთხო სისტემებს.

2. აღნიშნული დოკუმენტის შემუშავებისას ბიურო მჭიდროდ თანამშრომლობდა სამინისტროსთან და უცხოელ პარტნიორებთან კიბერუსაფრთხოების სფეროში.

3. 2016-2017 წლების სამოქმედო გეგმით გათვალისწინებული ამოცანების ეტაპობრივი განხორციელება გაზრდის ქვეყნის თავდაცვისუნარიანობას და დაიცავს ინფორმაციული და კომუნიკაციების ტექნოლოგიების სისტემებს იმ კიბერრისკებისა და კიბერსაფრთხეებისაგან, რომლებმაც შესაძლოა, ზიანი მიაყენონ სახელმწიფო უსაფრთხოებას.

4. წინამდებარე დოკუმენტის შესრულებაზე პასუხისმგებელია ბიურო, რომელიც აქტიური ძალისხმევით უზრუნველყოფს ინფორმაციული და კომუნიკაციების ტექნოლოგიების ეფექტურ და საიმედო ინფრასტრუქტურას სამინისტროს სისტემისთვის და შექმნის ჩვენი ქვეყნის ევროპულ და ევროატლანტიკურ სივრცეში ინტეგრაციის მყარ საფუძველს.

Contents

Cyber Security Development Action Plan

Chapter I

Foreword

Article 1.

"Cyber Security Development Action Plan" (hereinafter – the action plan) represents the core document of Cyber Security Bureau (hereinafter – Bureau) for 2016-2017 on implementation and development of cyber security in Georgian Defense Sector, describing the actions, steps and methods necessary for attaining the goals set forth in the Policy. The Action Plan is based on the strategic documents of Georgia: "National Security Concept of Georgia", "Threat Assessment Document of Georgia 2010-2013", "Strategic Review of Defense 2013-2016", "Cyber Security Strategy of Georgia and the Action Plan for Implementation of Cyber Security Strategy of Georgia 2013-2015", "Minister's Vision for 2013-2014", the "National Military Strategy of Georgia" and "Minister's Vision for 2015-2016". The document should be continuously evaluated and updated due to dynamic changes and impacts in cyber space.

Article 2.

The importance of Cyber Security for state and global security is recognized by every nation. Countries that strive for technological development are responsible to the society to protect its own cyber space, provide its security and dynamic progress.

Article 3.

1. Nowadays, the world is actively using cyber space for political, geopolitical, military and other purposes. The more technologies develop, more difficult it is to overcome and prevent present and future threats. Modern cyber-attacks can reach a level that threatens the security, prosperity and stability of countries. According to the world statistics the number of successful cyber incidents rise annually and therefore, the damage caused by cyber incidents is increasing. Accordingly, global security begins with countries' own cyber defense. Cyber-attacks from Russia against Georgia in the recent years brought to light the fact that cyber space protection is as crucial as land, air and maritime space defense.
2. Cyber Security was defined as one of the essential priorities at the NATO Wales summit in September 2014, declaring cyber defense as an integral part of NATO collective defense. Georgia shares cyber security related approaches of NATO member and partner countries and recognizes

cyber security as a global challenge that lies beyond the national borders. To this end cooperation on international level is fundamental.

3. In 2013 with the support of the NATO Liaison Office in Georgia, the working group of the Ministry of Defense of Georgia (hereinafter referred to as MoD) studied the existing situation in cyber security in MoD. An Estonian expert was actively involved in the mentioned process. Cyber security core problems and challenges were identified: there were no cyber security threat/risk monitoring/management, analysis and prevention tools available in MoD. As a result of the study, the "Roadmap" was elaborated, serving as a basis for the present document.

Article 4.

1. Georgia is already taking steps so that it can bring its information systems to match the ISO 27000 series international standard. To this end, Georgia will more closely align itself with EU and NATO, who state that information security protection is an inseparable part of future.

2. Cyber Security Policy in Georgian Defense Sector is implemented by LEPL Cyber Security Bureau (hereinafter referred to as Bureau) under MoD. The accomplishment of the Bureau's responsibilities and tasks set forth by the "Law of Georgia on Information Security" will facilitate effective functioning of information and communication technology systems.

