საქართველოს პრეზიდენტის

ბრძანებულება №321

2013 წლის 17 მაისი

ქ. თბილისი

საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013–2015 წწ. სამოქმედო გეგმის დამტკიცების შესახებ

1. დამტკიცდეს თანდართული „საქართველოს კიბერუსაფრთხოების სტრატეგია“ (დანართი №1).
2. დამტკიცდეს თანდართული „საქართველოს კიბერუსაფრთხოების 2013–2015 წწ. სტრატეგიის სამოქმედო გეგმა“ (დანართი №2).
3. ეს ბრძანებულება ამოქმედდეს გამოქვეყნებისთანავე.

საქართველოს პრეზიდენტი მიხეილ სააკაშვილი

დანართი №1

საქართველოს კიბერუსაფრთხოების

სტრატეგია

1. შესავალი

საქართველოს ხელისუფლება პირველად აქვეყნებს საქართველოს კიბერუსაფრთხოების სტრატეგიას. 2008 წლის აგვისტოში რუსეთის ფედერაციის მიერ საქართველოს წინააღმდეგ განხორციელებულმა ფართომასშტაბიანმა კიბერშეტევებმა ნათლად აჩვენა, რომ საქართველოს ეროვნული უსაფრთხოება ვერ შედგება კიბერსივრცის უსაფრთხოების უზრუნველყოფის გარეშე.

რუსეთ-საქართველოს ომის დროს, რუსეთის ფედერაციამ საქართველოს წინააღმდეგ სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, განახორციელა მიზანმიმართული და მასირებული კიბერშეტევები. აღნიშნულმა კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საზღვაო და საჰაერო სივრცეების დაცვა.

საქართველოს კიბერუსაფრთხოების სტრატეგია არის კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი, რომელიც ასახავს სტრატეგიულ მიზნებს, ძირითად პრინციპებს, აყალიბებს სამოქმედო გეგმებს და ამოცანებს. სტრატეგიაზე დაყრდნობით, საქართველოს ხელისუფლება გაატარებს ღონისძიებებს, რომლებიც ხელს შეუწყობს სახელმწიფო ორგანოების, კერძო სექტორისა და სამოქალაქო საზოგადოების კიბერსივრცეში დაცულად ფუნქციონირებას, ელექტრონული ოპერაციების უსაფრთხოდ განხორციელებას და ქვეყანაში ეკონომიკისა და ბიზნესის შეუფერხებლად მოქმედებას.

საქართველოს კიბერუსაფრთხოების სტრატეგია წარმოადგენს ,,ეროვნული უსაფრთხოების მიმოხილვის'' პროცესის ფარგლებში შექმნილი კონცეპტუალური და სტრატეგიული დოკუმენტების პაკეტის ნაწილს. შესაბამისად, აღნიშნული სტრატეგია ეფუძნება ,,საქართველოს საფრთხეების შეფასების 2010-2013 წ.წ. დოკუმენტს'' და ,,საქართველოს ეროვნული უსაფრთხოების კონცეფციას''.

წინამდებარე სტრატეგია შემუშავდა საქართველოს ეროვნული უშიშროების საბჭოსთან არსებული ეროვნული უსაფრთხოების სტრატეგიული დოკუმენტების შემუშავების მაკოორდინირებელი მუდმივმოქმედი საუწყებათაშორისო კომისიის მიერ.

2. საქართველოს კიბერუსაფრთხოების პოლიტიკის განხორციელების

ძირითადი პრინციპები

საქართველოს ეროვნული უსაფრთხოების კონცეფცია კიბერუსაფრთხოების უზრუნველყოფას განსაზღვრავს, როგორც უსაფრთხოების პოლიტიკის ერთ-ერთ მნიშვნელოვან მიმართულებას. საქართველოს მიზანია შექმნას კიბერ-უსაფრთხოების ისეთი სისტემა, რომელიც ხელს შეუწყობს, ერთი მხრივ, ინფორმაციული ინფრასტრუქტურის დაცულობას კიბერსაფრთხეების წინაშე და, მეორე მხრივ, იქნება დამატებითი ფაქტორი ქვეყნის შემდგომი ეკონომიკური და სოციალური განვითარებისათვის. ამ მიზნის მიღწევისათვის მნიშვნელოვანია თანამშრომლობის შემდეგი პრინციპების განხორციელება:

