საქართველოს მთავრობის

დადგენილება №482

2021 წლის 30 სექტემბერი

ქ. თბილისი

საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ

მუხლი 1
„საქართველოს მთავრობის სტრუქტურის, უფლებამოსილებისა და საქმიანობის წესის შესახებ“ საქართველოს კანონის მე-6 მუხლის გათვალისწინებითა და „ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ“ საქართველოს კანონის მე-15 მუხლის მე-4 პუნქტის შესაბამისად, დამტკიცდეს თანდართული საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგია (დანართი №1) და მისი სამოქმედო გეგმა (დანართი №2).

მუხლი 2
დადგენილება ამოქმედდეს გამოქვეყნებისთანავე.

პრემიერ-მინისტრი ირაკლი ღარიბაშვილი

დანართი №1

საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგია
სარჩევი

მიზანი 1: ინფორმაციული საზოგადოებისა და ორგანიზაციების კიბერკულტურის განვითარება და შესაძლებლობების გაძლიერება კიბერსივრცეში საფრთხეებსა და ინციდენტებთან გამკლავების მიზნით.

ამოცანა 1.1: კიბერსივრცეში უსაფრთხოდ და დაცულად ფუნქციონირებისთვის სკოლის მოსწავლეებისა და სტუდენტებისთვის საჭირო უნარ-ჩვევების განვითარება და განათლების დონის ამაღლება.

ამოცანა 1.2: კიბერსივრცეში უსაფრთხოდ და დაცულად ფუნქციონირებისთვის კიბერსაფრთხეებისა და რისკების შესახებ ინფორმაციული საზოგადოებისა და ორგანიზაციების ცნობიერების ამაღლება.

მიზანი 2: კიბერუსაფრთხოების მმართველობითი სისტემის მდგრადობა და საჯარო-კერძო თანამშრომლობის გაძლიერება.

ამოცანა 2.1: ეროვნულ დონეზე კიბერინციდენტებისა და კიბერსაფრთხეების დროული გამოვლენის, რეპორტინგისა და მათთან ეფექტიანი გამკლავების სისტემის შექმნა და განვითარება.

ამოცანა 2.2: კიბერდანაშაულის წინააღმდეგ ბრძოლის ეფექტიანი სისტემის განვითარება.

ამოცანა 2.3: ჩამოყალიბებული საკომუნიკაციო პლატფორმების გამოყენებით თანამედროვე ტენდენციების, საუკეთესო პრაქტიკისა და კიბერსაფრთხეების შესახებ ინფორმაციის გაცვლა და საერთაშორისო სტანდარტების დანერგვის ხელშეწყობა.

ამოცანა 2.4: ეროვნული კიბერუსაფრთხოების მიზნების განსაზღვრა.

ამოცანა 2.5: კიბერუსაფრთხოების სფეროში კვლევითი საქმიანობის მხარდაჭერა და გაძლიერება.

მიზანი 3: კიბერშესაძლებლობების განვითარება ძლიერი ადამიანური რესურსითა და სათანადო ტექნიკური უზრუნველყოფის საშუალებებით.

ამოცანა 3.1: დარგის სპეციალისტების ცოდნისა და კვალიფიკაციის ამაღლება.

ამოცანა 3.2: ეროვნული კიბერშესაძლებლობების გაძლიერება ტექნიკური უზრუნველყოფის საშუალებებით.

მიზანი 4: კიბერუსაფრთხოების საერთაშორისო ასპარეზზე საქართველოს, როგორც უსაფრთხო და დაცული ქვეყნის როლის გაძლიერება.

ამოცანა 4.1 კიბერსაფრთხეებსა და ინციდენტებთან დაკავშირებულ ინფორმაციაზე წვდომის ზრდა და საერთაშორისო მხარდაჭერის/თანამშრომლობის გაძლიერება.

ამოცანა 4.2 საერთაშორისო კიბერსწავლებებსა და კიბერსავარჯიშოებში ჩართულობის უზრუნველყოფა და ცოდნისა და გამოცდილების გაზიარება კიბერუსაფრთხოების გლობალურ დღის წესრიგში წვლილის შეტანისთვის.

ამოცანა 4.3 საერთაშორისო ორმხრივი და მრავალმხრივი ფორმატის პარტნიორობის გაძლიერება.

განხორციელება.

მონიტორინგი და შეფასება.

მონიტორინგი.

შეფასება.

შესავალი

საქართველო მესამედ აქვეყნებს კიბერუსაფრთხოების სფეროში ეროვნულ სტრატეგიას და ამგვარად აგრძელებს უწყვეტ ციკლს, რაც გამოიხატება ქვეყნის ურყევი პოზიციით, დაიცვას და გააძლიეროს კიბერსივრცე, როგორც ეროვნული უსაფრთხოების შემადგენელი ნაწილი.

საქართველოს პრეზიდენტის 2013 წლის 17 მაისის №321 ბრძანებულებით დამტკიცებული „საქართველოს კიბერუსაფრთხოების სტრატეგია და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013-2015 წწ. სამოქმედო გეგმა“, ასევე, საქართველოს მთავრობის 2017 წლის 13 იანვრის №14 დადგენილებით დამტკიცებული „საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგია და მისი სამოქმედო გეგმა“ ნათლად წარმოაჩენს ქვეყნის სისტემურ პოლიტიკას ეროვნულ დონეზე კიბერუსაფრთხოების განვითარების საკითხთან მიმართებით.

ამდენად, რიგით მესამე სტრატეგია ასახავს წინა სტრატეგიების მიღების შემდეგ ქვეყნის კიბერუსაფრთხოების გარემოში მომხდარ ცვლილებებს და უახლოესი 3 წლის განმავლობაში აყალიბებს ქვეყნის უსაფრთხო განვითარების ხედვას, განსაზღვრავს მის წინაშე არსებულ საფრთხეებსა და გამოწვევებთან გამკლავების ეფექტიან მექანიზმებს.

სტრატეგია, როგორც კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი, წარმოადგენს სტრატეგიული მიზნებისა და ამოცანების ერთობლიობას და მათ შესასრულებლად ითვალისწინებს კონკრეტულ აქტივობებს, რესურსებსა და პასუხისმგებელ უწყებებს. სტრატეგიით გათვალისწინებული აქტივობების შესრულებით, საქართველოს კიბერსივრცე გახდება მეტად დაცული, კიდევ უფრო მეტად განვითარდება ინფორმაციული საზოგადოება და ელექტრონული მომსახურების მიწოდებისთვის შეიქმნება სანდო გარემო. ეს ყოველივე, ცხადია, წარმოადგენს ქვეყნის შეუფერხებელი ფუნქციონირების, მისი ეროვნული უსაფრთხოების, თავდაცვისუნარიანობის უზრუნველყოფისა და ეკონომიკური განვითარების ერთ-ერთ მთავარ ფაქტორს.

მოცემული სტრატეგია წარმოადგენს სახელმწიფოს 3-წლიან გეგმას, თუ როგორ გახდეს საქართველო კიბერსივრცეში ძლიერი, დაცული და უსაფრთხო ქვეყანა. კერძოდ, ინფორმაციული საზოგადოების ყველა სამიზნე ჯგუფს აქვს კიბერსაფრთხეებთან გამკლავების მინიმალური ცოდნა და გამოცდილება, საქართველოში არსებული მმართველობითი მოდელი იძლევა შესაძლებლობას, რესურსების გაზიარებით, საჯარო და კერძო სექტორებმა როგორც ერთობლივად, ისე დამოუკიდებლად შეძლონ ქვეყნის კიბერუსაფრთხოებისა და მდგრადობის უზრუნველყოფა. გარდა ამისა, საქართველო, როგორც კიბერუსაფრთხოების სფეროში სანდო პარტნიორი, მოიპოვებს საერთაშორისო აღიარებასა და მხარდაჭერას ევროპული და ევროატლანტიკური სტრუქტურებისგან.

სტრატეგია და სამოქმედო გეგმა შემუშავდა როგორც საჯარო სექტორში არსებული უწყებების, ისე კერძო სექტორის (აკადემიური სექტორი, არასამთავრობო ორგანიზაციები, ბიზნესის წარმომადგენლები) წარმომადგენელთა აქტიური ჩართულობით, ევროპული საუკეთესო პრაქტიკისა და ადგილობრივი ექსპერტიზის გათვალისწინებით და ამ მხრივ წარმოადგენს საჯარო-კერძო პარტნიორობის პრაქტიკაში განხორციელების ნათელ მაგალითს. სტრატეგიის შემუშავების პროცესში საქართველოს მთავრობამ გაითვალისწინა პარტნიორი სახელმწიფოების რჩევები და რეკომენდაციები, საუკეთესო საერთაშორისო პრაქტიკა და გამოცდილება.

ეროვნული უსაფრთხოების საბჭოს აპარატის მიერ განხორციელდა სტრატეგიის პროექტის, როგორც ეროვნული დონის კონცეპტუალური დოკუმენტის შემუშავების პროცესის ორგანიზება და კოორდინაცია.

წინამდებარე სტრატეგია ეფუძნება საქართველოს კონსტიტუციას და შესაბამის კანონმდებლობას, ასევე, საქართველოს მიერ ნაკისრ საერთაშორისო ვალდებულებებს, საერთაშორისო შეთანხმებებსა და ხელშეკრულებებს. ამასთან, სტრატეგია ხელმძღვანელობს უსაფრთხოების სფეროში ეროვნული დონის ფუნდამენტური კონცეპტუალური დოკუმენტებით, როგორიცაა საქართველოს ეროვნული უსაფრთხოების კონცეფცია და საქართველოს საფრთხეების შეფასების დოკუმენტი. საქართველოს ეროვნული უსაფრთხოების კონცეფცია ფუძემდებლური დოკუმენტია, რომელიც განმარტავს ეროვნულ ღირებულებებსა და ინტერესებს, აყალიბებს ქვეყნის უსაფრთხო განვითარების ხედვას, მიმოიხილავს სახელმწიფოს წინაშე არსებულ საფრთხეებს, რისკებსა და გამოწვევებს და ადგენს ეროვნული უსაფრთხოების პოლიტიკის ძირითად მიმართულებებს. ეროვნული უსაფრთხოების კონცეფციას უნდა

შეესაბამებოდეს ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვის ყველა ეროვნული და უწყებრივი დონის დოკუმენტი.

საქართველოს საფრთხეების შეფასების დოკუმენტი ასახავს ეროვნული უსაფრთხოებისთვის არსებითი საფრთხის შემცველ სამხედრო, საგარეო პოლიტიკურ, შიდა პოლიტიკურ, ტრანსნაციონალურ, სოციალურ-ეკონომიკურ, ბუნებრივ და ადამიანური ფაქტორით გამოწვეულ საფრთხეებსა და გამოწვევებს. დოკუმენტი შესაბამისი საფრთხეების (მათ შორის, კიბერსაფრთხეების) განვითარების შესაძლო სცენარებს აღწერს და მათ შეფასებას მოიცავს.

აღნიშნულთან ერთად, მნიშვნელოვანია უსაფრთხოების სფეროში ეროვნული სტრატეგიები, რომლებიც კიბერუსაფრთხოების კომპონენტს შეიცავს და რომელთაც, მოცემული სტრატეგია თემატურად ეხმიანება. ამ კონტექსტში, შესაძლებელია, მაგალითების სახით, შემდეგი დოკუმენტების დასახელება: „ტერორიზმის წინააღმდეგ ბრძოლის შესახებ საქართველოს ეროვნული სტრატეგია“, „ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლის ეროვნული სტრატეგია“, „საქართველოს საგარეო პოლიტიკის სტრატეგია“ და სხვა. კიბერკომპონენტი მოცემულია აგრეთვე ცალკეულ სექტორულ დოკუმენტებში, რომლებიც კონკრეტულ სფეროში რისკების შეფასებას ეხება (მაგ. „საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების სტრატეგია 2021-2024“, საქართველოში ფულის გათეთრების და ტერორიზმის დაფინანსების რისკების შეფასება და შესაბამისი ანგარიში).

გარდა ამისა, დოკუმენტი ითვალისწინებს ოქსფორდის უნივერსიტეტის კიბერუსაფრთხოების გლობალური ცენტრის (The Global Cyber Security Capacity Centre) მიერ მომზადებულ შეფასების დოკუმენტს, სადაც შეფასებულია საქართველოში არსებული კიბერუსაფრთხოების გარემო და ასახულია კონკრეტული რეკომენდაციები და ინიციატივები მისი განვითარების მიზნით.

მოქმედების სფერო

კიბერუსაფრთხოების სფეროში რიგით მესამე ეროვნული სტრატეგია მნიშვნელოვანია იმ მხრივაც, რომ მასში გაერთიანდა, როგორც კიბერ და ინფორმაციული უსაფრთხოების გარემოს გაუმჯობესების, ისე კიბერდანაშაულთან ბრძოლისა და კიბერთავდაცვითი შესაძლებლობების გაძლიერებისკენ მიმართული კონკრეტული კომპონენტები. ხშირ შემთხვევაში, საკმაოდ რთულია გამიჯვნა, რადგან საქართველოს კიბერსივრცის უსაფრთხოებისკენ გადადგმული ნაბიჯები, უმრავლეს შემთხვევაში, თანაბრად ემსახურება როგორც კიბერთავდაცვითი გარემოს განვითარებას, ისე კიბერდანაშაულთან ეფექტიან გამკლავებას.

2010 წლიდან დღემდე ქვეყნის მიერ ინსტიტუციური და შესაძლებლობების გაძლიერების, კრიტიკული ინფორმაციული სისტემების დაცულობის, საერთაშორისო ასპარეზზე კონტაქტების დამყარებისა და საერთაშორისო ინიციატივებში ჩართულობის მიმართულებით გადადგმული ნაბიჯები იძლევა საფუძველს, რომ წინამდებარე სტრატეგიის ფარგლებში საქართველომ მიზნად დაისახოს მიღწეული შედეგების განმტკიცება და ახალი საფრთხეებისა და გამოწვევების საპასუხოდ კიბერ და ინფორმაციული უსაფრთხოების გარემოს მდგრადობის უზრუნველყოფა. ეს ყოველივე შესაძლებელია საჯარო და კერძო სექტორის, აკადემიური წრეების აქტიური ძალისხმევითა და კომპლექსური მიდგომების გამოყენებით.

ამდენად, კიბერსივრცეში საფრთხეებსა და ინციდენტებთან დროულად და ეფექტიანად გასამკლავებლად, წინამდებარე სტრატეგია მიზნად ისახავს კიბერუსაფრთხოების, კიბერთავდაცვისა და კიბერდანაშაულის სფეროებში კიბერკულტურისა და კიბერგანათლების განვითარებას, მმართველობითი სისტემის მდგრადობის უზრუნველყოფას, საჯარო-კერძო თანამშრომლობის გაძლიერებას, ძლიერი ადამიანური რესურსების შექმნასა და საერთაშორისო ასპარეზზე საქართველოს, როგორც უსაფრთხო და დაცული ქვეყნის როლის გაძლიერებას.

არსებული მდგომარეობის მიმოხილვა

კიბერუსაფრთხოების უზრუნველყოფა 21-ე საუკუნის ერთ-ერთი ყველაზე დიდი გამოწვევაა განვითარებული სამყაროსთვის.

ისევე როგორც მთელ მსოფლიოში, საქართველოშიც საკმაოდ გაიზარდა ინტერნეტით დაფარვის მასშტაბები. გაერო-ს საერთაშორისო სატელეკომუნიკაციო გაერთიანების (ITU) ოფიციალური

სტატისტიკის თანახმად, საქართველოს მოსახლეობის 70%-ზე მეტს აქვს წვდომა ინტერნეტთან. თუმცა, ქვეყნის სხვადასხვა შიდა გამოკითხვით (e-readiness survey) ეს მაჩვენებელი გაცილებით მაღალ ნიშნულს აღწევს: საქართველოს სტატისტიკის ეროვნული სამსახურის (საქსტატი) მონაცემებით, კომპანიებთან მიმართებით ის თითქმის 98%-ს შეადგენს.