Article 5.

Action Plan is elaborated on the basis of "Cyber Security Policy" (hereinafter referred to as "The Policy") that meets cyberspace global challenges and is applicable to NATO and EU member states' principles in cyber security.

Chapter II
Terminology

Article 6.

The terms used in the action plan have the following meanings:

a) Cyber Security - Condition of the information and communication systems which gives opportunities to protect Confidentiality, Integrity, Availability, from the existing/emerging threats in cyberspace.

b) Information Security - Activity that ensures protection of confidentiality, integrity, availability, authenticity and continuous operation of information and information systems.

c) Cyberspace - Environment characterized by the use of electronic devices and electromagnetic spectrum for storage, alteration or exchange of data through the networked systems and supporting physical infrastructure.

d) Cyber Incident - Action that aims at breaking down, violating, delaying and destroying the functioning of digital information system/equipment/device or/and at unauthorized access.

e) Information System - Any combination of actions implemented by means of information technologies that support handling or/and decision making.

f) Critical Information System - Information system whose continuous operation is essential for the national defense and/or economic security, government or/and society life cycle.

g) Critical Information System Subject - State or legal entity with information systems whose continuous operation is essential for the country defense or/and economic security, government or/and society life cycle.

h) Security of Information and Communication Technologies - Protection of digital and information networks and systems, which interconnect and process or generate data within each other.

i) Infrastructure - The basic structures and systems (the body of technical devices and equipment related to administrative and organizational actions) necessary for the organizations for effective functioning.

j) Cyber Defense - Protection of one's own cyber space.

k) Cyber Threat - Cyber security incident, during which Confidentiality, Integrity and Availability of information systems are violated;

l) Cyber Crisis - Crisis, triggered by a cyber-incident, when the consequences cannot be controlled anymore and which influence components in regard to the confidentiality, integrity and availability of information.

Chapter III
Strategic Goals and Objectives

Article 7.

The goal of Cyber Security Bureau is to implement and develop stable, effective and secure information and communication technology systems for the Ministry of Defense, including Civilian Office, General Staff of Georgian Armed Forces (hereinafter General Staff) and all Legal Entities of Public Law under MoD.

Article 8.

One of the main parts of cyber security provision is to meet security norms and standards, conduct pre-testing prior to implementation of new systems and services and respond to security requirements during establishment, modernization and expansion of information technology infrastructure. To this end, the Bureau aims to elaborate security standards and norms, make consultations and support MoD in implementation of new systems and services, actively participate in consideration and realization of all planned information technology projects in the areas of responsibility.

Article 9.

Implementation and development of secure systems for information and communication technology rely on rapid identification, responsive actions, preventive measures and in case of necessity, ensure crisis management through predictive, preventive, protective and recovery methods. These actions are implemented by Computer Security Incident Response Teams (hereinafter referred to as CSIRT) and meet world recognized standards based on best practice ensuring timely identification and recovery of cyber incidents. Therefore, development and improvement of the 24/7 computer incident response mechanisms remains one of the top priorities for the Cyber Security Bureau.

Article 10.

In the process of successful implementation of plans set by the Action Plan, Bureau will be in close coordination with MoD and its subordinate units providing the right focus on strategic directions in 2016-2017 budget (professional development, awareness-raising, computer licensed programs, etc.;), effective execution and monitoring of the budget, in case of necessity, attraction of additional funds, relevant identification of logistic requirements and development of management tools, logistic activity integration with military logistic standards, improvement of procurement services.

Article 11.

1. Successful accomplishment of the goals and objectives set out in the proposed document will require:

a) Sufficient funding;

b) Execution of professional development programs;

c) Identification of the emerging threats and risks in cyberspace;

d) Maintenance of the qualified employees, and creation of HR policy

e) Growth of public awareness in the field of cyber security

f) Compliance of Georgian Legislation with international norms in cyber security

g) Coordination with governmental structures

h) Identification of critical services, creation of the list and guaranteeing their compliance with international standards

2. Accomplishment of abovementioned tasks will ensure the compliance with international standards, integration of cyber elements into military operations and establishing of robust and firm cyber security system. Thus will enable effective, stable and secure functioning of Defense sphere, which creates the solid basis for national security.