- **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. გამომდინარე აქედან, მნიშვნელოვანია თანამშრომლობის მექანიზმის შემუშავება, რომელიც ხელს შეუწყობს, ერთი მხრივ, კრიტიკული ინფორმაციული ინფრასტრუქტურის გამართულად მუშაობას, მათ შორის, კრიზისების დროს და, მეორე მხრივ, დამატებითი მასტიმულირებელი ფაქტორი იქნება ეკონომიკური განვითარებისათვის.
- **აქტიური საერთაშორისო თანამშრომლობა.** საქართველოს მთავრობა აცნობიერებს, რომ არც ერთ მთავრობას მსოფლიოში არ შეუძლია 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.
- **ინდივიდუალური პასუხისმგებლობა.** თითოეული მოქალაქე, საწარმო თუ საჯარო დაწესებულება ვალდებულია ინდივიდუალურად უზრუნველყოს მის მფლობელობასა და განკარგულებაში არსებული ინფორმაციული სისტემების უსაფრთხოება. აღნიშნული სისტემების მფლობელებმა და უშუალოდ მომხმარებლებმა უნდა მიიღონ ყველა საჭირო ზომა მათი უსაფრთხო ფუნქციონირების უზრუნველსაყოფად.

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

3. კიბერსაფრთხეები და გამოწვევები

საქართველოს მიზანია შექმნას ინფორმაციული უსაფრთხოების ისეთი სისტემა, რომლის დროსაც ნებისმიერი კიბერშეტევის საზიანო შედეგები მინიმუმამდე იქნება შემცირებული და ასეთი შეტევის შემდეგ უმოკლეს დროში გახდება შესაძლებელი ინფორმაციული ინფრასტრუქტურის ფუნქციონირების სრული აღდგენა. ამასთან, ინფორმაციული უსაფრთხოების ერთიანი სისტემის შექმნის მიზანია კრიტიკული ინფორმაციული სისტემების მდგრადობის ამაღლება კიბერშეტევებისადმი და ეფექტიანი ღონისძიებების გატარება პოტენციური კიბერშეტევების პრევენციის მიზნით.

ელექტრონული მმართველობის პრინციპის დამკვიდრებასთან ერთად იზრდება საქართველოს კრიტიკული ინფორმაციული ინფრასტურქტურის წინაშე არსებული საფრთხეები და გამოწვევები. ამასთან,

ინფორმაციული სისტემის კრიტიკულობისა და კიბერუსაფრთხოებისადმი მდგრადობა განისაზღვრება ისეთი კრიტერიუმებით, როგორიცაა მოსალოდნელი მატერიალური ზარალის სიმძიმე და მასშტაბი, ინფორმაციული სისტემის აუცილებლობა სახელმწიფოსა და საზოგადოების ნორმალური ფუნქციონირებისათვის, სისტემის მომხმარებელთა რაოდენობა და კიბერუსაფრთხოების სათანადო დონის უზრუნველსაყოფად საჭირო რესურსები.

საქართველო დგას იმ საერთაშორისო საფრთხეების და გამოწვევების წინაშე, რომელიც ემუქრება მთლიანად დემოკრატიულ საზოგადოებას საერთაშორისო სისტემაში. გამომდინარე აქედან, საქართველოს უსაფრთხოების პოლიტიკის დაგეგმვისა და განხორციელებისას მნიშნელოვანი ყურადღება ექცევა კიბერ-უსაფრთხოების სფეროში შემდეგ საფრთხეებს და გამოწვევებს:

- **კიბერომი.** 2008 წელს რუსეთის ფედერაციამ საქართველოს წინააღმდეგ აგრესია, სამხედრო თავდასხმის პარალელურად, კიბერსივრცეშიც განახორციელა. საქართველოს პოტენციური მოწინააღმდეგეები ფლობენ კიბერსივრცეში ახალი ომის წარმოების დიდ შესაძლებლობებს. ამასთან, საქართველო კვლავ დგას მასიური კიბერშეტევის რისკის წინაშე.
- **კიბერტერორიზმი.** კრიტიკულ ინფორმაციულ ინფრასტრუქტურაზე, საქართველოს სახელმწიფო მართვის და ბიზნესის მნიშვნელოვანი სფეროების მზარდ დამოკიდებულებასთან ერთად იზრდება კიბერ ტერორიზმის საფრთხეები. კიბერსივრცეში განხორციელებულმა შეტევებმა კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტებზე შეიძლება მნიშნელოვანი ზიანი მიაყენოს ქვეყნის უსაფრთხოებას.
- **კიბერსივრცის გამოყენებით ჩადენილი სხვა ქმედებები.** საქართველოს უსაფრთხოების გამოწვევაა კიბერსივრცის გამოყენებით ჩადენილი დანაშაულის ის სახეები, რომელიც მიმართულია საქართველოს კრიტიკული ინფორმაციული სისტემების წინააღმდეგ.