კიბერუსაფრთხოება საქართველოს მთავრობის უსაფრთხოების პოლიტიკის სტრატეგიული მიმართულებაა და მთავრობის მხრიდან დიდი ყურადღება ეთმობა მის განვითარებაზე ზრუნვას. კერძოდ, საქართველოს მთავრობა მიიჩნევს, რომ სახელმწიფოს პრეროგატივაა, ქვეყანაში შექმნას ინფორმაციული საზოგადოების, ციფრული ეკონომიკისა და ელექტრონული მმართველობის ხელსაყრელი გარემო, ჩამოაყალიბოს ისეთი სტრატეგიული, ინსტიტუციურ-ორგანიზაციული და სამართლებრივ-მარეგულირებელი ჩარჩოები, რაც ხელს შეუწყობს ელექტრონულ სივრცეში მოქალაქეების, კერძო და საჯარო სექტორების უსაფრთხო ფუნქციონირებასა და ონლაინ სივრცის დაცულად გამოყენებას.

საქართველოს მთავრობა აქტიურად ისწრაფვის ღია, უსაფრთხო და დაცული კიბერსივრცის უზრუნველყოფისკენ, რათა კიდევ უფრო მეტად განვითარდეს ინფორმაციული საზოგადოება, შეიქმნას საჯარო და კერძო სექტორში ელექტრონული კომერციის, ინფორმაციულ-საკომუნიკაციო ტექნოლოგიებისა და ტრანზაქციების, ასევე, ელექტრონული მმართველობის მომსახურებისთვის სანდო გარემო.[1] აღნიშნული, თავის მხრივ, ქვეყნის შეუფერხებელი ფუნქციონირების, ეროვნული და სამოქალაქო უსაფრთხოების, თავდაცვისა და სოციალურ-ეკონომიკური განვითარების მნიშვნელოვან ხელშემწყობ ფაქტორს წარმოადგენს.

სიძლიერე

კიბერუსაფრთხოება სახელმწიფოს პრიორიტეტი 2008 წლის რუსეთ-საქართველოს ომის შემდგომ გახდა, როდესაც ფართომასშტაბიანი კიბერშეტევების სამიზნედ იქცნენ როგორც სამთავრობო, ისე საბანკო და მედიასექტორები. შესაბამისად, კიბერუსაფრთხოების სფეროში სხვადასხვა აქტორი მოქმედებს, რომელთა მიზანი, სხვა საკითხებთან ერთად, სწორედ ამგვარ საფრთხეებთან გამკლავებაა.

საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი სსიპ – ციფრული მმართველობის სააგენტოს საქმიანობის მიზანია საკუთარი კომპეტენციის შესაბამისად, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების განვითარება და უზრუნველყოფა. სააგენტო, საკუთარი უფლებამოსილების ფარგლებში, ზედამხედველობას უწევს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით გათვალისწინებული ვალდებულებების შესრულებას.

სააგენტო ქმნის სამუშაო ჯგუფებს და წარმართავს მათ საქმიანობას აღნიშნულ სფეროში პოლიტიკის, სტანდარტების და მეთოდოლოგიის შესამუშავებლად. ის კოორდინაციას უწევს საგანმანათლებლო და ცნობიერების ამაღლების კამპანიებს ეროვნულ დონეზე, ასევე, სფეროს სპეციალისტების შესაძლებლობების გაზრდის მიზნით, ერთობლივი კიბერსავარჯიშოებისა და კიბერსწავლების ღონისძიებების ჩატარებას. სააგენტო ქმნის და ადმინისტრირებას უწევს კიბერინციდენტების რეესტრს.

საკუთარი კომპეტენციის შესაბამისად, სააგენტო, საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, აგრეთვე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ, მასთან დაკავშირებულ სხვა საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს მისი კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის (CERT.DGA.GOV.GE) მეშვეობით.

სსიპ –კიბერუსაფრთხოების ბიუროს საქმიანობის სფერო მოიცავს თავდაცვის სამინისტროს სისტემაში არსებული / მოქმედი კრიტიკული ინფორმაციული სისტემის სუბიექტების ინფორმაციული და კიბერუსაფრთხოების პოლიტიკის შემუშავებასა და მისი განხორციელების ხელშეწყობას. თავდაცვის სფეროში კომპიუტერული უსაფრთხოების ინციდენტების, სისუსტეებისა და შესაბამისი მტკიცებულებების დამუშავებას, ანალიზს, რეაგირების მხარდაჭერასა და კოორდინაციას ახორციელებს ბიუროს ერთ-ერთი სტრუქტურული ქვედანაყოფის, კერძოდ კიბერუსაფრთხოების ოპერაციების დეპარტამენტის ფარგლებში მოქმედი, კომპიუტერულ ინციდენტებზე რეაგირების სამმართველო.

2021 წ. 10 ივნისს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში განხორციელებული ცვლილების შედეგად, საკანონმდებლო დონეზე მკაფიოდ განისაზღვრა საქართველოს სახელმწიფო უსაფრთხოების სამსახურის უფლებამოსილებები ქვეყნის კიბერ და ინფორმაციული უსაფრთხოების უზრუნველყოფის პროცესში. შესაბამისი კანონმდებლობის საფუძველზე, კრიტიკული ინფორმაციული სისტემის სუბიექტების კატეგორიზაციის შემდეგ, პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების დაცვაზე პასუხისმგებლობა, საქართველოს სახელმწიფო უსაფრთხოების სამსახურის მმართველობის სფეროში შემავალ საჯარო სამართლის იურიდიულ პირს, საქართველოს ოპერატიულ-ტექნიკურ სააგენტოს დაეკისრება.

საკუთარი კომპეტენციის შესაბამისად, სააგენტო, საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, აგრეთვე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ, მასთან დაკავშირებულ სხვა საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, მისი კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის (CERT.OTA.GOV.GE) მეშვეობით განახორციელებს.

საქართველოს შინაგან საქმეთა სამინისტროში, ცენტრალური კრიმინალური პოლიციის დეპარტამენტში, ორგანიზებულ დანაშაულთან ბრძოლის მთავარი სამმართველოს ფარგლებში, ფუნქციონირებს კიბერდანაშაულთან ბრძოლის სამმართველო. ამასთან, კიბერდანაშაულთან ბრძოლაში, საკუთარი უფლებამოსილების ფარგლებში, ჩართულია საქართველოს პროკურატურა.

სახელმწიფო ინსპექტორის სამსახური ახორციელებს ქვეყანაში პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლს და პასუხისმგებელია მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის შესრულებაზე. სახელმწიფო ინსპექტორის სამსახური კონტროლს უწევს კიბერსივრცეში ფარული საგამოძიებო მოქმედებების განხორციელების პროცესს.

საქართველოს ეროვნული ბანკი უფლებამოსილია, მისი ზედამხედველობის ქვეშ მოქმედ, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკს დაუდგინოს დამატებითი სტანდარტები და მოთხოვნები როგორც ინფორმაციული უსაფრთხოების პოლიტიკის, ისე ინფორმაციული აქტივების მართვისა და შინასამსახურებრივი გამოყენების წესების მიმართ. ეროვნული ბანკი უფლებამოსილია, კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკს მოსთხოვოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების განსახილველად წარდგენა, აგრეთვე, მიიღოს ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის დასრულების შედეგად მომზადებული სამოქმედო გეგმა და მისი შესრულების გრაფიკი და მათი შეფასების საფუძველზე, გასცეს რეკომენდაციები ან/და შესასრულებლად სავალდებულო მითითებები. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკის მიმართ ადმინისტრაციული სამართალდარღვევის საქმის განხილვისა და ადმინისტრაციული სახდელის დადების უფლებამოსილება ეროვნულ ბანკს გააჩნია.

2019 წ. საქართველოში ეროვნული უსაფრთხოების საბჭო შეიქმნა, რომლის ფუნქციონირებასაც საბჭოს აპარატი უზრუნველყოფს. „ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ“ საქართველოს კანონის შესაბამისად, საბჭო ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვის მაკოორდინირებელ უწყებას წარმოადგენს. ეროვნული უსაფრთხოების საბჭოს აპარატი, საინფორმაციო-ანალიტიკურ საქმიანობასთან ერთად, ეროვნული უსაფრთხოების სფეროში, ეროვნული დონის კონცეპტუალური დოკუმენტების შემუშავების პროცესის ორგანიზებასა და კოორდინაციას უზრუნველყოფს. საბჭოს აპარატი რეგულარულად იღებს და ამუშავებს ინფორმაციას ეროვნული უსაფრთხოების წინააღმდეგ მიმართული კიბერსაფრთხეების შესახებ, რის შედეგადაც, საინფორმაციო-ანალიტიკური დოკუმენტების შემუშავების მეშვეობით, შესაბამისი ადრესატების მხარდაჭერას უზრუნველყოფს.

აღნიშნულთან ერთად, საბჭოს აპარატის ფუნქციების კონტექსტში, მნიშვნელოვანია ეროვნულ დონეზე კრიზისული ვითარების მართვის კომპონენტი. საბჭოს აპარატის ერთ-ერთი სტრუქტურული ერთეული, კერძოდ კი, კრიზისული ვითარების მართვის ეროვნული ცენტრი (დეპარტამენტი), ეროვნული სიტუაციური ოთახის ფუნქციონირებას უზრუნველყოფს. აღნიშნული ინფრასტრუქტურა, ეროვნული ინტერესებისთვის საფრთხის შემცველი კრიზისული ვითარების დროს აქტიურდება და მისი მეშვეობით, საქართველოს პრემიერ-მინისტრის მიერ, შესაბამისი ვითარების პოლიტიკურ /

სტრატეგიულ დონეზე მართვა ხორციელდება.

ბოლო ათი წლის განმავლობაში საქართველომ მიიღო და განახორციელა კიბერუსაფრთხოების ორი თანმდევი ეროვნული სტრატეგია შესაბამისი სამოქმედო გეგმებით; ჩამოყალიბდა ინფორმაციული და კიბერუსაფრთხოების სამართლებრივი ბაზა – „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი და მისგან გამომდინარე კანონქვემდებარე აქტები; განისაზღვრა კრიტიკული ინფორმაციული სისტემის სუბიექტები და კიბერუსაფრთხოების უზრუნველყოფაზე პასუხისმგებელი სახელმწიფო ორგანოები; საფუძველი ჩაეყარა ქვეყნის შიგნით საჯარო-კერძო პარტნიორობას კიბერუსაფრთხოების ფორუმის სახით; საქართველომ მონაწილეობის მიღება დაიწყო საერთაშორისო და რეგიონულ დონეზე ორმხრივ და მრავალმხრივ ფორმატებში (EU, NATO, OSCE, UN, EaP, CoE, EUROPOL & INTERPOL, CEPOL, ENISA) კიბერუსაფრთხოების საერთაშორისო პროექტებსა და შეხვედრებში; საქართველოს სამთავრობო უწყებების ორგანიზებით განხორციელდა ცნობიერების ამაღლების ფართომასშტაბიანი კამპანიები, რომელთა მიზანია მოსახლეობაში კიბერჰიგიენის დანერგვა; ასევე, დღემდე აქტიურად მიმდინარეობს სხვადასხვა სამიზნე ჯგუფის სწავლება-გადამზადება ამ მიმართულებით. საქართველოს მთავრობასა და დიდი ბრიტანეთისა და ჩრდილოეთ ირლანდიის გაერთიანებულ სამეფოს შორის, 2018 წლის ნოემბერში გაფორმდა მემორანდუმი კიბერუსაფრთხოების სფეროში გრძელვადიანი და კომპლექსური თანამშრომლობის თაობაზე. ამას გარდა, საქართველოს ეროვნულ და სამთავრობო კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფს (CERT.GOV.GE) გაფორმებული აქვს ცოდნისა და გამოცდილების გაზიარების შესახებ თანამშრომლობითი მემორანდუმები ევროპულ და აღმოსავლეთ პარტნიორობის არაერთი ქვეყნის შესაბამის უწყებებთან (მაგ.: ლიეტუვა, რუმინეთი, მოლდოვა, უკრაინა). საქართველო აქტიურად მონაწილეობს საერთაშორისო კიბერსავარჯიშოებსა და სწავლებებში და შედეგების თვალსაზრისით, მოწინავე ადგილს იკავებს.

ამასთან, სსიპ – საქართველოს ოპერატიულ-ტექნიკურმა სააგენტომ გააფორმა მემორანდუმი მსოფლიოში აღიარებულ კიბერუსაფრთხოებისა და ციფრული ექსპერტიზის საგანმანათლებლო დაწესებულებასთან – ირლანდიის ეროვნული უნივერსიტეტის კიბერუსაფრთხოებისა და კიბერდანაშაულის გამოძიების ცენტრთან, რომელიც მომავალ წლებში სააგენტოს მისცემს საშუალებას, გადაამზადოს საკუთარი თანამშრომლები ევროკავშირის სამართალდამცავი უწყებების მიერ აღიარებული სპეციალიზებული და ელიტური სასწავლო პროგრამების მიხედვით.

მნიშვნელოვანია, აღინიშნოს, რომ საქართველოს ევროპული და ევროატლანტიკური კურსის ერთ-ერთ მდგრად ქვაკუთხედს საქართველოს NATO-სთან თანამშრომლობა წარმოადგენს. შესაბამისად, საქართველოს თავდაცვის სამინისტროს სსიპ კიბერუსაფრთხოების ბიურო თანამშრომლობის აქტიურ ფაზაშია NATO-ს წევრ სახელმწიფოებთან და მონაწილეობს როგორც ინდივიდუალურად, ისე NATO-ს ეგიდით გამართულ სხვადასხვა სახის პროექტებსა და სტრატეგიულ თუ ტექნიკურ სწავლებებში. გარდა ზემოთქმულისა, ბიურომ თანამშრომლობა გააძლიერა EU CSDP პლატფორმის ფარგლებშიც, რაც ეხმიანება ორგანიზაციის საერთაშორისოდ განსაზღვრულ სტრატეგიულ მიზნებს და ჯამში, საქართველოს თავდაცვის სფეროს კიბერუსაფრთხოების შესაძლებლობების განვითარებით ხელს უწყობს ეროვნული უსაფრთხოების განმტკიცებას. საქართველოს მთავრობა აქტიურად ზრუნავს კიბერუსაფრთხოების სფეროში საჯარო სექტორში დასაქმებულ პროფესიონალთა კვალიფიკაციის ამაღლებაზე. შედეგად, თანამშრომელთა კვალიფიკაციის დონე მაღალია და დასაქმებულთაგან არაერთი ფლობს საერთაშორისოდ აღიარებულ და მაღალი რეპუტაციის მქონე სერტიფიკატებს (SANS, ISACA, ISO).

ეროვნული უსაფრთხოების საბჭოს აპარატს, კიბერუსაფრთხოების სფეროს განვითარებაში საკუთარი წვლილი შეაქვს. საბჭოს აპარატის ორგანიზებითა და საქართველოს მთავრობის მხარდაჭერით, 2020 წლის სექტემბერში, „საქართველოს კიბერუსაფრთხოების ფორუმი“ იქნა ინიცირებული. ფორუმი მაღალი დონის ღონისძიებას წარმოადგენს და ის ყოველწლიურად ჩატარდება. აღნიშნულმა ღონისძიებამ, კიბერსივრცეში ქვეყნის (და შავი ზღვის რეგიონის) წინაშე არსებულ გამოწვევებსა და შესაძლებლობებთან დაკავშირებით, იდეების გაზიარებისთვის პლატფორმის ფუნქცია უნდა შეასრულოს. აქედან გამომდინარე, ის, ერთი მხრივ, საქართველოს ეროვნული კიბერუსაფრთხოების არქიტექტურის განმტკიცებას ემსახურება, მეორე მხრივ კი, შავი ზღვის რეგიონში ქვეყნის შესაბამის „სექტორულ პოზიციონირებას“ ამყარებს.