Chapter IV
Tasks for Strategic Implementation

Article 12.

Strategy and Environment

a) Objective 1 - Elaboration of conceptual documents as per to the decree on "Approval of Information Security Minimal Requirements" issued by the Defense Minister meeting global security norms and worldwide recognized standards.

a.a) Activities:

a.a.a.) Elaborate and implement Information Security Management System Policy, which describes goals, main priorities, principles, results and all necessary phases for implementation, functioning and monitoring of information security management system;

a.a.b) Define the areas of information security management system and represent organization structure, activities, assets and technologies in a documentary form;

a.a.c) Elaborate instructions and regulations on identification, description, classification, modification or destruction of material and non-material assets existing in Bureau and provide all relevant implementable procedures;

a.a.d.) Develop and implement Risk Treatment Plan describing actions, resources, responsibilities, priorities, assessment criteria for the risk effects and analysis necessary for information security risk management;

a.a.e.) Work out important policies, standards, norms and approaches.

a.b.) Outcome: Successful implementation of this objective will ensure effective management of information security risks, rapid identification, handling, monitoring, analysis and prevention of cyber incidents, efficient establishment and development of information and communication technology infrastructure for Georgian Defense Sector.

a.c.) Timelines: 2016.

a.d.) Supporters: MoD - Information Technology Department, Defense Policy and Planning Department, General Inspection.

b) Objective 2 - Establishment of Information Security Council in MoD according to the decree on "Approval of Information Security Minimal Requirements" issued by the Defense Minister.

b.a) Activities: Elaborate and approve the relevant decree.

b.b.) Outcome: Mentioned activities will support effective management of information security systems in Defense Sector of Georgia.

b.c.) Timelines: 2016.

b.d.) Supporters: MoD – Legal Support Division of the Administration.

c) Objective 3 - Conduct of research and analysis of emerging threats, risks and challenges on a regular basis in cyber space of the Georgian Defense Sector.

c.a.) Activities:

c.a.a.) Intensification of analytical research in the Bureau;

c.a.b.) Provide research and analysis of the emerging threats and risks in cyberspace;

c.a.c) Monitor and analyze current events in the sphere of information technology using open sources, development of analysis and recommendations in order to prevent the existing/emerging threats, minimize the risks and increase the information security awareness;

c.a.d.) Elaborate and carry out preventative measures on the basis of analysis;

c.b.) Outcome: Analysis of existing and emerging threats and challenges, preparation of proposals, conduction of statistics on cyber threats, risk-assessment and elaboration of relevant recommendations essential to furthering cyber security field.

c.c.) Timelines: 2016-2017.

c.d.) Supporters: General Staff of Georgian Armed Forces – Military Intelligence Department, J6 Communication and Information Systems Department, J2 Intelligence Department,
MoD - Information Technology Department, Analytical Department.

Article 13.
Operational Requirements

a) Objective 4 - Monitoring of information security management system and carrying out responsive measures against information security incidents in accordance with the decree on "Approval of Information Security Minimal Requirements" issued by the Defense Minister.

a.a.) Activities:

a.a.a.) Establish control tools and procedures, monitor and analyze its results and if needed, determine the ways for improvement, conduct periodical audit of information security system effectiveness and ensure risk assessment review;

a.a.b.) Provide audit and periodic review of information security management systems.

a.b.) Outcome: These activities will support Bureau to define relevant control tools necessary for information security system functioning, consider methods for effective management systems, depending on the monitoring results formulate plans for implementation of information security measures in the Defense Sector of Georgia.

a.c.) Timelines: 2016-2017.

a.d.) Supporters: MoD - Information Technology Department, General Inspection, General Staff of GAF – J6 Communication and Information Systems Department.

b) Objective 5 - Provision of proper functioning and enhancement of MoD information and communication technology infrastructure. Creation of additional technical capabilities in adequacy to network infrastructure development, establishment and operationalization of supplementary tools for security control, which will lead to increased demand for material, technical and human resources in the Bureau and provision of security regulations, standards and norms.