4. საქართველოს კიბერუსაფრთხოების პოლიტიკის

ძირითადი მიმართულებები

საქართველოს კიბერუსაფრთხოების პოლიტიკის ძირითადი მიმართულებებია:

- კვლევა და ანალიზი;
- ახალი საკანონმდებლო-ნორმატიული ბაზა;
- კიბერუსაფრთხოების უზრუნველყოფის ინსტიტუციური კოორდინაცია;
- საზოგადოებრივი ცნობიერების ამაღლება და საგანმანათლებლო ბაზის ჩამოყალიბება;
- საერთაშორისო თანამშრომლობა.

4. კვლევა და ანალიზი

მნიშვნელოვანია, რომ კიბერუსაფრთხოების სფეროში საქართველოს მიერ შემუშავებული საკანონმდებლო ინიციატივები, კანონქვემდებარე აქტები, ინსტრუქციები, რეკომენდაციები და განხორციელებული ქმედებები ემყარებოდეს კვლევასა და ანალიზს, რომელიც კიბერუსაფრთხოების პოლიტიკის ეფექტიანობას უზრუნველყოფს, ასევე ითვალისწინებს 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.

ამ მიზნით, კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განხორციელებისათვის აუცილებელია კვლევა და ანალიზი შემდეგი მიმართულებებით:

- 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.

4.2. ახალი საკანონმდებლო-ნორმატიული ბაზა

2012 წლის მდგომარეობით, საქართველოს არ გააჩნია სპეციალიზებული ეროვნული კანონმდებლობა კიბერუსაფრთხოების სფეროში. მნიშვნელოვანია კიბერუსაფრთხოების სფეროში საკანონმდებლო ბაზის ფორმირება, რაც ხელს შეუწყობს კიბერუსაფრთხოების დაცვის ქმედითი და ეფექტიანი მექანიზმების შექმნას.

კიბერუსაფრთხოების სფეროში სამართლებრივი ბაზის სრულყოფისათვის აუცილებელია შემდეგი ღონისძიებების გატარება:

- ინფორმაციული უსაფრთხოების შესახებ საკანონმდებლო აქტების ინიციირება;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის განმსაზღვრელი და მისი კიბერუსაფრთხოების უზრუნველმყოფი ნორმატიული ბაზის შექმნა;
- კომპიუტერულ ინცინდენტებზე დახმარების ჯგუფის ფუნქციონირების სამართლებრივი უზრუნველყოფა;
- ევროპის საბჭოს 2001 წლის ,,კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირების შედეგად აღებული ვალდებულებების შესრულება;
- იმ ორგანოს ან ორგანოთა საკანონმდებლო დონეზე იდენტიფიცირება, რომელთა უფლებამოსილებაში შევა ინფორმაციული უსაფრთხოების პოლიტიკის განსაზღვრა და მაკოორდინირებელი ფუნქციის განხორციელება;
- კიბერუსაფრთხოებასთან დაკავშირებული კრიზისული სიტუაციების დროს მოქმედების სარეზერვო გეგმების და პროცედურების გაწერა.

4.3. ინსტიტუციური კოორდინაცია კიბერუსაფრთხოების უზრუნველყოფის სფეროში

კიბერუსაფრთხოების უზრუნველსაყოფად მნიშვნელოვანია აღნიშნულ სფეროში სახელმწიფო უწყებების ფუნქციების მკაფიო განსაზღვრა, საქართველოს მთავრობის ერთიანი მიდგომის განხორციელებისათვის უწყებათაშორისი საკოორდინაციო მექანიზმის შექმნა და სახელმწიფო და კერძო სექტორებს შორის თანამშრომლობა.

კიბერუსაფრთხოების სფეროში კოორდინაციის უზრუნველყოფისათვის აუცილებელია შემდეგი ღონისძიებების გატარება:

- კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შემდგომი განვითარება;
- მაღალტექნოლოგიური დანაშაულის (კიბერდანაშაული) საერთაშორისო საკონტაქტო პუნქტის 24/7 შემდგომი განვითარება;
- კიბერდანაშაულის საქმეებზე საექსპერტო დახმარების ჯგუფის (დანაყოფი) განსაზღვრა;
- სახელმწიფო და კერძო სექტორებს შორის თანამშრომლობის ფორმატისა და მექანიზმების ჩამოყალიბება.