ეროვნული უსაფრთხოების საბჭოს აპარატს, კიბერუსაფრთხოების სფეროში სტრატეგიული და ტექნიკური სავარჯიშოების ორგანიზების / კოორდინაციის კუთხით, მნიშვნელოვანი გამოცდილება დაუგროვდა. 2020 წ., ეროვნული უსაფრთხოების საბჭოს აპარატის კოორდინაციით, ევროსაბჭოსა და

ევროკავშირის მხარდაჭერით, “CyberEast”-ისა და “CyberSecurity EAST”-ის პროექტების ფარგლებში, არჩევნების (კიბერ) უსაფრთხოების თემატიკაზე ტექნიკური და სტრატეგიული სავარჯიშოები ჩატარდა. საბჭოს აპარატის მიერ, იგეგმება თანამშრომლობის აღნიშნული მიმართულების გაღრმავება და საარჩევნო კონტექსტს მიღმა, შესაბამის სფეროში სავარჯიშოების კომპონენტის გააქტიურება.

ამასთან, ეროვნული უსაფრთხოების საბჭოს აპარატი, ცალკეულ, მნიშვნელოვან საკითხებზე საუკეთესო საერთაშორისო პრაქტიკის ქართული მხარისთვის გაზიარებას უზრუნველყოფს (აღსანიშნავია, მაგ. საბჭოს აპარატისა და NATO-საქართველოს პროფესიული განვითარების პროგრამის (PDP) ერთობლივი პროექტის ფარგლებში, ესტონურ მხარესთან თანამშრომლობით ორგანიზებული დისტანციური სემინარი კიბერუსაფრთხოების სფეროში საჯარო და კერძო სექტორებს შორის თანამშრომლობის (PPP) აქტუალურ საკითხებზე).

საქართველოს მიერ კიბერუსაფრთხოების უზრუნველყოფისკენ ბოლო ათწლეულში გადადგმული ნაბიჯები, განხორციელებული რეფორმები და მიმდინარე პროცესები პოზიტიურად არის შეფასებული საერთაშორისო ასპარეზზე. აღმოსავლეთ პარტნიორობისა და პოსტსაბჭოთა ქვეყნებს შორის კიბერუსაფრთხოების განვითარების თვალსაზრისით, საქართველო მოწინავე პოზიციაზეა. ის ითვლება სამხრეთ კავკასიისა და შავი ზღვის აუზის ქვეყნებს შორის რეგიონის ლიდერ ქვეყნად, წინ უსწრებს აღმოსავლეთ და ცენტრალური ევროპის არაერთ სახელმწიფოს, რისი დასტურიცაა საერთაშორისო სატელეკომუნიკაციო გაერთიანების (ITU) კიბერუსაფრთხოების გლობალური ინდექსის (GCI – Global Cybersecurity Index) მაჩვენებლები. სამართლებრივი, ტექნიკური და ადამიანური რესურსების შესაძლებლობების, თანამშრომლობითი ფორმატებისა და ორგანიზაციული კომპონენტების შეფასებით, 2018 წლის შედეგებით, საქართველო მსოფლიოში – მე-18, ხოლო ევროპაში მე-9 ადგილზე იყო. აღსანიშნავია ისიც, რომ 2017 წელს საქართველო 0.81 ქულით ევროპაში საფრანგეთთან ერთად იყოფდა მე-2, ხოლო მსოფლიოში იკავებდა მე-8 ადგილს. კიბერუსაფრთხოების სფეროში საქართველოს შესაძლებლობები, ასევე, შეფასდა ოქსფორდის უნივერსიტეტის კიბერუსაფრთხოების გლობალური ცენტრის მიერ.

განვითარების პრიორიტეტული ასპექტები

თანამედროვე ტექნოლოგიების განვითარებასთან ერთად, ინფორმაციულ-საკომუნიკაციო საშუალებებზე საზოგადოებისა და ბიზნესის მზარდი დამოკიდებულების, ელსერვისების ფართომასშტაბიანი დანერგვისა და ციფრულ ეკონომიკაზე გადასვლის კვალდაკვალ, რადიკალურად იზრდება ტექნოლოგიებიდან მომდინარე რისკები, საფრთხეები და ინციდენტები. დღესდღეობით, პრაქტიკულად, აღარ არსებობს სოციალურ-ეკონომიკურ-საზოგადოებრივი საქმიანობის არცერთი დარგი, საჯარო თუ კერძო სექტორი, რომელიც არ არის მოწყვლადი კიბერსაფრთხეების მიმართ. სწორედ ამიტომ, საქართველო კიბერსაფრთხეებს აღიარებს როგორც ერთ-ერთ მნიშვნელოვან გამოწვევას და რისკფაქტორს ეროვნული უსაფრთხოების უზრუნველყოფის პროცესში.

ადამიანური ფაქტორი ყველაზე მნიშვნელოვანი რისკია ციფრულ სამყაროში. როგორც საერთაშორისო კვლევები ადასტურებს, ყველაზე მეტი კიბერინციდენტი მსოფლიოში სწორედ ადამიანური რესურსის გამოყენებით ხორციელდება, მათ მიერ რისკებისა და საფრთხეების არასათანადო შეფასების, ცოდნისა და ცნობიერების სიმწირის ან/და განზრახ მიმართული არასანქცირებული ქმედებების შედეგად. განსაკუთრებით მნიშვნელოვანია საჯარო სექტორში დასაქმებული პირების ცნობიერების ამაღლების საკითხი, რადგან დღესდღეობით ადამიანური შეცდომებით გამოწვეული კიბერინციდენტები გაცილებით აღემატება კიბერშეტევათა რიცხვს. შესაბამისად, მსოფლიოს მრავალი ქვეყანა, მათ შორის, საქართველო, სტრატეგიულ დონეზე უდგება, ერთი მხრივ, ინფორმაციული საზოგადოების კიბერკულტურის, კიბერუსაფრთხოების საკითხებზე საზოგადოების ცნობიერების ამაღლებისა და მეორე მხრივ, განათლებისა და პროფესიონალთა გადამზადების საკითხებს. ქვეყანაში არის კიბერუსაფრთხოების სპეციალისტთა როგორც რაოდენობრივი სიმწირე, ისე კვალიფიკაციის ნაკლებობა. საქართველოს შრომით ბაზარზე კიბერუსაფრთხოების სპეციალისტების მიმართ მოთხოვნა მაღალია როგორც საჯარო, ისე კერძო სექტორში, თუმცა, ამ მოთხოვნას არსებული საკადრო რესურსი სრულად ვერ აკმაყოფილებს.

უნდა აღინიშნოს ბიუჯეტის სიმცირისა და დაგეგმვის საკითხიც, რომელიც მნიშვნელოვან გავლენას ახდენდა 2013 და 2017 წლებში მიღებული სტრატეგიების იმპლემენტაციის პროცესზე და ზოგადად, კიბერ და ინფორმაციული უსაფრთხოების მიმართულებით სტრატეგიული ინიციატივების განხორციელებაზე. აღნიშნული ნაკლოვანება გათვალისწინებულ იქნა საბიუჯეტო სახსრებისა და

საერთაშორისო ფონდების მოძიებით სტრატეგიის სამოქმედო გეგმის შემუშავებისას.

„Business Software Alliance“ (BSA)-ს 2018 წლის შეფასებით[2], საქართველოში არალიცენზირებული პროგრამული უზრუნველყოფის გამოყენების მაჩვენებელი 81%-ია. საკითხი კვლავ ერთ-ერთ მნიშვნელოვან პრობლემად რჩება, რაც, თავისთავად, ზრდის ამგვარი პროდუქტებიდან მომდინარე უსაფრთხოების ინციდენტების რისკს და მოწყვლადს ხდის მათ მიმართ ბიზნესსუბიექტებსა და ყველა სხვა მომხმარებელს.

გარდა არალიცენზირებული პროგრამული უზრუნველყოფის გამოყენებისა, ერთ-ერთ მთავარ გამოწვევას წარმოადგენს ის გარემოება, რომ საქართველოს ბაზარზე ინფორმაციულ-საკომუნიკაციო ტექნოლოგიური პროდუქტების შესყიდვისას სამთავრობო სექტორსა და კრიტიკულ ინფრასტრუქტურებს არ გააჩნიათ უსაფრთხოების კომპონენტის გათვალისწინების ვალდებულება. მოქმედი სამართლებრივი რეგულაციებისა და არსებული გარემოებების გათვალისწინებით, სახელმწიფო შესყიდვების პროცესში შესაძლოა, სამთავრობო სექტორისა და კრიტიკული ინფრასტრუქტურების მხრიდან არსებობდეს ისეთი პროდუქციის/მომსახურების შესყიდვის საფრთხე, რომელმაც შეიძლება რისკის ქვეშ დააყენოს მათი ინფორმაციული სისტემების მთლიანობა, ხელმისაწვდომობა და კონფიდენციალურობა.

როგორც გაერო-ს საერთაშორისო სატელეკომუნიკაციო კავშირის ინდექსი და სხვადასხვა შიდა კვლევები აჩვენებს, საქართველოში ინტერნეტის მომხმარებელთა რაოდენობა ყოველდღიურად იზრდება, რაც, ბუნებრივია, დღის წესრიგში აყენებს კიბერშეტევებისა და ინციდენტების მიმართ ინტერნეტინფრასტრუქტურის მდგრადობის ამაღლების საკითხს. ელექტრონული მმართველობისა და ელექტრონული კომერციის განვითარების პირობებში, ინტერნეტინფრასტრუქტურის დაცულობა ქვეყნის წინაშე მდგარი ერთ-ერთი მთავარი გამოწვევაა, ინტერნეტინფრასტრუქტურის დივერსიფიკაციის საკითხი კი, სახელმწიფოს ერთ-ერთი მთავარი პრიორიტეტია.

სახელმწიფო სექტორში ოპერირებად საინფორმაციო და საკომუნიკაციო ტექნოლოგიების ლიცენზირებასთან ერთად, არსებითი მნიშვნელობის მქონეა საჯაროდ ხელმისაწვდომი (open source) პროგრამული საშუალებების დანერგვა, იმის გათვალისწინებით, რომ ეს მნიშვნელოვნად დაზოგავს საბიუჯეტო რესურსებს. ამასთან, შეიძლება ზემოხსენებული პროგრამული საშუალებების ფუნქციონირების იმგვარად მოდიფიცირება, რომ შესაძლებელი გახდეს მათი სახელმწიფო სექტორში არსებულ საჭიროებებთან მისადაგება.

შესაძლებლობები

ქვეყნის წინაშე არსებულ კიბერსაფრთხეებსა და გამოწვევებზე ეფექტიანი რეაგირების, მდგრადი და გამართული კიბერუსაფრთხოების ეკოსისტემის განვითარებისთვის იდენტიფიცირებულია სტრატეგიული მიმართულებები, რომლებიც ფართოდ აისახა სტრატეგიულ მიზნებსა და შესაბამის ამოცანებში.

უპირველეს ყოვლისა, მნიშვნელოვანია, რომ კიბერუსაფრთხოების სფეროში არსებობდეს მმართველობის სტრატეგიული მოდელი, რომლის ფარგლებშიც კიბერუსაფრთხოების ეროვნული სტრატეგია და მისი სამოქმედო გეგმა უნდა გახდეს საქართველოს კიბერუსაფრთხოების გზამკვლევი როგორც შიდა დაინტერესებული მხარეებისთვის, ისე გარე აქტორებისთვის. აქვე აღსანიშნავია, რომ არსებული ინსტიტუციური ჩარჩოს მიუხედავად, მნიშვნელოვანია, შეფასდეს ჯერ კიდევ არარსებული ან განსავითარებელი შესაძლებლობები საჯარო სექტორში და მათი განვითარებისათვის გადაიდგას საჭირო ნაბიჯები, ასევე, ჩამოყალიბდეს უწყებათაშორისი კომუნიკაციისა და კოორდინაციის ქმედითი და ეფექტიანი მექანიზმი. მიუხედავად იმისა, რომ საქართველოში კიბერუსაფრთხოების სფეროში შექმნილია გარკვეული ნორმატიული აქტები, სამართლებრივ-მარეგულირებელი ბაზა მაინც რჩება სფეროდ, რომელშიც არის განვითარების შესაძლებლობა.

მიზანშეწონილია, გადაიხედოს საქართველოს კიბერუსაფრთხოების მარეგულირებელი მოქმედი სამართლებრივი საფუძვლები და სამართლებრივი ბაზა განახლდეს საუკეთესო საერთაშორისო მაგალითებისა და პრაქტიკის გათვალისწინებით.

თანამედროვე კიბერსაფრთხეებთან ბრძოლაში სიმძიმის ცენტრი, გარკვეულწილად, კერძო სექტორში კიბერუსაფრთხოების უმაღლესი სტანდარტების უზრუნველყოფისკენ იხრება. კერძო სექტორი სულ

უფრო მაღალი ინტენსივობით ხდება ეროვნული უსაფრთხოების შემადგენელი კომპონენტი, რადგან კრიტიკული ინფორმაციული ინფრასტრუქტურის ძირითადი ნაწილი სწორედ კერძო ბიზნესის ხელშია. ზემოთქმულის გათვალისწინებით, მნიშვნელოვანია, რომ სტრატეგიით განსაზღვრული აქტივობების განხორციელებისას, ერთი მხრივ, რაციონალურად იქნეს გამოყენებული ქვეყნის საჯარო და კერძო სექტორში არსებული კომპეტენცია და მეორე მხრივ, მოხდეს არსებული ერთობლივი ინიციატივების ინსტიტუციონალიზაცია აღნიშნული პარტნიორობისთვის. მთავრობა, ერთი მხრივ, იწყებს პარტნიორობის ახალ ეტაპს, რომელშიც იგულისხმება ინფორმაციაზე წვდომის შესაძლებლობების შექმნა, თანამშრომლობა კიბერინციდენტებთან გამკლავების კუთხით, ცოდნისა და გამოცდილების გაზიარება და ა.შ., ხოლო მეორე მხრივ, სახელმწიფო კერძო სექტორთან მიმართებით ქმნის ახალ მარეგულირებელ სამართლებრივ ჩარჩოს, რომელთან თავსებადობა გახდება კერძო სექტორის კრიტიკული ინფრასტრუქტურების ვალდებულება. თანამშრომლობისა და რეგულირების ორივე ფორმა მიზნად ისახავს ქვეყნის კიბერმდგრადობის ზრდას.

რაც შეეხება ცოდნის დონისა და ცნობიერების ამაღლებას, საქართველოს მთავრობამ ცნობიერების ამაღლების პროგრამები საჯარო მოხელეთა სწავლებით დაიწყო. დღემდე ადმინისტრაციულ ორგანოებში დასაქმებულ 500-ზე მეტ თანამშრომელს გავლილი აქვს ინფორმაციული და კიბერუსაფრთხოების მინიმალური მოთხოვნების ე.წ. კიბერჰიგიენის კურსები, მონაწილეობა აქვს მიღებული შესაბამის პრაქტიკულ სავარჯიშოებსა და სწავლებებში. გარდა საჯარო სექტორში დასაქმებული პირებისა, წინამდებარე სტრატეგიის ფარგლებში ცნობიერების ამაღლების კუთხით ცალკეული აქტივობა განხორციელდება საზოგადოების სხვადასხვა ფოკუსჯგუფისთვის. წინამდებარე სტრატეგიით საქართველოს მთავრობა განახორციელებს რეგულარული და სისტემური ხასიათის ფართომასშტაბიან, სამიზნე ჯგუფებზე მორგებულ ცნობიერების ამაღლების კამპანიებს (მოსწავლეები, მასწავლებლები, ჟურნალისტები, ბიზნესსექტორი, ბიბლიოთეკარები, სტუდენტები, საჯარო მოხელეები, თავდაცვის სფეროს თანამშრომლები (მათ შორის, მენეჯერული რგოლი) და ა.შ.) და კიბერუსაფრთხოებასთან დაკავშირებულ საგანმანათლებლო აქტივობებს აქცევს როგორც საშუალო, ისე უმაღლესი განათლების სისტემის განუყოფელ ნაწილად.