b.a.) Activities:

b.a.a.) Study the existing ICT infrastructure of MoD, provide periodic audit of information security, i.e. feasibility-study to assess security and penetration level of ICT system, identification of predictable/unpredictable vulnerabilities and gaps in information and communication technology systems, elaboration of recommendations on the basis of received information in order to increase information systems security level and modernize information technologies, development of short and long term plans for information technology and information system enhancement.

b.a.b.) Provide modern technological equipment required for meeting worldwide challenges in ICT sphere and participate in international programs/projects; integrate cyber security capabilities into military operations. Develop an action plan ensuring permanent readiness against crisis situations, work out documents on simulations for combatting emerging cyber threats and its further implementation on a regular basis. To this end, it is vital for the Bureau to provide:
- Active participation in annual military exercises organized by MoD;
- Organization and conduct of cyber exercises by the Bureau covering both technical and operational aspects as well as strategic decision-making procedures;
- Participation in international technical and cyber exercises.
- Research and assess (analyze) emerging cyber risks and threats in cyberspace of Georgian Defense Sector;
- Define the Bureau's requirements caused by infrastructure development.

b.b.) Outcome: In the 21st century a new term "Hybrid Warfare" was coined, which involve non-conventional warfare activities and operations in cyber space. Therefore, it is necessary to integrate cyber security capabilities into military operations that will enhance defense capacity, increase preparedness level of both Cyber Security Bureau and MoD against emerging threats in cyber space, create important tools for improving cyber crisis management, support strong interagency cooperation, facilitate coordinated actions between Cyber Security Bureau and MoD. Mentioned activities will mitigate the threats and risks in cyber space and ensure effective protection of Georgian Defense Sector and its further enhancement.

b.c.) Timelines: 2016-2017.

b.d.) Supporters: General Staff of GAF – J6 Communication and Information Systems Department, Military Intelligence Department, J3 Operational Planning Department, J4/8 Logistics and Resource Planning Department, J2 Intelligence Department, Army Logistic Support Command, National Guard, MoD - Information Technology Department, Analytical Department.

c) Objective 6 - Setting and implementation of relevant human resources policy and effective methods to ensure personnel professional development & capacity building; maintenance of qualified employees.

c.a.) Activities:

c.a.a.) Elaborate conceptual documents aiming at managing human resources and developing professional skills:

c.a.b.) Elaborate and approve Human Resources Management and Professional Development Concept;

c.a.c) Elaborate and approve Cyber Security Bureau Personnel Management System Development Strategy for 2016-2017;

c.a.d.) Elaborate and approve Cyber Security Bureau Gender Equality Strategy.

c.a.e.) Conduct activities aiming at improving the planning of professional development programs, selection of candidates and their efficiency assessment regulation: create a council for planning professional development programs and selecting candidates for the programs.

c.a.f.) Conduct activities for providing Bureau with qualified human resources, creating systems for work performance assessment, career planning and management:
- Elaborate system for job classification;
- Elaborate quality management and assessment system for work performance.

c.a.g.) Conduct GAP analysis in order to identify personnel knowledge, experience, skills and qualification;

c.a.h.) Provide the certified training, professional development oriented projects and educational programs that are the main components of human resources policy. For continuous professional development it is vital to involve personnel in world recognized and certified training/programs meeting cyber security requirements and providing modern approaches and technologies. Priorities for the Bureau organizational development and enhancement are:

c.a.i.) Cyber defense exercises, incident handling, research, analysis and investigation; Information security system management, audit, monitoring and preventive measures etc.;

c.a.j.) International law, administrative procedures, international relations, state procurement service, document processing and accounting, logistic support and financial resource management;

c.a.k.) Participate in local and international cyber & technical exercises, seminars, conferences and symposiums related to cyber field;

c.a.l.) Elaborate and implement methods to ensure a sustainable human resources policy: build organizational culture providing opportunity to Bureau personnel to better demonstrate their knowledge and skills; create relevant working conditions and environment; maintain qualified personnel in the Bureau; if needed, mentioned processes consider the involvement of military components into core divisions of Bureau and integration of cyber capabilities with military forces;

c.a.m.) Encourage the development of information technologies and innovations within Bureau; create various intellectual products in cyber security field; determine cyber security related terminology for the right perception of various documents to avoid any misunderstanding;

c.a.n.) Support the establishment of cyber security discipline and elaboration of educational programs in Georgian Defense Sector;

c.a.o.) Involve military contingent in preparation process to participate in NATO cyber exercises in 2016.