4.4. საზოგადოებრივი ცნობიერების ამაღლება და საგანმანათლებლო ბაზის ჩამოყალიბება

საქართველოს კიბერუსაფრთხოების სტრატეგიის მნიშვნელოვან ნაწილს ამ სფეროში საზოგადოებრივი ცნობიერების და შესაბამისი სპეციალისტების პროფესიული დონის ამაღლება წარმოადგენს.

ამ მიზნით მნიშვნელოვანია შემდეგი ღონისძიებების გატარება:

- კიბერუსაფრთხოების სფეროში საზოგადოებრივი ცნობიერების ამაღლებისა

და საგანმანათლებლო პროგრამების შექმნა;

- კრიტიკული ინფორმაციული ინფრასტრუქტურის სუბიექტების და სხვა

  დაინტერესებული ორგანიზაციების კადრებისა და ტექნიკური პერსონალის

  გადამზადება ინფორმაციული უსაფრთხოების საერთაშორისო და ეროვნული

  სტანდარტების შესწავლისათვის;

- კიბერდანაშაულის ექსპერტების სპეციალიზებული ტრენინგები ელექტრონული მტკიცებულებების (კიბერკრიმინალისტიკის) დარგში;
- კიბერუსაფრთხოების სფეროში სამეცნიერო-კვლევითი პროექტების ხელშეწყობა;
- კვლევითი ლაბორატორიის შექმნა.

4.5. საერთაშორისო თანამშრომლობა

კიბერუსაფრთხოების უზრუნველყოფის მიზნით საერთაშორისო თანამშრომლობის განვითარებისათვის საქართველო ატარებს შემდეგ ღონისძიებებს:

- კიბერუსაფრთხოების საკითხებზე საერთაშორისო ურთიერთობების განმტკიცება ამ სფეროში მომუშავე საერთაშორისო ორგანიზაციებთან (OECD, EU, OSCE, NATO, CoE, UN, ITU) 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.

5. სტრატეგიის განხორციელების მექანიზმები და ვადები

სტრატეგიის განხორციელების ვადებია 2013-2015 წლები. სტრატეგიის შესრულებაზე პასუხისმგებელი უწყებები შესაბამის სფეროში პოლიტიკის განხორციელებისას ითვალისწინებენ ამ სტრატეგიის მოთხოვნების შესრულებისათვის საჭირო ღონისძიებებებს.

სტრატეგიის შესრულების შედეგები ყოველწლიურად შეფასდება და შეფასების ყოველწლიური ანგარიში წარედგინება საქართველოს ეროვნული უშიშროების საბჭოსთან არსებულ ეროვნული უსაფრთხოების სტრატეგიული დოკუმენტების შემუშავების მაკოორდინირებელ მუდმივმოქმედ საუწყებათა-შორისო კომისიას.

დანართი №2

საქართველოს კიბერუსაფრთხოების სტრატეგიის 2013–2015 წწ. განხორციელების სამოქმედო გეგმა

№	მიზანი	საქმიანობა	პერიოდი	პასუხისმგებელი უწყება
1	კვლევა და ანალიზი			
1.1		სხვა ქვეყნების საუკეთესო პრაქტიკის შესწავლა და გამოცდილების გაზიარება; შესაბამისი მოხსენების მომზადება.	2013	საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო
		კრიტიკული ინფორმაციული სისტემების სუბიექტების		საქართველოს შინაგან საქმეთა სამინისტრო, საჯარო

1.2		იდენტიფიცირების კრიტერიუმების და სტანდარტების კვლევა; შესაბამისი მოხსენების მომზადება.	2013	სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო
1.3		კრიტიკული ინფორმაციული სისტემების მდგრადობის ანალიზი; შესაბამისი მოხსენების მომზადება.	2013	საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო
1.4		კიბერუსაფრთხოების სფეროში რეგიონში არსებული პრობლემატიკის შესწავლა; შესაბამისი მოხსენების მომზადება.	2013	საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო
1.5		კიბერუსაფრთხოების განმსაზღვრელი სტანდარტების შემუშავება მათი შემდგომი დანერგვის მიზნით.	2014	საქართველოს შინაგან საქმეთა სამინისტრო, საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო
1.6		საქართველოს კიბერსივრცის წინაშე მდგარი საფრთხეების და რისკების გამოვლენაზე წინადადებების პერიოდულად მომზადება.	2013-2015	საქართველოს შინაგან საქმეთა სამინისტრო, საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო
2	**ახალი საკანონმდებლო ბაზა**			
2.1		ინფორმაციული უსაფრთხოების შესახებ საკანონმდებლო აქტების ინიციირება.	2013	საქართველოს იუსტიციის სამინისტრო
2.2		კრიტიკული ინფორმაციული სისტემების განმსაზღვრელი და მისი კიბერუსაფრთხოების უზრუნველმყოფი ნორმატიული ბაზის შექმნა.	2013	საქართველოს იუსტიციის სამინისტრო