საყოველთაოდ აღიარებულია, რომ კიბერუსაფრთხოების სფეროში რაიმე წარმატების მიღწევა შეუძლებელია პროფესიონალთა ძლიერი გუნდის გარეშე. კიბერუსაფრთხოების მაღალი კვალიფიკაციის სპეციალისტთა რესურსის მოზიდვა და შენარჩუნება ქვეყნის სტრატეგიული მიმართულებაა. საქართველოს მთავრობა იზრუნებს, ხელი შეუწყოს პროფესიონალთა შესაბამის მომზადება-გადამზადების პროცესს. უმაღლესი განათლების საფეხურზე საერთაშორისო სტანდარტების შესაბამისი საგანმანათლებლო პროგრამების შექმნა, თუ სამოქმედო გეგმით გათვალისწინებული სხვა აქტივობების წარმატებით განხორციელება, დარგის სპეციალისტთა მომზადების თვალსაზრისით, ერთ-ერთი წინგადადგმული ნაბიჯი იქნება.

კიბერუსაფრთხოების უზრუნველსაყოფად საერთაშორისო თანამეგობრობასთან პარტნიორულ-თანამშრომლობითი კავშირების გაღრმავება და თანამოაზრე სტრატეგიული მოკავშირეების მხარდაჭერის მოპოვება კიბერუსაფრთხოების სტრატეგიული მიმართულებაა. ამ პროცესში, საქართველოს მთავრობა განსაკუთრებულ ყურადღებას დაუთმობს როგორც საქართველოს სტრატეგიულ მოკავშირე ქვეყნებთან (აშშ, დიდი ბრიტანეთისა და ჩრდილოეთ ირლანდიის გაერთიანებული სამეფო, ესტონეთი, ლიეტუვა, ლატვია და სხვა), ისე ევროპულ და ევროატლანტიკურ სტრუქტურებთან თანამშრომლობის განმტკიცებას.

საფრთხეები

კიბერსაფრთხეების „ტრადიციულ“ ფორმებთან ერთად, შესაბამის სივრცეში საქართველოს მოწყვლადობას, აღნიშნული საფრთხეების თანამედროვე გამოვლინებები განაპირობებს. ახალი კორონავირუსის (COVID-19) პანდემიით გამოწვეულ, დისტანციური მუშაობის უზრუნველყოფის მიზნით ელ. სერვისებზე მზარდ დამოკიდებულებას, შესაბამისი ქსელების / სისტემების უსაფრთხოების კუთხით დამატებითი გამოწვევები მოაქვს.

კიბერსივრცის უსაფრთხოებაზე საკუთარი გავლენა აქვს ხელოვნური ინტელექტის განვითარებას. ამასთან, ყოველდღიურ ცხოვრებაზე, 5-G და ბლოკჩეინ ტექნოლოგიები უშუალო და სულ უფრო მზარდ ზეგავლენას ახდენს. შესაბამისად, კიბერუსაფრთხოების სფეროში, მათთან დაკავშირებული სირთულეების გათვალისწინებაც ხდება საჭირო. აღნიშნული ტექნოლოგიები, ინფორმაციის მიღების, ცოდნის გენერირებისა და მონაცემთა გაცვლის ახალ შესაძლებლობებს ქმნიან, თუმცა, შესაბამისი

სისტემების „ახალი ფორმით“ მოწყვლადობასაც განაპირობებენ.

შესაბამის ინფრასტრუქტურაზე / ტექნოლოგიებზე მზარდი დამოკიდებულება, შესაძლებლობებთან ერთად, საფრთხის აქტორების მხრიდან აღნიშნული ინოვაციების ბოროტად გამოყენების რისკებსაც ზრდის. ახალი ტექნოლოგიების განვითარება იწვევს კიბერთავდასხმების მეთოდებისა და საშუალებების დივერსიფიცირებასა და შემდგომ დახვეწას. აღნიშნული სიტუაცია კიბერუსაფრთხოების უზრუნველყოფის კონტექსტში გარკვეული მიდგომების ცვლილებას / ადაპტაციას განაპირობებს და საერთაშორისო თანამეგობრობის მხრიდან სათანადო რეაგირებას მოითხოვს.

მიუხედავად გარკვეული აღმავლობისა, მომდევნო ნაწილში აღწერილ საფრთხეებსა და რისკებთან გამკლავების მიზნით საქართველოს ჯერ კიდევ დიდი ძალისხმევა დასჭირდება კიბერუსაფრთხოების ეროვნულ-სტრატეგიულ დონეზე განვითარების თვალსაზრისით. თუკი წინა წლებში შეიქმნა მყარი საფუძველი კიბერუსაფრთხოებისთვის, დღეს და სამომავლოდ კრიტიკულია ამ ხელშემწყობი ჩარჩოების მდგრადი განვითარება, არსებული პროგრესის შენარჩუნება და მასზე დაშენებით კიბერუსაფრთხოების ეროვნული შესაძლებლობებისა და საქართველოს კიბერუსაფრთხოების პოლიტიკის სტრატეგიული მიმართულებების გაძლიერება.

კომპიუტერულ ინციდენტებზე დახმარების ეროვნული და სამთავრობო ჯგუფის (CERT.GOV.GE) მიერ ინციდენტების აღმოჩენისა და მათზე რეაგირების სხვადასხვა ტექნოლოგიური საშუალების გამოყენებით (ქსელისა და IP მონიტორინგის სისტემა, პორტალები, სენსორები და ა.შ.) მიღებული სტატისტიკა ცხადყოფს, რომ 2014 წლიდან 2019 წლამდე დარეგისტრირებული ინციდენტების რაოდენობა, სულ მცირე, ორჯერ გაიზარდა. ამასთან, იმატა დაინფიცირებული IP მისამართების რიცხვმა და პორტალებთან დაკავშირებულმა უსაფრთხოების მოვლენებმა.

· კიბერომი, საინფორმაციო ომი, კიბერჯაშუშობა, სახელმწიფო აქტორების მიერ მართული კიბერშეტევები

საქართველო არის ერთ-ერთი პირველი ქვეყანა მსოფლიოში, რომელსაც სახმელეთო, საჰაერო და საზღვაო სივრცის დაცვასთან ერთად, ჯერ კიდევ 2008 წელს, რუსეთ-საქართველოს ომის დროს, დღის წესრიგში დაუდგა კიბერსაომარი მოქმედებებისგან საკუთარი კიბერსივრცის უსაფრთხოების უზრუნველყოფა. გეოპოლიტიკური მდებარეობა, ქვეყნის პოლიტიკური კურსი და ევროატლანტიკურ სტრუქტურებში ინტეგრაციისკენ სწრაფვა საქართველოს, პირველ რიგში, რუსეთის ფედერაციის მხრიდან ხდის პოლიტიკურად მოტივირებული კიბერშეტევების, ინფორმაციული პროპაგანდის, ყალბი ინფორმაციის, კიბერჯაშუშობისა და კიბერტერორიზმის სამიზნედ.

რუსეთის ფედერაციის მხრიდან საქართველოს წინააღმდეგ მართული საინფორმაციო ომი, რომელიც, თავის მხრივ, მოიცავს პროპაგანდისა და დეზინფორმაციის მაღალ ხარისხს, ქმნის ნიადაგს საზოგადოებრივი აზრის მანიპულაციისთვის, რაც, მიმდინარე სამხედრო ოკუპაციის კვალდაკვალ, ეროვნული უსაფრთხოებისთვის სერიოზულ გამოწვევას წარმოადგენს.

ქართული საზოგადოების არჩევანზე, რომელიც ეროვნული უსაფრთხოების მდგრადობის გაძლიერებას, რუსული გავლენისგან გათავისუფლებასა და დასავლურ სტრუქტურებში ინტეგრაციას ითვალისწინებს, ხდება მიზანმიმართული ზემოქმედება სახელმწიფოს საგარეო პოლიტიკური კურსის სახეცვლილებისა და ერთგვარად ნეიტრალური საგარეო კურსის გატარების მიზნით.

ევროინტეგრაციის პროცესში მიღწეული წარმატებისა და ამ პროცესით გამოწვეული განვითარების გადაფარვა, საქართველოში დასავლური გზის მარგინალიზება და დასავლელი პარტნიორების თვალში საქართველოს როლის დაკნინება რუსეთის ფედერაციის ის სტრატეგიული მიზანია, რომელსაც კრემლის მიერ, პრაქტიკულ დონეზე გამოყენებული ყველა მეთოდი, კინეტიკური თუ ჰიბრიდული ომი, მკაცრად ემსახურება.

ხაზგასასმელია ის გარემოებაც, რომ იზრდება რუსეთის ფედერაციის მხრიდან მომდინარე საფრთხეები (Advanced Persistent Threats), რომელთა მიზანია საქართველოს კერძო და საჯარო კრიტიკული ინფრასტრუქტურების ინფორმაციასთან არაავტორიზებული წვდომა.

ამრიგად, ამ ტიპის მაღალი ინტენსივობის, მიზანმიმართული და ფართომასშტაბიანი შეტევები კვლავ

რჩება საქართველოსთვის ერთ-ერთ მთავარ გამოწვევად, რომელთან გამკლავებაც, საქართველოს ეროვნული კიბერუსაფრთხოების მთავარი სტრატეგიული ამოცანაა.

ინტერნეტის გამოყენება ტერორისტების მიერ, კომპიუტერული საშუალებებით ჩადენილი დანაშაულის კიდევ ერთი სახეობაა. ტერორისტები სულ უფრო ხშირად მიმართავენ ინფორმაციულ სისტემებს ინფორმაციის გავრცელების, კომუნიკაციისა და პროპაგანდის მიზნით. უკანასკნელი წლების პრაქტიკამ დაადასტურა, რომ რიგი ტერორისტული ორგანიზაციების მხრიდან, როგორიცაა მაგალითად, „ისლამური სახელმწიფო“, ინტენსიურად გამოიყენებოდა თანამედროვე ინფორმაციული და საკომუნიკაციო საშუალებები, როგორც ტერორისტულ ორგანიზაციაში რეკრუტირებისა და ტერორისტული პროპაგანდის გავრცელებისთვის, ისე ქვეყნის შიგნით ტერორისტული ქსელის შექმნის მიზნებისთვის.

გარდა ზემოაღნიშნული მაღალი ინტენსივობის, სახელმწიფო აქტორების ჩართულობით მართული მიზანმიმართული შეტევებისა, ძალზედ მნიშვნელოვანი სამიზნე გახდა კრიტიკული ინფორმაციული ინფრასტრუქტურა, კერძოდ, სახელმწიფოსა და საზოგადოებისთვის კრიტიკულად მნიშვნელოვანი ფუნქციების განხორციელებისა და სერვისების მიწოდების პროცესში გამოყენებული ინფორმაციული სისტემები და ტექნოლოგიები. კრიტიკული ინფრასტრუქტურების მიმართ საფრთხის წყაროს არამარტო „გარე აქტორები“ წარმოადგენენ, არამედ აღნიშნულ სუბიექტებთან დაკავშირებით, საფრთხის აქტორები ასევე, შესაბამისი „სისტემის შიგნით“ აქტიურდებიან (ე.წ. “insider threat”). ამასთან, მნიშვნელოვან გამოწვევას წარმოადგენს „მიწოდების ჯაჭვის“ (supply chain) მოწყვლადობა და შესაბამის ინფორმაციულ ტექნოლოგიებსა და სისტემებს, ასევე სხვა პროდუქტებსა და მომსახურებასთან დაკავშირებული რისკები.

კიბერინციდენტებისა და კომპიუტერული საფრთხეების ზრდამ შესაძლოა, გამოიწვიოს სასიცოცხლოდ მნიშვნელოვანი, ინფორმაციული სისტემებისა და კრიტიკული სერვისების ფუნქციონირების შეწყვეტა ან შეჩერება, ეკონომიკური აქტივობების შეზღუდვა, მნიშვნელოვანი ფინანსური ზარალი და მომხმარებელთა ნდობის დაკარგვა სრულიად ელექტრონული მმართველობის მიმართ. დღეს საქართველოს სახელმწიფო და კერძო სექტორში არსებული კრიტიკული ინფრასტრუქტურები ყოველდღიურ საქმიანობაში, უმეტესწილად, სწორედ ინფორმაციულ-საკომუნიკაციო ტექნოლოგიებს იყენებენ. შესაბამისად, მათ მიერ გამოყენებული ტექნოლოგიების კომპრომეტირება და ამით სახელმწიფო და ბიზნესინტერესებისა თუ ინდივიდუალური მომხმარებლების დაზარალება მრავალი დანაშაულებრივი დაჯგუფების მიზანია. შედეგად, პოტენციური ზიანი იქნება გაცილებით მაღალი, ვიდრე ეს 2008 წელს იყო სწორედ სახელმწიფო და კერძო სერვისების ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე მაღალი დამოკიდებულების გამო. ამ მიზეზებისა და იმ არსებული მდგომარეობის გათვალისწინებით, რომ კრიტიკული ინფორმაციული სისტემისა და სერვისების განმახორციელებელ სუბიექტებს არ გააჩნიათ ინფორმაციული და კიბერუსაფრთხოების უზრუნველყოფის სათანადო დონე, საქართველოს კიბერუსაფრთხოებისთვის სტრატეგიული საკითხია საჯარო და კერძო სექტორში მოქმედი კრიტიკული ინფორმაციული ინფრასტრუქტურების უსაფრთხოებისა და დაცულობის ხარისხის ამაღლება.

უნდა აღინიშნოს, რომ ამ მიმართულებითაც საქართველოსთვის მთავარი საფრთხე კვლავ მომდინარეობს რუსეთის ფედერაციის მხრიდან იმდენად, რამდენადაც სწორედ ეს უკანასკნელი ახორციელებდა 2008 წელს საქართველოს საჯარო თუ კერძო სექტორის წინააღმდეგ თავდასხმებს. სახელმწიფო აქტორებთან ერთად, ამ კუთხით მნიშვნელოვან საფრთხეებს ქმნიან ტერორისტული ორგანიზაციებიც, რომელთა წინააღმდეგ საქართველო ჩართულია საერთაშორისო კოალიციებში.

· კიბერდანაშაული (მათ შორის, კრიტიკული ინფრასტრუქტურების წინააღმდეგ მიმართული შეტევები)

კიბერსივრცე დანაშაულებრივი ქმედებების ჩასადენად საკმაოდ ხელსაყრელი გარემოა, ვინაიდან, ხშირ შემთხვევაში, ტექნოლოგიური ინოვაციები, დანაშაულის დისტანციურად და ფარულად ჩადენის შესაძლებლობა, მტკიცებულებათა ცვალებადობა, დამნაშავეთა იდენტიფიცირების სირთულეები და იურისდიქციასთან დაკავშირებული პრობლემები კრიმინალებისთვის ინტერნეტსივრცის არაკანონიერი გზით გამოყენებას მიმზიდველს ხდის. „კიბერ“ ელემენტი თითქმის ყველა კატეგორიის დანაშაულის შემადგენელი ნაწილი ხდება. ინტერნეტსივრცე, ტექნოლოგიური გარემო, ერთი მხრივ, ხელს უწყობს სხვადასხვა დანაშაულებრივი ქმედების ჩადენას (მაგ.: თაღლითობა, საკუთრების წინააღმდეგ მიმართული სხვა დანაშაულები, ნარკოტიკული საშუალებების რეალიზაცია ინტერნეტის

გამოყენებით) და წარმოადგენს დანაშაულის ჩადენის დამხმარე საშუალებას. მეორე მხრივ, ვიწრო, „კლასიკური გაგებით“ გვხვდება კომპიუტერული მონაცემებისა და სისტემების კონფიდენციალურობის, ხელმისაწვდომობისა და მთლიანობის წინააღმდეგ ჩადენილი დანაშაულები.