c.b.) Outcome: Proper management and development of human resources will facilitate in effective execution of strategic goals and objectives related to cyber security in Georgian Defense Sector. Bureau's educational policy is oriented on certified programs by world recognized institutions (NATO CCD COE, SANS, ISACA, ENISA, FIRST, etc;).

c.c.) Timelines: 2016-2017.

c.d.) Supporters: MoD - Human Resources Management and Professional Development Department, NATO Classified Information Security Service, International Relations and Euro-Atlantic Integration Department, Mass Media Relations Division, Legal Affairs and Relations with Parliament Department, GS of GAF - Training and Military Education Command, Professional Development Center (PDC) of National Defence Academy, CUBIC, Georgian MOD Representative Office to NATO, NATO Liaison Office in Georgia (NLO), NATO-Georgia Professional Development Program (PDP).

d) Objective 7 - Implementation, operationalization and development of computer security incident response 24/7 mechanisms.

d.a.) Activities:

d.a.a.) Gathering of Computer Emergency Response Team (CERT) by motivated and highly qualified IT specialists;

d.a.b.) Continuously develop Computer Incident Support Teams 24/7 capabilities and elaborate of policies, procedures and SOPs for rapid mitigation of incidents;

d.a.c.) Participate in international certification programs for professional development. The initiation covers information system auditor, information security manager, information system risks, control management and other certification programs. The mentioned certification programs will facilitate Bureau staff in acquiring world recognized information technologies audit certificates creating audit capabilities for the Bureau;

d.a.d.) Establish and strengthen close cooperation with Computer Security Incident Response Teams of NATO and European Union countries;

d.a.e.) Apply for membership in CIRT/CERT international alliance and forums;

d.a.f.) Participate in international conferences and symposiums on both international and national levels;

d.a.g.) Plan and conduct various joint projects with governmental and non-governmental sectors in the field of cyber security;

d.b.) Outcome: Such initiatives will facilitate Bureau CERTs to share experience and best practice, familiarize contemporary approaches/standards and implement them on a local level, jointly elaborate and develop security policies, procedures and strategies. This will provide secure ICT infrastructure of MoD through rapid identification of threats and risks, responsive and preventive measures and in case of necessity, ensure crisis management through predictive, preventive, protective and recovery methods.

d.c.) Timelines: 2016.

d.d.) Supporters: GS of GAF – J6 Communication and Information Systems Department,
MoD - Human Resources Management and Professional Development Department, International Relations and Euro-Atlantic Integration Department, Information Technology Department, Defense Attachés' and Civil Representative Division,
National Defense Academy (PDC), NATO Liaison Office in Georgia.

e) Objective 8 - Creation of Cyber Unit and preparation of Cyber Reserve in collaboration with the National Guard of the General Staff of the Georgian Armed Forces. The goal of the above-mentioned task is to support the development and improvement of Georgia's cyber capabilities,

which will ultimately result in the enhancement of the country's defense potential as a whole and its overall preparedness.

e.a.) Activities:

e.a.a.) Create a legal base, upon which the volunteer association will be founded;

e.a.b.) Determine the qualifications for the future recruits;

e.a.c.) Create a database for the cyber reserve;

e.a.d.) Draw out the educational program;

e.a.e.) Select the instructors;

e.a.f.) Determine the drafting procedures and period;

e.a.g.) Prepare the Cyber Reserve.

e.b.) Outcome: The cyber forces will help the active players in the cyber sphere to effectively secure the cyberspace. The aim of the Cyber Reserve is to strengthen and develop the country's cyber capabilities based entirely on free will and initiative, including:

e.b.a.) Cooperation between the public and private sectors in regard to securing the information technology infrastructure;

e.b.b.) Initiation of development operations on a permanent basis that will ensure growth and maintenance in resilience against cyber threats and cyber risks;

e.b.c.) Provision of adequate response in the times of crises, or in the states of active warfare or emergency; or out of the national security interests;

e.b.d.) Sharing the knowledge and experience in the field of cyber security;

e.b.e.) Unification of the information security specialists from public and private sectors. This type of union will create additional opportunities of merging the national security interests with those of private organizations, and will further help defend the critical infrastructure and service in peaceful and critical situations.