2.3		კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფის ფუნქციონირების სამართლებრივი უზრუნველყოფა.	2013	საქართველოს იუსტიციის სამინისტრო
2.4		ევროპის საბჭოს 2001 წლის ,,კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირების შედეგად აღებული ვალდებულებების შესრულება.	2013	საქართველოს შინაგან საქმეთა სამინისტრო
2.5		იმ ორგანოს ან ორგანოთა საკანონმდებლო დონეზე იდენტიფიცირება, რომელთა უფლებამოსილებაში შევა ინფორმაციული უსაფრთხოების პოლიტიკის განსაზღვრა და მაკოორდინირებელი ფუნქციის განხორციელება.	2013	საქართველოს იუსტიციის სამინისტრო
2.6		კიბერუსაფრთხოებასთან დაკავშირებული კრიზისული სიტუაციების დროს მოქმედების სარეზერვო გეგმების და პროცედურების გაწერა.	2013-2015	საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო
3	**კიბერუსაფრთხოების სფეროში კოორდინაციის უზრუნველყოფა**			
3.1		კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფის შემდგომი განვითარება.	2013-2015	საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო
3.2		მაღალტექნოლოგიური დანაშაულის (კიბერდანაშაული) საერთაშორისო საკონტაქტო პუნქტის 24/7 შემდგომი განვითარება.	2013-2015	საქართველოს შინაგან საქმეთა სამინისტრო
3.3		კიბერდანაშაულის საქმეებზე საექსპერტო დახმარების ჯგუფის (დანაყოფი) განსაზღვრა.	2013	საქართველოს შინაგან საქმეთა სამინისტრო
3.4		სახელმწიფო და კერძო სექტორებს შორის თანამშრომლობის ფორმატისა და მექანიზმების ჩამოყალიბება.	2013-2014	საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო
	საზოგადოებრივი ცნობიერების ამაღლება			

4	**და საგანმა ნათლებლო ბაზის ჩამოყალიბება**			
4.1		კიბერუსაფრთხოების სფეროში საზოგადოებრივი ცნობიერების ამაღლებისა და საგანმანათლებლო პროგრამების შექმნა.	2013-2015	საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო, საერთა-შორისო დახმარება
4.2		კრიტიკული ინფორმაციული სისტემების სუბიექტების და სხვა დაინტერესებული ორგანიზაციების კადრებისა და ტექნიკური პერსონალის გადამზადება ინფორმაციული უსაფრთხოების საერთაშორისო და ეროვნული სტანდარტების შესწავლისათვის.	2013-2015	საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო, საერთაშორისო დახმარება
4.3		კიბერდანაშაულის ექსპერტების სპეციალიზებული ტრენინგები ელექტრონული მტკიცებულებების (კიბერკრიმინალისტიკის) დარგში.	2013-2015	საერთაშორისო დახმარება
4.4		კვლევითი ლაბორატორიის შექმნა.	2014-2015	საერთაშორისო დახმარება
5	**საერთაშორისო თანამშრომლობა**			
5.1		კიბერუსაფრთხოების საკითხებზე საერთაშორისო ურთიერთობების განმტკიცება ამ სფეროში მომუშავე საერთაშორისო ორგანიზაციებთან (OECD, EU, OSCE, NATO, CoE, UN, ITU) და სახელმწიფო ორგანოებთან.	2013-2015	საქართველოს საგარეო საქმეთა სამინისტრო, საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო, საქართველოს ეროვნული უშიშროების საბჭოს აპარატი, საქართველოს შინაგან საქმეთა სამინისტრო
				საქართველოს საგარეო საქმეთა სამინისტრო, საჯარო

5.2		კიბერუსაფრთხოების სფეროში საერთაშორისო ინიციატივებში აქტიური მონაწილეობის მიღება და ამ ინიციატივების რეგიონის მასშტაბით მხარდაჭერა.	2013-2015	სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო, საქართველოს ეროვნული უშიშროების საბჭოს აპარატი, საქართველოს შინაგან საქმეთა სამინისტრო
5.3		სხვა ქვეყნების CERT-ებთან კიბერუსაფრთხოების სფეროში ორმხრივ და მრავალმხრივ ფორმატებში თანამშრომლობის ინიციირება.	2013-2015	საჯარო სამართლის იური-დიული პირი - მონაცემთა გაცვლის სააგენტო, საქარ-თველოს CERT