დღესდღეობით ფართოდ არის გავრცელებული კიბერდანაშაულის ისეთი სახეები, როგორიცაა: კომპიუტერულ სისტემაზე უნებართვო წვდომა, კომპიუტერულ მონაცემთა არამართლზომიერი დაუფლება, მონაცემთა ხელყოფა, კომპიუტერული მოწყობილობების არასანქცირებული გამოყენება, არასრულწლოვანთა პორნოგრაფიასა და ინტელექტუალურ საკუთრებასთან დაკავშირებული დანაშაულები. განსაკუთრებით ფართოდ გავრცელებული შემთხვევებია ე.წ. ფიშინგი, პერსონალური მონაცემების მოპარვა (Identity Theft), მავნე კოდისა და „Deface“-ის გამოყენება.

ბოლო პერიოდის პრაქტიკა აჩვენებს, რომ სახელმწიფო კრიტიკულ სექტორებთან ერთად, შეტევის სამიზნედ სულ უფრო ხშირად გვევლინებიან კომერციული სუბიექტებიც, რაც მიზნად ისახავს აღნიშნული სექტორისთვის, სულ მცირე, რეპუტაციული ზიანის მიყენებას და სათანადო პირობების არსებობისას, მის პარალიზებას. ზემოთქმულის მაგალითია 2016 წელს, საბანკო სექტორისა და სახელმწიფო ელექტრონული ფინანსური სერვისების წინააღმდეგ განხორციელებული ფართომასშტაბიანი „DDoS“ შეტევა, რომლის შედეგადაც, ადგილი ჰქონდა ონლაინ საბანკო სერვისებისა და სახელმწიფო საგადასახადო სისტემის მუშაობის შეფერხებას.

ბოლო პერიოდში, კრიტიკული ინფრასტრუქტურების წინააღმდეგ მიმართულ შეტევებს შორის ყველაზე გავრცელებულია: „ფიშინგი“ (phishing), „რანსომვეარი“ (Ransomeware), „დიფეისი“ (deface), „დიდოსი“ (DDoS) და „ელფოსტის სპუფინგი“ (mail spoofing).

სტრატეგიის შემუშავებისა და განხორციელების პრინციპები

- კიბერუსაფრთხოება, როგორც **ეროვნული უსაფრთხოების განუყოფელი ნაწილი** – წინამდებარე სტრატეგია საქართველოს კანონმდებლობისა და ეროვნული უსაფრთხოების ფუნდამენტური კონცეპტუალური დოკუმენტების თანახმად, კიბერუსაფრთხოებას აცხადებს ეროვნული უსაფრთხოების პოლიტიკის განუყოფელ ნაწილად და შესაბამისად, მისი უზრუნველყოფა განხორციელდება ეროვნული უსაფრთხოების სხვა სფეროებთან უშუალო კავშირში;

- **ერთიანი სახელმწიფოებრივი მიდგომა** – კიბერუსაფრთხოება „ყველას“ პასუხისმგებლობაა. ერთი მხრივ, სახელმწიფო უზრუნველყოფს კიბერუსაფრთხოების ხელშემწყობი ჩარჩოების ჩამოყალიბებას; ძირითადი სტრატეგიული, ინსტიტუციური და მარეგულირებელი მექანიზმების ფუნქციონირებასა და საბაზისო სერვისების მიწოდებას; ხოლო მეორე მხრივ, კერძო სექტორისა და მოქალაქეების ჩართულობა მნიშვნელოვან როლს ასრულებს ეროვნული კიბერუსაფრთხოების განვითარების პროცესში. ინდივიდუალური პასუხისმგებლობის გარეშე, ასევე, ბიზნესსექტორის, კრიტიკული ინფორმაციული ინფრასტრუქტურების, აკადემიური წრეებისა და ინფორმაციული საზოგადოების ჩართულობის გარეშე, საჯარო უწყებების მიერ განხორციელებული ღონისძიებები ვერ უზრუნველყოფს საქართველოს კიბერუსაფრთხოების განვითარებას;

- **ერთიანი სამთავრობო ხედვა** – კიბერუსაფრთხოების უზრუნველყოფა შესაძლებელი გახდება მხოლოდ მკაფიოდ დელეგირებული უფლებამოსილებებით აღჭურვილი უწყებების კოორდინირებული ქმედებებით, მაკოორდინირებელი უწყების იდენტიფიცირებით, საზედამხედველო სისტემის ჩართულობითა და პოლიტიკური და ფინანსური მხარდაჭერით;

- **კანონიერება** – გულისხმობს ფიზიკური და იურიდიული პირების უფლებათა და თავისუფლებათა დაცვასა და პატივისცემას ონლაინ სივრცეში, ისევე როგორც ეს გარანტირებულია ფიზიკურ სივრცეში;

- კიბერუსაფრთხოების უზრუნველყოფა უნდა განხორციელდეს **პროპორციულ, თანაზომიერ და აუცილებელ ღონისძიებათა ერთობლიობით** ისე, რომ არ ილახებოდეს პირადი ცხოვრების ხელშეუხებლობა და უზრუნველყოფილი იყოს პერსონალურ მონაცემთა დაცვა;

- **საჯარო და კერძო აქტორებს შორის რესურსების გაზიარებით კიბერუსაფრთხოების სფეროში პროფესიონალიზმის გაძლიერება** – მნიშვნელოვანია საჯარო და კერძო სექტორის

შესაძლებლობების ზრდა ცოდნისა და გამოცდილების, ინციდენტებისა და საფრთხეების შესახებ ინფორმაციისა და საუკეთესო პრაქტიკის გაზიარებით;

- **ახალი ტალანტების მოძიება** – კიბერუსაფრთხოების მდგრადი გარემოს შექმნა შესაძლებელია სწორედ ადამიანური და ტექნოლოგიური რესურსების ეფექტიანი გაზიარებითა და შესაძლებლობების განვითარებით;

- **საზოგადოების ცნობიერების ამაღლება** – ინფორმაციულ საზოგადოებაში, კულტურულ დონეზე ცვლილებების მიღწევა, ფუნდამენტური ცვლილებების ადვილად განხორციელების საფუძველს და ამავე დროს, მთელი რიგი კიბერსაფრთხეების თავიდან აცილების საშუალებას წარმოადგენს;

- **რისკების მართვაზე დაფუძნებული სისტემა** – ვინაიდან არ არსებობს კიბერსაფრთხეების საწინააღმდეგო 100%-იანი ეფექტის მქონე მექანიზმები, მათთან გამკლავება რისკებზე დაფუძნებული კიბერუსაფრთხოების პოლიტიკით მოხდება;

- **ინოვაციებზე ორიენტირება** – საქართველო მიზნად ისახავს თანამედროვე საერთაშორისო ტენდენციების გათვალისწინებასა და ტექნოლოგიური თვითმყოფადობის მიღწევას, რაც ხელს შეუწყობს ქვეყნის ეკონომიკურ განვითარებას;

- **აქტიური საერთაშორისო თანამშრომლობა** – საქართველოს მთავრობა აცნობიერებს, რომ შესაბამისი საფრთხეების ტრანსნაციონალური ხასიათიდან გამომდინარე, შეუძლებელია, მხოლოდ საკუთარი რესურსებით უზრუნველყოს კიბერუსაფრთხოების სფეროში არსებულ გამოწვევებსა და საფრთხეებთან გამკლავება. იმის გათვალისწინებით, რომ კიბერინციდენტების გამოძიებისთვის საჭირო მონაცემები ინახება სხვადასხვა ქვეყნის იურისდიქციის ქვეშ არსებულ ინფრასტრუქტურაში, სწორედ საერთაშორისო თანამშრომლობა წარმოადგენს ამ ტიპის ინციდენტების პრევენციისა და აღკვეთის აუცილებელ წინაპირობას.

კიბერუსაფრთხოების ეროვნული სტრატეგიის მიზნები და ამოცანები

საქართველოს კიბერუსაფრთხოების გარემოს ანალიზის შედეგად, წინამდებარე სტრატეგიის ხედვის სისრულეში მოყვანის მიზნით, საქართველოს მთავრობა სტრატეგიის სამოქმედო პერიოდის გათვალისწინებით განსაზღვრავს 4 პრიორიტეტულ მიზანს:

მიზანი 1: ინფორმაციული საზოგადოებისა და ორგანიზაციების კიბერკულტურის განვითარება და შესაძლებლობების გაძლიერება კიბერსივრცეში საფრთხეებსა და ინციდენტებთან გამკლავების მიზნით

ელექტრონული მომსახურებების გამოყენების ზრდის პარალელურად იზრდება კიბერინციდენტების რიცხვიც და ბუნებრივია, სულ უფრო მეტად მნიშვნელოვანი ხდება საზოგადოების წევრთა ცნობიერების ამაღლება, კიბერკულტურის განვითარება და კიბერსივრცეში არსებულ საფრთხეებთან გამკლავების ეფექტიანი მექანიზმების დანერგვა. ეს ყოველივე, საბოლოო ჯამში, კიბერუსაფრთხოების გარემოს მდგრადობის უზრუნველყოფის მიზანს ემსახურება. საჯარო სექტორი უზრუნველყოფს უწყებათაშორისი კოორდინაციის გზით განათლებისა და ცნობიერების ამაღლების ერთიანი კამპანიის წარმოებას, რომელიც მოიცავს კიბერსივრცის დაცვასთან დაკავშირებულ სხვადასხვა მიმართულებას (კიბერუსაფრთხოების საფუძვლები და კიბერჰიგიენა, კიბერთავდაცვა, კიბერდანაშაული, მედიაწიგნიერება, პერსონალური მონაცემების დაცვა კიბერსივრცეში). საუკეთესო საერთაშორისო გამოცდილების გათვალისწინებით, შესაბამისი, მაღალი ხარისხის საგანმანათლებლო პროგრამები შეიქმნება როგორც საშუალო, ისე უმაღლესი განათლების საფეხურზე. ამასთან, კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების კამპანიები ჩატარდება საჯარო (მათ შორის, თავდაცვის) და კერძო სექტორის, მოსახლეობისა და მედიისთვის, რაც უზრუნველყოფს კიბერსაფრთხეებსა და რისკებთან მოპყრობის შესახებ საზოგადოების ინფორმირებას და რაც მთავარია, საზოგადოებაში კიბერკულტურის ჩამოყალიბებას. თავის მხრივ, ინფორმაციული საზოგადოების ცნობიერების ამაღლება და კიბერკულტურის განვითარება წინაპირობა იქნება მომავალი კიბერსპეციალისტების მოზიდვისა და გადამზადებისთვის.

საბოლოო ჯამში, აღნიშნული მიმართულებებით განხორციელებული აქტივობები გახდება

კიბერსაფრთხეებისა და შეტევების მიმართ საქართველოს მდგრადობის ერთ-ერთი საფუძველი.

აღნიშნული მიზნის მისაღწევად ძირითად ამოცანებს წარმოადგენს:

ამოცანა 1.1: კიბერსივრცეში უსაფრთხოდ და დაცულად ფუნქციონირებისთვის სკოლის მოსწავლეებისა და სტუდენტებისთვის საჭირო უნარ-ჩვევების განვითარება და განათლების დონის ამაღლება

აღნიშნული ამოცანის ფარგლებში, როგორც საშუალო სკოლებში, ისე საუნივერსიტეტო დონეზე შემუშავდება და დაინერგება მაღალი ხარისხის საგანმანათლებლო პროგრამები. საბაკალავრო და სამაგისტრო კურსები უნდა დამკვიდრდეს საქართველოში აკრედიტებულ სასწავლებლებში, მათ შორის, სახელმწიფო უსაფრთხოების სასწავლო-სატრენინგო ცენტრებსა და შსს-ის აკადემიაში. შედეგად, განათლების სისტემამ უნდა უზრუნველყოს შრომის ბაზარზე არსებული მოთხოვნების შესაბამისი სპეციალისტების მომზადება. სტრატეგიის ფარგლებში, ახალგაზრდა ტალანტების აღმოსაჩენად გათვალისწინებულია კიბერტრენინგებისა და სავარჯიშოების ჩატარება სკოლის მოსწავლეებისა და სტუდენტებისთვის (მაგ.: Cyberclass), ასევე, მასწავლებელთა და ტრენერთა გადამზადება (ToT) ამ სფეროში. „ციფრული მოქალაქეობის“ (digital citizenship) კურსი მოიცავს ასაკობრივად ადაპტირებული სასწავლო მასალების შექმნას კიბერუსაფრთხოების, კიბერდანაშაულის, კიბერბულინგის, პერსონალურ მონაცემთა დაცვისა და კიბერსივრცეში მედიაწიგნიერების საფუძვლების შესახებ. შესაბამისი უნარ-ჩვევებით აღჭურვილ სკოლის მოსწავლეებსა და სტუდენტებს ექნებათ კიბერსაფრთხეების იდენტიფიცირების, კიბერინციდენტების პრევენციისა და მათთან დამოუკიდებლად გამკლავებისთვის აუცილებელი საბაზისო კომპეტენცია. აღნიშნული ამოცანის წარმატებით განხორციელების შემთხვევაში, სპეციალური ცოდნისა და უნარების მქონე მოქალაქეები სამომავლოდ დასაქმდებიან კიბერუსაფრთხოების სფეროში და ამგვარად ხელს შეუწყობენ ქვეყნის კიბერუსაფრთხოების განვითარებას.

ამოცანა 1.2: კიბერსივრცეში უსაფრთხოდ და დაცულად ფუნქციონირებისთვის კიბერსაფრთხეებისა და რისკების შესახებ ინფორმაციული საზოგადოებისა და ორგანიზაციების ცნობიერების ამაღლება

კიბერსივრცის უსაფრთხოება და დაცულობა მიიღწევა მხოლოდ კიბერსაფრთხეებისა და რისკების შესახებ სამიზნე აუდიტორიის დროული ინფორმირების, მათი მხრიდან რისკების სათანადოდ გაცნობიერებისა და პრევენციული და სხვა სახის თავდაცვითი ღონისძიებების გატარების გზით. მიუხედავად იმისა, რომ კიბერუსაფრთხოება ყველა აქტორის ინდივიდუალური პასუხისმგებლობაა, სახელმწიფო, თავის მხრივ, ვალდებულია, იზრუნოს საფრთხეებისა და რისკების შესახებ საზოგადოების წევრთა ცნობიერების ამაღლებაზე, რათა მათ შეძლონ, სათანადოდ გაუმკლავდნენ კიბერინციდენტებს. მოცემული სტრატეგიის ფარგლებში, ცნობიერების ამაღლების აქტივობები, შესაძლოა განხორციელდეს საზოგადოების სხვადასხვა ფოკუსჯგუფში, საერთაშორისო (Safer Internet Day, Stop. Think. Connect Cybersecurity Month.) და ადგილობრივი ინიციატივების ფარგლებში, ტრენინგების, დისტანციური სწავლების პლატფორმებისა და სასწავლო მასალების შექმნის, გაცნობითი და სამუშაო შეხვედრების, საინფორმაციო ვიდეორგოლების დამზადებისა და სხვა სარეკლამო-საინფორმაციო კამპანიების წარმოების გზით.