e.b.f.) Organization and oversight of military training programs for the volunteer information security specialists; provision of the necessary training, courses and atmosphere. They will acquire additional professional skills thanks to the education and expertise they receive.

e.c.) Timelines: 2016-2017

e.d.) Supporters: The Ministry of Defense of Georgia, the National Guard of the General Staff of the Georgian Armed Forces, J3 Operational Planning Department, Ministry of Justice – LEPL Data Exchange Agency.

Article 14.
Education, Collaboration & Outreach

a) Objective 9 - Reinforcement of institutional coordination on a local level in accordance with the decree on "Approval of Cyber Security Policy" issued by the Minister of Defense.

Joint support – interagency cooperation and active coordination between Ministries, civil and private sectors is the most significant component in cyber security. Based on the world practice none of the agencies are able to protect its own information and communication technology systems in isolation.

a.a.) Sub-activities:

a.a.a.) Ensure close cooperation with governmental structures in cyber security that will facilitate in best practice sharing, coordinated collaboration and timely information exchange on modern and emerging threats, incidents and preventative measures;

a.a.b.) Provide active collaboration with non-governmental sector, organize meetings and consultations aiming at discussing conceptual documents, modern challenges and other key issues related with cyber, elaborating/providing recommendations in this regard. The involvement of non-governmental organizations will support the raising of transparency in reference with ongoing processes.

a.a.c.) Establish and strengthen cooperation platform between public and private sectors (PPP-Public Private Partnership) will facilitate in cyber capabilities enhancement, trust raising, permanent information exchange in cyber security field.

a.b.) Outcome: The implementation of the mentioned task is of crucial importance for providing institutional framework in cyber security field.

a.c.) Timelines: 2016-2017.

a.d.) Supporters: MoD - Defense Policy and Planning Department, Mass Media Relations Division, Protocol Service. National Defense Academy (PDC).

b) Objective 10 - Participation in the elaboration process of national conceptual documents (such as Threat Assessment Document of Georgia) and other national and structural level documents in the areas of responsibility

b.a.) Sub-activities: Identify and classify threats and risks in military sphere, elaborate responsive actions, probable scenarios, events and potential analysis results.

b.b.) Outcome: Mentioned activities will address cyber challenges and prevent cyber threats in Georgian Defense Sector, ensure national security and enhance defense of the country.

b.c.) Timelines: 2016-2017.

b.d.) Supporters: GS of GAF – J6 Communication and Information Systems Department, Military Intelligence Department, J2 Intelligence Department, MoD - Information Technology Department, Analytical Department.

c) Objective 11 - Provision of awareness-building as per to the decrees on "Approval of Information Security Minimal Requirements" and "Approval of Cyber Security Policy" issued by the Defense Minister of Georgia. The implementation and enhancement of "Cyber Security Culture" is one of the strategic components of cyber security provision that implies awareness-raising in the field of cyber security. Cyber security is a rather new term in the world both for citizens and academia. Raising awareness in cyber security will facilitate society in better perceiving the importance and the role of cyber security, understanding the possible outcomes caused by cyber attacks.

c.a.) Sub-activities: Organize and conduct information days, seminars and conferences, develop and implement educational programs on a regular basis for the personnel of General Staff, civilian part of MoD, its subordinate units, students of universities accredited in Georgia, special target audience;

c.b.) Outcome: Activities in this direction will facilitate each constituent in avoiding the minimal risks, getting familiar with updated information on computer, mobile and other communication devices, studying e-mail safety rules, etc.; getting information on the tools necessary for secure functioning of the devices. Promotion of awareness-raising in cyber security will create a solid basis for close and coordinated cooperation among Bureau and other structures.

c.c.) Timelines: 2016-2017.

c.d.) Supporters: MoD - Human Resources Management and Professional Development Department, Mass Media Relations Division, Information Technology Department, Strategic Commutation Department, GS of GAF - Training and Military Education Command, J6 Communication and Information Systems Department, Professional Development Center (PDC) of National Defense Academy, NATO Liaison Office in Georgia (NLO), NATO-Georgia Professional Development Program (PDP).