მიზანი 2: კიბერუსაფრთხოების მმართველობითი სისტემის მდგრადობა და საჯარო-კერძო თანამშრომლობის გაძლიერება

წინამდებარე სტრატეგიის მეორე მიზანს წარმოადგენს საერთაშორისო სტანდარტებისა და საუკეთესო პრაქტიკის შესაბამისი, თანამედროვე გამოწვევებზე მორგებული სამართლებრივი ბაზის (მათ შორის, კიბერდანაშაულის მარეგულირებელი სამართლებრივი ჩარჩოს) განვითარება, ქმედითი და ეფექტიანი ინსტიტუციური არქიტექტურის შექმნა და ეროვნულ დონეზე კიბერაქტორების კოორდინირებული და თანამშრომლობითი ურთიერთობის ჩამოყალიბება, რაც უზრუნველყოფს ეროვნული კიბერუსაფრთხოების გარემოს, მათ შორის, კრიტიკული ინფორმაციული სისტემის სუბიექტების დაცულობასა და მდგრად ფუნქციონირებას. ამ ხელშემწყობი ჩარჩოების ჩამოყალიბება წაადგება ქვეყნის მიერ როგორც პროაქტიური, პრევენციული ღონისძიებების გატარებას, ისე კიბერინციდენტებთან გამკლავებისა და კიბერთავდაცვითი ზომების მიღებას.

აღნიშნული მიზნის მისაღწევად ძირითად ამოცანებს წარმოადგენს:

ამოცანა 2.1: ეროვნულ დონეზე კიბერინციდენტებისა და კიბერსაფრთხეების დროული გამოვლენის, რეპორტინგისა და მათთან ეფექტიანი გამკლავების სისტემის შექმნა და განვითარება

ქმედითი და ეფექტიანი ინსტიტუციური მოდელის ჩამოსაყალიბებლად აუცილებელია, ერთი მხრივ, კრიტიკული ინფორმაციული სისტემის სუბიექტთა განსაზღვრის მეთოდოლოგიის, კიბერინციდენტების კლასიფიცირების, ხოლო მეორე მხრივ, კიბერინციდენტების შესახებ ინფორმაციის გაცვლის, ინციდენტებზე რეაგირებისა და კრიზისულ სიტუაციებთან გამკლავების მაკოორდინირებელი მექანიზმის შექმნა შესაბამისი საკანონმდებლო და ინსტიტუციური ცვლილებებისა და ტექნოლოგიური გადაწყვეტების გზით. მათ შორის, კიბერინციდენტების კლასიფიცირების მიხედვით, ეროვნული უსაფრთხოებისთვის მაღალი საფრთხის შემცველ კიბერინციდენტებზე ერთიანი რეაგირების მიზნით, საჭიროა შეიქმნას უწყებათაშორისი სამუშაო ჯგუფი (Task Force), რომელიც უშუალოდ ოპერატიულ დონეზე შეძლებს ამ ტიპის კიბერინციდენტების მართვასა და აღმოფხვრას.

საქართველო მიზნად ისახავს სამთავრობო უწყებების მიერ საჯარო სექტორსა და კრიტიკულ ინფორმაციულ სისტემებში ინციდენტების აღმოჩენის, მონიტორინგისა და მათთან გამკლავების შესაძლებლობების განვითარებას. ამდენად, ზემოაღნიშნული ხელს შეუწყობს კრიტიკული ინფორმაციული სისტემების მდგრადობას როგორც საჯარო, ისე კერძო სექტორებში.

უნდა განისაზღვროს სექტორების მარეგულირებლების როლი და ფუნქციები. ინსტიტუციური ჩარჩო უნდა უზრუნველყოფდეს, რომ ფუნქციების დუბლირება და ორმაგი რეგულირება თავიდან იქნას აცილებული. საერთაშორისო სტანდარტების შესაბამისი, თანამედროვე გამოწვევებზე მორგებული ქმედითი და ეფექტიანი ინსტიტუციური სტრუქტურის ჩამოყალიბებამ უნდა უზრუნველყოს ამ სფეროში არსებული ინციდენტების მართვა. კიბერინციდენტებზე რეაგირების ქმედითი და ეფექტიანი მოდელის ჩამოსაყალიბებლად მიღწეულ უნდა იქნას სფეროს მარეგულირებელი სამართლებრივი აქტების ისეთ საერთაშორისო რეგულაციებთან თავსებადობის უზრუნველყოფა, როგორიცაა მაგალითად, ePrivacy Directive.

კიბერინციდენტებსა თუ კიბერსაფრთხეებთან დროული და ეფექტიანი ბრძოლის სისტემის შექმნა წარმოუდგენელია პრევენციული ღონისძიებებისა და მათი აღსრულების მექანიზმების (მათ შორის, საკანონმდებლო დონეზე) დანერგვის გარეშე, ვინაიდან სხვაგვარად სახელმწიფო მუდმივად იქნება რეაგირების რეჟიმში.

ამოცანა 2.2: კიბერდანაშაულის წინააღმდეგ ბრძოლის ეფექტიანი სისტემის განვითარება

კიბერდანაშაულზე რეაგირების ქმედითი და ეფექტიანი მოდელის ჩამოსაყალიბებლად უნდა განხორციელდეს კიბერდანაშაულის საკითხების მარეგულირებელი სამართლებრივი ბაზის სრულყოფა, ასევე, შეიქმნას კიბერდანაშაულის რეპორტინგის (ინფორმაციის მიწოდების) ერთიანი საკონტაქტო პუნქტი.

ამოცანა 2.3: ჩამოყალიბებული საკომუნიკაციო პლატფორმების გამოყენებით თანამედროვე ტენდენციების, საუკეთესო პრაქტიკისა და კიბერსაფრთხეების შესახებ ინფორმაციის გაცვლა და საერთაშორისო სტანდარტების დანერგვის ხელშეწყობა

სტრატეგიის მეორე მიზნის მისაღწევად ერთ-ერთი გადასაჭრელი ამოცანაა საერთაშორისო სტანდარტებისა და საუკეთესო პრაქტიკის, ინოვაციური მიდგომებისა და ახალი სანდო პროდუქტებისა და გადაწყვეტების დანერგვის ხელშეწყობა, რაც გულისხმობს საჯარო და კერძო სექტორებს შორის ცოდნისა და გამოცდილების გაზიარების გზით, მდგრადი და უსაფრთხო კიბერსისტემის შექმნას. მაგალითად, საფრთხის შემცველი პროგრამული უზრუნველყოფის გამოყენებისგან თავის არიდების მიზნით, ასევე, შიფრაციისა და კრიპტოგრაფიული კონტროლის მექანიზმების გამოყენების მიმართულებით რეკომენდაციების გაზიარება, მნიშვნელოვნად შეუწყობს ხელს ეროვნულ დონეზე კიბერსივრცის დაცულობასა და მის მდგრადობას.

იმის გათვალისწინებით, რომ საჯარო და კერძო უწყებების მონაწილეობით არსებული საკომუნიკაციო ჩარჩო არის ე.წ. "Ad hoc" სახის და არ გააჩნია სტრუქტურირებული ფორმა, ასევე, არ არის მკაფიოდ განსაზღვრული მისი მოქმედების არეალი, კიბერ და ინფორმაციული უსაფრთხოების ფორუმების, კონფერენციებისა და სხვა ღონისძიებების რეგულარულად ჩატარებისა და ინფორმაციის გაზიარების

გზით, უნდა მოხდეს საკომუნიკაციო არხების ინსტიტუციონალიზაცია, რაც, თავის მხრივ, ხელს შეუწყობს ეროვნულ დონეზე ქვეყნის კიბერშესაძლებლობების ამაღლებას.

საკომუნიკაციო პლატფორმის ერთ-ერთი ამოცანა, ასევე, უნდა იყოს მთავრობასა და კერძო სექტორს შორის კიბერდაზვერვითი (ე.წ. "threat intelligence") ინფორმაციის დროული და ეფექტიანი გაცვლა. აღნიშნული პლატფორმის ფარგლებში იარსებებს კონკრეტული მავნე პროგრამული საშუალებების შესახებ ინფორმაციისა და სხვა სახის მონაცემების გაცვლის შესაძლებლობაც (მაგ. MISP პლატფორმა).

ამოცანა 2.4: ეროვნული კიბერუსაფრთხოების მიზნების განსაზღვრა

სტრატეგიის ფარგლებში, ერთ-ერთ სამოქმედო მიმართულებად, შემუშავებული მეთოდოლოგიის საფუძველზე, ეროვნულ დონეზე კიბერუსაფრთხოების მიზნების განსაზღვრა არის გათვალისწინებული. ეროვნული კიბერუსაფრთხოების მიზნების ჩამოყალიბება ეროვნული დონის კიბერაქტორების მჭიდრო ურთიერთთანამშრომლობის ფარგლებში განხორციელდება. აღნიშნული ასპექტი, თემატურად, ასევე ეროვნული კიბერუსაფრთხოების ინდექსის შემუშავების საკითხს ეხმიანება. ზემოხსენებული ორი კომპონენტი (ეროვნული კიბერუსაფრთხოების მიზნები და ეროვნული კიბერუსაფრთხოების ინდექსი), რომლებთან მიმართებითაც კიბერუსაფრთხოების ეროვნული სტრატეგიის შესაბამისობის „შემოწმება" არის გათვალისწინებული, შეფასების გარკვეული დამატებითი მექანიზმის ნაწილს წარმოადგენს, რომელიც კიბერუსაფრთხოების სფეროში რეფორმის იმპლემენტაციას ხელს შეუწყობს.

ამოცანა 2.5: კიბერუსაფრთხოების სფეროში კვლევითი საქმიანობის მხარდაჭერა და გაძლიერება

სტრატეგიაში და შესაბამისად, სამოქმედო გეგმაში, განსაკუთრებით არის ხაზგასმული კიბერუსაფრთხოების სფეროში კვლევითი საქმიანობის მხარდაჭერისა და გაძლიერების მნიშვნელობა. შესაბამისად, აღნიშნული სამოქმედო მიმართულება, ცალკე კომპონენტად არის დოკუმენტ(ებ)ში გამოტანილი. გასათვალისწინებელია, რომ აღნიშნული არამარტო ეროვნულ დონეზე საკითხის მნიშვნელობამ, არამედ ასევე, საერთაშორისო დონორების რეკომენდაციამ განაპირობა (რომელიც, მაგ. ევროკავშირის TWINNING-ის პროექტის („კიბერუსაფრთხოების შესაძლებლობების გაძლიერება საქართველოში") ფარგლებში სტრატეგიის პროექტის შესწავლის შედეგად იქნა წარმოდგენილი).

აღნიშნულის გათვალისწინებით, საქართველოში კიბერუსაფრთხოების სფეროში კვლევითი საქმიანობის ხარისხის გაუმჯობესება, ერთ-ერთ პრიორიტეტულ მიმართულებად განისაზღვრა. შესაბამისი სამოქმედო მიმართულება სხვადასხვა აქტივობას მოიცავს (კვლევებისა და განვითარების ცენტრის შექმნა, უშუალოდ კვლევითი საქმიანობის განხორციელება და საერთაშორისო / ინსტიტუციური თანამშრომლობის განვითარება), რომელთა განხორციელებაშიც აქტორთა ფართო წრე იქნება ჩართული.

მიზანი 3: კიბერშესაძლებლობების განვითარება ძლიერი ადამიანური რესურსითა და სათანადო ტექნიკური უზრუნველყოფის საშუალებებით

წინამდებარე სტრატეგიის შემუშავების დროისთვის, ქვეყანაში არსებული მდგომარეობიდან გამომდინარე, გამოიკვეთა კიბერუსაფრთხოების სპეციალისტთა როგორც რაოდენობრივი სიმწირე, ისე კვალიფიკაციის ნაკლებობა. საქართველოს შრომით ბაზარზე კიბერუსაფრთხოების სპეციალისტების მიმართ მოთხოვნა მაღალია როგორც საჯარო, ისე კერძო სექტორში, თუმცა, ამ მოთხოვნას არსებული საკადრო რესურსი სრულად ვერ აკმაყოფილებს. საქართველოს კიბერუსაფრთხოების სისტემა ვერ იქნება მდგრადი, თუ ქვეყანაში არ იარსებებს კვალიფიციურ სპეციალისტთა გუნდი, რომელიც ფლობს კიბერსაფრთხეებსა და ინციდენტებთან გასამკლავებლად საჭირო ცოდნასა და გამოცდილებას. აქედან გამომდინარე, საქართველოს სტრატეგიული მიზანია, უზრუნველყოს თანამედროვე ტექნოლოგიებითა და უნარ-ჩვევებით აღჭურვილი სპეციალისტების მომზადება-გადამზადება კიბერუსაფრთხოების სფეროში არსებულ ყველა საკვანძო პოზიციაზე. მნიშვნელოვანია, შეიქმნას კიბერუსაფრთხოების სპეციალისტთა შესაძლებლობების განვითარების ერთიანი ჩარჩო და ე.წ. „Ad hoc" კვალიფიკაციის ასამაღლებელი აქტივობები ჩანაცვლდეს რეგულარული და სისტემური პოლიტიკით.

ამ მიზნით, მნიშვნელოვანია შეიქმნას კიბერსავარჯიშოების ჩატარების სიმულაციური პლატფორმა (Cyber Range), რაც მუდმივ ციკლზე დამყარებული სწავლებებით, ხელს შეუწყობს უწყებებს ინციდენტებზე რეაგირებისას კოორდინირებულ მუშაობაში და ცხადად გამოაჩენს პოტენციურ

საოპერაციო ხარვეზებს.

ადამიანური რესურსების კვალიფიკაციის ამაღლების გარდა, მნიშვნელოვანია ორგანიზაციულ დონეზე კიბერუსაფრთხოების უზრუნველმყოფი ძირითადი სუბიექტების გაძლიერება ტექნიკური და პროგრამული უზრუნველყოფის საშუალებებით.

ამოცანა 3.1: დარგის სპეციალისტების ცოდნისა და კვალიფიკაციის ამაღლება

აღნიშნული ამოცანის ფარგლებში უნდა განხორციელდეს ისეთი აქტივობები, რომლებიც უზრუნველყოფს როგორც საჯარო სექტორიდან, ისე კრიტიკული ინსფრასტრუქტურებიდან კიბერ და ინფორმაციული უსაფრთხოების, ასევე, კიბერდანაშაულისა და კიბერთავდაცვის სფეროს სპეციალისტებისთვის ცოდნისა და საკვალიფიკაციო მოთხოვნების ჩამოყალიბებას მათთვის ტრენინგებისა და სავარჯიშოების ჩატარების, სერტიფიცირების (მაგ.: ISO 9001, 22301, 27001 LI/LA, SANS, ISACA, NIST), სპეციალიზებული სასწავლო-სატრენინგო პროგრამების შემუშავებისა და დისტანციური სწავლების პლატფორმის განვითარების საშუალებით. ეს ყოველივე ხელს შეუწყობს სპეციალისტთა კვალიფიკაციის ამაღლებასა (მათ შორის, სპეციალისტთა რეზერვის, გამომძიებლების, პროკურორებისა და მოსამართლეებისთვის სატრენინგო პროგრამების შექმნას) და დარგის სპეციალისტთა რაოდენობის ზრდას. უნდა განისაზღვროს მარეგულირებლების როლი ცოდნისა და კვალიფიკაციის ამაღლების ამოცანის აქტივობების განხორციელებისას.

ამოცანა 3.2: ეროვნული კიბერშესაძლებლობების გაძლიერება ტექნიკური უზრუნველყოფის საშუალებებით

ცოდნისა და კვალიფიკაციის ამაღლების გარდა, მნიშვნელოვანია, რომ კიბერუსაფრთხოების სფეროს მთავარი მოთამაშეების (ეროვნული უსაფრთხოების საბჭო/ მისი აპარატი, სსიპ – ციფრული მმართველობის სააგენტო, სსიპ – კიბერუსაფრთხოების ბიურო, საქართველოს შინაგან საქმეთა სამინისტრო, სახელმწიფო უსაფრთხოების სამსახური, სსიპ საქართველოს ოპერატიულ-ტექნიკური სააგენტო, CERT/CSIRT-ები, ასევე, კრიტიკული ინფორმაციული სისტემის სუბიექტები) შესაძლებლობები გაძლიერდეს ტექნიკური და პროგრამული უზრუნველყოფის საშუალებებით, რათა მათ შეძლონ საკუთარი ფუნქციების ეფექტიანად განხორციელება. აღნიშნული ამოცანის ფარგლებში, კიბერუსაფრთხოების შესაძლებლობების განსავითარებლად უნდა განხორციელდეს, მათ შორის, ისეთი აქტივობები, როგორიცაა: კიბერუსაფრთხოების ლაბორატორიის, სიმულაციური პლატფორმა Cyber Range-ის და კიბერუსაფრთხოების ოპერაციების ცენტრის ჩამოყალიბება, საიდუმლო ინფორმაციის გაცვლის მიზნით საინფორმაციო-საკომუნიკაციო სისტემ(ებ)ის შექმნა.

მიზანი 4: კიბერუსაფრთხოების საერთაშორისო ასპარეზზე საქართველოს, როგორც უსაფრთხო და დაცული ქვეყნის როლის გაძლიერება

კიბერუსაფრთხოების სფეროში საქართველოს სურს სტრატეგიული პარტნიორობის გაღრმავება ორმხრივ (ევროკავშირის წევრ ქვეყნებსა და სხვა პარტნიორ ქვეყნებთან თანამშრომლობითი მემორანდუმების გაფორმება და სახელშეკრულებო ურთიერთობების დამყარება) და მრავალმხრივ ფორმატებში (EU, NATO, OSCE, UN, EaP, CoE, EUROPOL & INTERPOL, CEPOL, ENISA). კიბერსაფრთხეებსა და ინციდენტებთან გამკლავების პროცესში, მნიშვნელოვანია საერთაშორისო თანამეგობრობის მხარდაჭერის მოპოვების, საერთაშორისო ინიციატივებსა და პლატფორმებში საქართველოს ჩართულობის, ასევე, საქართველოს რეგიონის ლიდერად ჩამოყალიბების გზით, ქვეყნის პოზიციის განმტკიცება კიბერუსაფრთხოების საერთაშორისო ასპარეზზე. საქართველო გააგრძელებს აქტიურ მონაწილეობას ინტერნეტმმართველობის საერთაშორისო დიალოგსა და კოლექტიური კიბერუსაფრთხოების სხვა საერთაშორისო ინიციატივებში.

აღნიშნული მიზნის მისაღწევად ძირითად ამოცანებს წარმოადგენს:

ამოცანა 4.1 კიბერსაფრთხეებსა და ინციდენტებთან დაკავშირებულ ინფორმაციაზე წვდომის ზრდა და საერთაშორისო მხარდაჭერის/თანამშრომლობის გაძლიერება

საერთაშორისო ორგანიზაციებისა და პარტნიორი ქვეყნების მიერ აღმოჩენილ კიბერინციდენტებზე წვდომის მოპოვება და პოტენციურ საფრთხეებზე ინფორმაციის მიღება, ასევე, საერთაშორისო ექსპერტების ჩართვა საქართველოს კიბერსივრცეში მიმდინარე ინციდენტებთან გამკლავების

პროცესში, ისევე როგორც მნიშვნელოვანი კიბერუსაფრთხოების მოვლენის დროს საერთაშორისო პარტნიორების მხარდაჭერის მობილიზება, საქართველოს საშუალებას მისცემს, სწრაფად და ეფექტიანად გაუმკლავდეს მისი კიბერსივრცის წინააღმდეგ წარმოებულ ინციდენტებს და შედეგად, გახდეს მდგრადი კიბერშეტევების მიმართ.

ამოცანა 4.2 საერთაშორისო კიბერსწავლებებსა და კიბერსავარჯიშოებში ჩართულობის უზრუნველყოფა და ცოდნისა და გამოცდილების გაზიარება კიბერუსაფრთხოების გლობალურ დღის წესრიგში წვლილის შეტანისთვის

საქართველოს ჩართულობა საერთაშორისო ეგიდით გამართულ კიბერსავარჯიშოებსა და სხვადასხვა სახის სტრატეგიულ-ტექნიკურ სასწავლო-საგანმანათლებლო ინიციატივებში მნიშვნელოვნად შეუწყობს ხელს პროფესიული კადრების ცოდნის დონის ამაღლებასა და სხვა ქვეყნების პროფესიონალებთან მჭიდრო თანამშრომლობითი კავშირების დამყარებას. ამასთან, საქართველო აქტიურად გააგრძელებს მონაწილეობას კიბერუსაფრთხოების გლობალური დღის წესრიგის შექმნაში, ჩაერთვება ინტერნეტმმართველობის საერთაშორისო დიალოგის ჩამოყალიბებისა და ინტერნეტსივრცეში საერთაშორისო სამართლის გამოყენების პროცესებში.

ამოცანა 4.3 საერთაშორისო ორმხრივი და მრავალმხრივი ფორმატის პარტნიორობის გაძლიერება

საქართველოს რეგიონულ ჰაბად ჩამოყალიბება და რეგიონის მასშტაბით მისი, როგორც კიბერუსაფრთხოების წარმატებული რეფორმატორის როლის გაძლიერება ხელს შეუწყობს საერთაშორისო ასპარეზზე ქვეყნის სანდო და საიმედო პარტნიორად განხილვას საერთაშორისო თანამეგობრობის მიერ. ამ პროცესში მიზანშეწონილი იქნება, საქართველომ კავკასიის, ცენტრალური აზიისა და შავი ზღვის ქვეყნების შესაბამის უწყებებს გაუზიაროს საკუთარი გამოცდილება კიბერდანაშაულთან ბრძოლის, კიბერსაფრთხეების აღკვეთა-პრევენციისა და ელექტრონული მმართველობის მიმართულებით, ასევე, ჩაერთოს ამ კუთხით არსებულ ორმხრივ და მრავალმხრივ საერთაშორისო ინიციატივებში.

განხორციელება

სტრატეგიის პროექტს საქართველოს მთავრობას დასამტკიცებლად წარუდგენს ეროვნული უსაფრთხოების საბჭოსთან არსებული ეროვნული დონის კონცეპტუალური დოკუმენტების შემუშავების მაკოორდინირებელი მუდმივმოქმედი უწყებათაშორისი კომისია და მის განხორციელებას კოორდინაციას გაუწევს ეროვნული უსაფრთხოების საბჭოს აპარატი.

წინამდებარე სტრატეგიის იმპლემენტაციის მთავარ მექანიზმს წარმოადგენს თანდართული სამოქმედო გეგმა, რომლითაც განსაზღვრულია კონკრეტული ამოცანებისა და აქტივობების შესასრულებლად უფლებამოსილი პასუხისმგებელი უწყებები და შესაბამისი რესურსები. მოცემული სტრატეგიის სამოქმედო გეგმის განხორციელებაზე პასუხისმგებლები არიან კონკრეტული აქტივობის შესრულებაზე თავად სამოქმედო გეგმით ასეთად განსაზღვრული უწყებები. სამოქმედო გეგმით გათვალისწინებული კონკრეტული აქტივობის შესრულებაზე რამდენიმე პასუხისმგებელი უწყების განსაზღვრის შემთხვევაში, მთავარ პასუხისმგებელ უწყებას წარმოადგენს შესაბამის ჩამონათვალში პირველ ადგილზე მითითებული უწყება. დამხმარე უწყებები, ახორციელებენ პასუხისმგებელი სახელმწიფო ორგანოების საქმიანობის ხელშეწყობას კომპეტენციის იმ ფარგლებში, რასაც მოქმედი კანონმდებლობა აღნიშნულ უწყებებს სამოქმედო გეგმით გათვალისწინებულ საკითხებთან მიმართებით ანიჭებს. მთავარი პასუხისმგებელი უწყება უფლებამოსილია, დამხმარე ან/და სხვა პასუხისმგებელი უწყებების ჩართულობით შექმნას აქტივობის შესრულებისთვის სამუშაო ჯგუფი და წარმართოს მისი საქმიანობა.

საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგიის სამოქმედო გეგმით განსაზღვრულ პასუხისმგებელ უწყებებს ევალებათ შიდაუწყებრივი სამოქმედო გეგმების შემუშავება, რომლებიც განსაზღვრავს ამავე სამოქმედო გეგმით მათზე დაკისრებული ვალდებულებების შესრულების მექანიზმებსა და ეტაპებს.

სტრატეგიის განხორციელების ვადებია 2021-2024 წლები. სტრატეგიის განხორციელებისთვის განსაზღვრულია 3-წლიანი სამოქმედო გეგმა. კიბერუსაფრთხოების 2021-2024 წლების ეროვნული სტრატეგია და მისი სამოქმედო გეგმა განახლებადი დოკუმენტია და მისი იმპლემენტაციის შედეგად გამოვლენილი გამოწვევების საფუძველზე განხორციელდება შესაბამისი ცვლილებები.

სტრატეგიის სამოქმედო გეგმის განხორციელება ფინანსდება საქართველოს სახელმწიფო ბიუჯეტით, დონორი ორგანიზაციებისა და პარტნიორი ქვეყნების ფინანსური მხარდაჭერით.

მონიტორინგი და შეფასება

მონიტორინგი, ანგარიშგება და შეფასება სტრატეგიის განხორციელების პროცესის განუყოფელი ნაწილია და შესაბამისად, საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგიის შესრულების შედეგები, მათი ინდიკატორების საფუძველზე, ყოველწლიურად შეფასდება.

მონიტორინგი

სტრატეგიის ამოცანებით განსაზღვრული შედეგების მიღწევის პროგრესისა და სამოქმედო გეგმით განსაზღვრული აქტივობების განხორციელების თაობაზე ინფორმაციის შეგროვების მიზნით, ეროვნული უსაფრთხოების საბჭოს აპარატის მიერ ხორციელდება სტრატეგიის შესრულების მონიტორინგი.

მონიტორინგის პროცესი იწყება სტრატეგიის განხორციელების პარალელურად, კერძოდ აქტივობების განხორციელებასთან ერთად პასუხისმგებელი უწყებები აწარმოებენ მათ მიერ შესრულებული აქტივობების შესახებ ინფორმაციისა და მტკიცებულებების შეგროვებას, დახარისხებას და სტატუსანგარიშების ფორმით აწვდიან ეროვნული უსაფრთხოების საბჭოს აპარატს, რომელიც, თავის მხრივ, ამუშავებს მიღებულ ინფორმაციას და მის საფუძველზე, ყოველწლიურად ქმნის ერთ პროგრეს-(შუალედურ) და ერთ წლიურ ანგარიშს. მონიტორინგის როგორც შუალედური, ისე წლიური ანგარიში მოიცავს ძირითად ფაქტობრივ ინფორმაციას შესრულებული აქტივობებისა და განხორციელების დონის შესახებ.

ეროვნული უსაფრთხოების საბჭოს აპარატი უფლებამოსილია, დადგენილ ვადაზე ადრე, შესაბამისი სახელმწიფო უწყებ(ებ)იდან მოცემული სტრატეგიის სამოქმედო გეგმით განსაზღვრულ ცალკეულ აქტივობაზე გამოითხოვოს ინფორმაცია.

ეროვნული უსაფრთხოების საბჭოს აპარატი, მონიტორინგის ანგარიშებს აცნობს ეროვნული უსაფრთხოების საბჭოს, საქართველოს მთავრობისთვის წარსადგენად.

შეფასება

შეფასება არის სტრატეგიის განხორციელების ციკლის ბოლო ეტაპი, როდესაც დგინდება, თუ რამდენად წარმატებით, ეფექტიანად და სრულყოფილად განხორციელდა ის. შეფასება, ძირითადად, ორიენტირებულია უშუალოდ გრძელვადიანი შედეგებისა და სტრატეგიით გათვალისწინებული აქტივობების განხორციელების შეფასებაზე და ინფორმაციას გვაძლევს სტრატეგიის დოკუმენტში იდენტიფიცირებული მიზნების მიღწევისა და ამოცანების შესრულების შესახებ.

მონიტორინგის წლიური ანგარიშების საფუძველზე, თუ იკვეთება კონკრეტული მიმართულებით არსებული ჩავარდნები, ეროვნული უსაფრთხოების საბჭოს აპარატმა, შესაძლებელია მიიღოს მთელი სტრატეგიის ან მისი მხოლოდ ერთი ან რამდენიმე მიზნის მიღწევის შეფასების ჩატარების გადაწყვეტილება. ამგვარი გადაწყვეტილების მიღების შემთხვევაში, სტრატეგიის ლოგიკურ ჩარჩოსთან მიმართებით შეფასების დოკუმენტი უნდა მომზადდეს სტრატეგიის მონიტორინგის წლიური ანგარიშის მომზადებიდან 3 თვის ვადაში. ეროვნული უსაფრთხოების საბჭოს აპარატის მიერ შემუშავებული შეფასების საბოლოო ანგარიში მოიცავს დასკვნებსა და რეკომენდაციებს, რომლებიც გადაეცემა ეროვნული უსაფრთხოების საბჭოს საქართველოს მთავრობისთვის წარსადგენად.

---

[1] 2019 წლის ივნისის მონაცემებით, 2 700 000 (ორი მილიონ შვიდასი ათას) მოქალაქეზე მეტი ფლობს ელექტრონული პირადობის მოწმობას; ამას გარდა, ყოველდღიურად იზრდება ელექტრონული სერვისების ერთიანი პორტალის (Mygov.ge) მომხმარებელთა რიცხვი; 2019 წლის ივნისის მონაცემებით,

პორტალზე რეგისტრირებულია 100 000-ზე მეტი ფიზიკური და 1500-ზე მეტი იურიდიული პირი.

[2] BSA, Software Management: Security Imperative, Business Opportunity (BSA Global Software Survey, June 2018), გვ.10, ხელმისაწვდომია ბმულზე: https://www.bsa.org/files/2019-02/2018_BSA_GSS_Report_en_.pdf

დანართი №2

საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგიის სამოქმედო გეგმა

<table>
<tr><td colspan="2">მიზანი 1:</td><td colspan="5">ინფორმაციული საზოგადოებისა და ორგანიზაციების კიბერკულტურის განვითარება
და შესაძლებლობების გაძლიერება კიბერსივრცეში საფრთხეებსა და ინციდენტებთან
გამკლავების მიზნით</td><td>მდგრადი განვითარების მიზნებთან (SDGs) კავშირი</td></tr>
<tr><td colspan="2" rowspan="3">გავლენის ინდიკატორი 1.1:</td><td rowspan="3">საქართველოს ინფორმაციულ საზოგადოებაში კიბერკულტურის განვითარების დონე</td><td></td><td>საბაზისო</td><td>სამიზნე</td><td>დადასტურების წყარო</td></tr>
<tr><td>წელი</td><td>2019</td><td>2024</td><td rowspan="2">„ეროვნულ-დემოკრატიული ინსტიტუტის“ (NDI) ვებგვერდი</td></tr>
<tr><td>მაჩვენებელი</td><td>„ეროვნულ-დემოკრატიული ინსტიტუტის“ (NDI) მიერ ჩატარებული კვლევის მიხედვით, 90%-ზე მეტი კიბერსაფრთხეს არ განიხილავს საფრთხედ.</td><td>„ეროვნულ-დემოკრატიული ინსტიტუტის“ (NDI) მიერ ჩატარებული კვლევის მიხედვით, საქართველოში კიბერკულტურისა და განათლების დონე ამაღლებულია.</td></tr>
<tr><td colspan="2">ამოცანა 1.1:</td><td colspan="5">კიბერსივრცეში უსაფრთხოდ და დაცულად ფუნქციონირებისთვის სკოლის მოსწავლეებისა და სტუდენტებისთვის საჭირო უნარ-ჩვევების განვითარება და განათლების დონის ამაღლება</td></tr>
<tr><td colspan="2" rowspan="3">ამოცანის შედეგის ინდიკატორი 1.1.1:</td><td rowspan="3">საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებულ კვლევაში კიბერგანათლების ქვეკომპონენტის (3.2) შეფასება</td><td></td><td>საბაზისო</td><td>სამიზნე</td><td>დადასტურების წყარო</td></tr>
<tr><td>წელი</td><td>2019</td><td>2024</td><td rowspan="2">საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებული კვლევა</td></tr>
<tr><td>მაჩვენებელი</td><td>ჩამოყალიბების პროცესში (Formative)</td><td>წლისთვის ჩამოყალიბებული (Established)</td></tr>
<tr><td colspan="2">აქტივობა</td><td>აქტივობის შედეგის ინდიკატორი</td><td>დადასტურების წყარო</td><td>პასუხისმგებელი უწყება</td><td>პარტნიორი უწყება</td><td>შესრულების ვადა</td></tr>
<tr><td>1.1.1</td><td>ზოგადი განათლების სამივე საფეხურზე (დაწყებითი, საბაზო და საშუალო) „ციფრული მოქალაქეობის შესახებ სწავლების“ დანერგვა</td><td>1.1.1.1</td><td>„ციფრული მოქალაქეობა“ აღწერილია ეროვნულ სასწავლო გეგმაში და დანერგილია ზოგადი განათლების სამივე საფეხურზე.</td><td>ეროვნული სასწავლო გეგმების პორტალი - http://ncp.ge/</td><td>საქართველოს განათლებისა და მეცნიერების სამინისტრო</td><td>სსიპ – ციფრული მმართველობის სააგენტო;
საქართველოს კომუნიკაციების ეროვნული კომისია;
საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;</td><td>2024 წ.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>სსიპ – ციფრული მმართველობის სააგენტო;
საქართველოს ეკონომიკისა და მდგრადი განვითარების</td><td></td></tr>
</table>