d) Objective 12 - Harmonization of Georgian Legislation with international legal norms in accordance with the decree on "Approval of Cyber Security Policy" issued by the Minister of Defense.

d.a.) Activities:

d.a.a.) Comply the Legislation of Georgia with international regulations and standards;

d.a.b.) Elaborate appropriate normative acts in information technology field;

d.a.c.) Formulate specialized legislation through legal regulations, laws and by-laws in cyber security field;

d.a.d.) Elaborate and issue the instructions and guidelines necessary for identification, description, classification, modification and destruction of assets in accordance with the rules set by the Legislation;

d.a.e.) Ensure legal support to Computer Incident Support Teams by preparing relative documentation and providing legal consultation within its competence;

d.a.f.) Provide legal support for 24/7 consultation;

d.a.g.) Meet the terms foreseen by the article 35 set in European Council Convention – establishment and operationalization of Call Center 24/7 in the field of cyber security for Georgian Defense Sector.

d.b.) Outcome: Improvement of legislative framework in the field of cyber security will develop and enhance solid legal grounds for effective formation of cyber security system in the Defense Sector, enable countries to work jointly for achieving certain goals and making decisions in cyber sphere.

d.c.) Timelines: 2016-2017.

d.d.) Supporters: MoD - Legal Affairs and Relations with Parliament Department, Defense Policy and Planning Department, Legal Support Division.

e) Objective 13 - Development and bolstering of international cooperation in cyber security.

e.a.) Sub-activities:

e.a.a.) Strengthen international mechanisms, develop bilateral and multilateral relations in cyber security field with cyber divisions of NATO and EU countries;

e.a.b.) Establish and develop cooperation with sub-structures of international organizations in cyber and take part in the educational programs, trainings, cyber exercises, seminars and conferences (EU-ENISA, NATO-CCD COE, OSCE, etc.);

e.a.c.) Enhance cooperation with the main strategic partner – USA in cyber security field in the framework of strategic partnership;

e.a.d.) Participate in Annual National Program (ANP) and Plan and Review Process Program (PARP) within the framework of NATO-Georgia Cooperation;

e.a.e.) Establish close collaboration with Defense attaches accredited to Georgia and Georgian Defense attaches accredited in different countries in the direction of cyber security;

e.a.f.) Create and enhance regional cooperation format in cyber sphere.

e.b.) Outcome: Successful implementation of the mentioned tasks will facilitate Bureau in: creation the possibilities for taking part into educational programs, trainings, international cyber exercises; changing information on modern and potential threats, new incidents and their prevention measures; sharing best practice and experience, getting familiar with world recognized standards and implementing them on a local level in cyber security field. International cooperation will increase capabilities to create, develop and operate robust and secure system for ICT in the Defense Sector.

e.c.) Timelines: 2016-2017.

e.d.) Supporters: MoD - International Relations and Euro-Atlantic Integration Department, NATO Classified Information Security Service, Defense Attachés' and Civil Representative Division, GS of GAF - Training and Military Education Command, Professional Development Center (PDC of National Defense Academy, CUBIC, Georgian MOD Representative Office to NATO, Georgian Mission to EU, NATO-Liaison Office in Georgia (NLO).

Chapter V
Conclusion

Article 15.

1. The proposed document reviews objectives that differ, but at the same time are closely related to each other and jointly provide resilient, effective and secure systems for ICT in the Defence Sector.

2. In the document elaboration process Cyber Security Bureau worked in close coordination with the Ministry of Defense of Georgia and foreign partners in the field of cyber security.

3. The timelines for goals implementation set by the Action Plan are defined as 2016-2017. Step-by-step realization of the Action Plan will enhance defence capabilities of the country and protect ICT systems from cyber threats/risks, which could harm state security.

4. Cyber Security Bureau bearing the responsibility to fulfill Cyber Security Development Action Plan will provide effective and reliable infrastructure for Georgian Defense Sector and by doing so will greatly contribute to our country's integration process with European and Euro-Atlantic structures.