						სამინისტრო;	
1.1.2	უმაღლეს საგანმანათლებლო დაწესებულებებში კიბერუსაფრთხოების სასწავლო კურსების დანერგვის ხელშეწყობა	1.1.2.1	უმაღლეს საგანმანათლებლო დაწესებულებებში დანერგილია კიბერუსაფრთხოების შესაბამისი სასწავლო კურსები	უმაღლესი საგანმანათლებლო დაწესებულებების ვებგვერდები	საქართველოს განათლებისა და მეცნიერების სამინისტრო	საქართველოს კომუნიკაციების ეროვნული კომისია; სახელმწიფო ინსპექტორის სამსახური; საქართველოს შინაგან საქმეთა სამინისტრო;	2024 წ.
1.1.3	მასწავლებლების, სკოლის ადმინისტრაციის წარმომადგენლებისა და მანდატურების სასწავლო პროგრამებში კიბერუსაფრთხოებასთან დაკავშირებული საკითხების ასახვა	1.1.3.1	მასწავლებლების, სკოლის ადმინისტრაციის წარმომადგენლებისა და მანდატურების სასწავლო პროგრამებში ასახულია კიბერუსაფრთხოებასთან დაკავშირებული საკითხები	შესაბამისი სასწავლო პროგრამები	საქართველოს განათლებისა და მეცნიერების სამინისტრო	სსიპ – ციფრული მმართველობის სააგენტო;	2023 წ.

ამოცანა 1.2:	კიბერსივრცეში უსაფრთხოდ და დაცულად ფუნქციონირებისთვის კიბერსაფრთხეებისა და რისკების შესახებ ინფორმაციული საზოგადოებისა და ორგანიზაციების ცნობიერების ამაღლება

ამოცანის შედეგის ინდიკატორი 1.2.1:	საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებულ კვლევაში ცნობიერების ამაღლების ქვეკომპონენტის (3.1) შეფასება.		საბაზისო	სამიზნე	დადასტურების წყარო
		წელი	2019	2024	საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებული კვლევა
		მაჩვენებელი	ჩამოყალიბების პროცესში (Start-up to Formative)	ჩამოყალიბებული (Established)	

აქტივობა		აქტივობის შედეგის ინდიკატორი		დადასტურების წყარო	პასუხისმგებელი უწყება	პარტნიორი უწყება	შესრულების ვადა
1.2.1	სამიზნე ჯგუფებში კიბერსაფრთხეების შესახებ ცნობიერების დონის განსაზღვრის მიზნით შესაბამისი კვლევის განხორციელება	1.2.1.1	ჩატარებულია კვლევა, რომლითაც შეფასდება ცნობიერების დონე კიბერსაფრთხეების შესახებ და მისი შედეგები წარედგინება შესაბამის უწყებებს.	ცნობიერების დონის განმსაზღვრელი კვლევა	სსიპ – ციფრული მმართველობის სააგენტო	საქართველოს განათლებისა და მეცნიერების სამინისტრო; საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო; საქართველოს კომუნიკაციების ეროვნული კომისია;	2022 წ. II კვ.
1.2.2							

						სსიპ – კიბერუსაფრთხოების ბიურო;		
						სახელმწიფო უსაფრთხოების სამსახური;		
						საქართველოს განათლებისა და მეცნიერების სამინისტრო;		
	ცნობიერების ამაღლების სტრატეგიის შემუშავება	1.2.2.1	სტრატეგია შექმნილია და შეთანხმებულია უწყებებს შორის.	სსიპ – ციფრული მმართველობის სააგენტოს ვებგვერდი	სსიპ – ციფრული მმართველობის სააგენტო	საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;	2022 წ. IV კვ.	
						საქართველოს კომუნიკაციების ეროვნული კომისია;		
						სახელმწიფო ინსპექტორის სამსახური;		
						საქართველოს შინაგან საქმეთა სამინისტრო;		

1.2.3	კიბერჰიგიენის დამატებითი სავალდებულო ტრენინგების ჩატარება საჯარო მოხელეებისთვის/ადმინისტრაციულ ორგანოებში დასაქმებულ პირებისათვის	1.2.3.1	სულ მცირე, 500-მა საჯარო მოხელემ/ადმინისტრაციულ ორგანოებში დასაქმებულმა პირმა გაიარა სავალდებულო ტრენინგები.	სსიპ საჯარო სამსახურის ბიუროს ვებგვერდი	სსიპ – ციფრული მმართველობის სააგენტო საჯარო სამსახურის ბიურო (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	სსიპ –კიბერუსაფრთხოების ბიურო; სახელმწიფო უსაფრთხოების სამსახური;	2024 წ. II კვ.
1.2.4		1.2.4.1	შემუშავებულია შესაბამისი საკანონმდებლო ცვლილებები „სახელმწიფო საიდუმლოების შესახებ“ საქართველოს კანონსა და მასთან დაკავშირებულ სხვა ნორმატიულ აქტებში შეტანისთვის.	საკანონმდებლო ცვლილებების პროექტი	სახელმწიფო უსაფრთხოების სამსახური	საქართველოს შინაგან საქმეთა სამინისტრო; სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო;	2023 წ.

	სახელმწიფო საიდუმლოებაზე დაშვების მქონე პირთა სავალდებულო ტრენინგებისა და ტესტირების სისტემის შემუშავება	1.2.4.2	შემუშავებულია შესაბამისი ტრენინგის კონცეფცია და კურიკულუმი სახელმწიფო საიდუმლოების შემცველი მონაცემების ინფორმაციული და საკომუნიკაციო ტექნოლოგიების მეშვეობით დამუშავების თაობაზე, რომლის შედეგადაც მნიშვნელოვნად გაზრდილია სახელმწიფო საიდუმლოებაზე დაშვების მქონე პირების კომპეტენციის დონე, რაც შემოწმებულია განსაზღვრული მეთოდოლოგი ით.	ტრენინგის კოცეფციისა და კურიკულუმის დოკუმენტები	სახელმწიფო უსაფრთხოების სამსახური	საქართველოს შინაგან საქმეთა სამინისტრო; სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო;	2024 წ. II კვ.

1.2.5	სამუშაო შეხვედრებისა და ტრენინგების ჩატარება მედიის წარმომადგენლებისთვის კიბერუსაფრთხოებასთან დაკავშირებული თემატიკის ხარისხიანი გაშუქების მიზნით	1.2.5.1	სულ მცირე, მედიის 30 წარმომადგენელი არის დატრენინგებული.	სსიპ – ციფრული მმართველობის სააგენტოს ვებგვერდი	სსიპ – ციფრული მმართველობის სააგენტო	საქართველოს კომუნიკაციების ეროვნული კომისია; ბიზნესომბუდსმენი; სსიპ –კიბერუსაფრთხოების ბიურო;	2023 წ. III კვ.
1.2.6	მცირე და საშუალო ბიზნესის წარმომადგენლებისთვის ცნობიერების ამაღლების კამპანიების ჩატარება	1.2.6.1	მცირე და საშუალო ბიზნესის, სულ მცირე, 50 წარმომადგენელი დატრენინგდა	სსიპ – ციფრული მმართველობის სააგენტოს ვებგვერდი	სსიპ – ციფრული მმართველობის სააგენტო	ბიზნესომბუდსმენი	2023 წ. III კვ.
1.2.7	საქართველოს დედაქალაქისა და რეგიონების მოსახლეობის ცნობიერების ამაღლების მიზნით საინფორმაციო კამპანიის ჩატარება	1.2.7.1	დედაქალაქსა და რეგიონებში მცხოვრები მოსახლეობისთვის ჩატარდა, სულ მცირე, 15 საინფორმაციო შეხვედრა.	სსიპ – ციფრული მმართველობის სააგენტოს ვებგვერდი	სსიპ – ციფრული მმართველობის სააგენტო	საქართველოს რეგიონული განვითარებისა და ინფრასტრუქტურის სამინისტრო	2024 წ. I-III კვ.
1.2.8	მაღალი რანგის თანამდებობის პირების ინფორმირების მიზნით კიბერუსაფრთხოების დაიჯესტის მიწოდება	1.2.8.1	შექმნილია კიბერუსაფრთხოების დაიჯესტი.	საჯარო სამსახურის ბიუროს ვებგვერდი	საჯარო სამსახურის ბიურო	სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო;	2021 წ.
		1.2.8.2	კიბერუსაფრთხოების დაიჯესტი სულ მცირე, ორჯერ მიეწოდათ მაღალი რანგის თანამდებობის პირებს.				2024 წ. II კვ.
						სსიპ – ციფრული მმართველობის სააგენტო; საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;	

1.2.9	ბავშვებისა და მოზარდებისთვის კიბერსივრცეში უსაფრთხოების შესახებ სახელმძღვანელოს შექმნა	1.2.9.1	სახელმძღვანელო შექმნილია, დაბეჭდილია და ხელმისაწვდომია მოსწავლეებისათვის როგორც ელექტრონულად ონლაინ სივრცეში, ისე ბეჭდური სახით.	საქართველოს განათლებისა და მეცნიერების სამინისტროს ვებგვერდი;	საქართველოს განათლებისა და მეცნიერების სამინისტრო	კომუნიკაციების ეროვნული კომისია; სახელმწიფო ინსპექტორის სამსახური; საქართველოს შინაგან საქმეთა სამინისტრო;	2023 წ.
1.2.10	კიბერბულინგთან დაკავშირებული საერთაშორისო-სამართლებრივი ბაზის შესწავლა და ანალიზი	1.2.10.1	შესწავლილია შესაბამისი საერთაშორისო-სამართლებრივი ბაზა და მომზადებულია ანალიტიკური დოკუმენტი	საერთაშორისო-სამართლებრივი ბაზის შესწავლის ანალიტიკური დოკუმენტი	საქართველოს შინაგან საქმეთა სამინისტრო; ეროვნული უსაფრთხოების საბჭოს აპარატი; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	საქართველოს განათლებისა და მეცნიერების სამინისტრო; სსიპ – ციფრული მმართველობის სააგენტო; საქართველოს კომუნიკაციების ეროვნული კომისია;	2024 წ. IV კვ.

1.2.11	საფრთხის შემცველი აპლიკაციებისა და თამაშების იდენტიფიცირებისა და მათ შესახებ საზოგადოების ცნობიერების ამაღლების მიზნით საჯარო-კერძო პარტნიორობის ფორმატის განსაზღვრა და რეკომენდაციების მომზადება	1.2.11.1	განისაზღვრება საჯარო-კერძო პარტნიორობის ფორმატი, რომელიც პასუხისმგებელი იქნება საფრთხის შემცველი აპლიკაციებისა და თამაშების იდენტიფიცირებაზე, მათ შესახებ საზოგადოების ცნობიერების ამაღლებაზე	სამუშაო შეხვედრების ანგარიშები	სსიპ – ციფრული მმართველობის სააგენტო		2023 წ.
		1.2.11.2	განსაზღვრული/იდენტიფიცირებული იქნება საფრთხის შემცველი აპლიკაციები და თამაშები.			საქართველოს კომუნიკაციების ეროვნული კომისია;	2024 წ. II კვ.
		1.2.11.3	ჩატარებული იქნება, სულ მცირე, 3 შეხვედრა საზოგადოების ცნობიერების ამაღლების მიზნით			საქართველოს განათლებისა და მეცნიერების სამინისტრო; საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო; სახელმწიფო ინსპექტორის სამსახური;	2024 წ. III კვ.
1.2.12	საერთო სარგებლობის დისტანციური სატრენინგო პლატფორმის ტექნიკური და შინაარსობრივი განვითარება	1.2.12.1	შექმნილია საერთო სარგებლობის პლატფორმა	სსიპ – ციფრული მმართველობის სააგენტოს ვებგვერდი	სსიპ – ციფრული მმართველობის სააგენტო		2022 წ.
		1.2.12.2	წლისთვის პლატფორმაზე განთავსებულია, სულ მცირე, 2 კურსი.			სსიპ –კიბერუსაფრთხოების ბიურო;	2023 წ.
		1.2.12.3	წლისთვის პლატფორმაზე განთავსებული კურსი გამოიყენა, სულ მცირე, 50-მა მომხმარებელმა.			სსიპ საჯარო სამსახურის ბიურო; საქართველოს განათლებისა და მეცნიერების სამინისტრო;	2023 წ. II კვ.

						სახელმწიფო ინსპექტორის სამსახური;	
1.2.13	GITI-ს ჩატარება	1.2.13.1	საანგარიშო პერიოდში GITI ტარდება ყოველწლიურად.	http://www.ictbc.ge/	სსიპ – ციფრული მმართველობის სააგენტო ICT ბიზნეს საბჭოსთან თანამშრომლობით	სსიპ –კიბერუსაფრთხოების ბიურო; საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;	2024 წ. IV კვ.

მიზანი 2:	კიბერუსაფრთხოების მმართველობითი სისტემის მდგრადობა და საჯარო-კერძო თანამშრომლობის გაძლიერება				მდგრადი განვითარების მიზნებთან (SDGs) კავშირი
გავლენის ინდიკატორი 2.1:	მმართველობითი სისტემის განგრძობადი ტრანსფორმაცია განაპირობებს კრიტიკული ინფრასტრუქტურების კიბერმდგრადობასა და საჯარო-კერძო პარტნიორობის გაძლიერებას.		საბაზისო	სამიზნე	დადასტურების წყარო
		წელი	2021	2024	საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებული კვლევა
		მაჩვენებელი	არსებული მმართველობითი მოდელი ვერ უზრუნველყოფს კრიტიკული ინფრასტრუქტურების უსაფრთხოებასა და მდგრად საჯარო-კერძო პარტნიორობას.	მმართველობითი სისტემა იქნება საფუძველი კრიტიკული ინფრასტრუქტურების დაცვისა და მდგრადი საჯარო-კერძო პარტნიორობის უზრუნველსაყოფად.	
ამოცანა 2.1:	ეროვნულ დონეზე კიბერინციდენტებისა და კიბერსაფრთხეების დროული გამოვლენის, რეპორტინგისა და მათთან ეფექტიანი გამკლავების სისტემის შექმნა და განვითარება				
ამოცანის შედეგის ინდიკატორი 2.1.1:			საბაზისო	სამიზნე	დადასტურების წყარო
		წელი	2019	2024	

	საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებულ კვლევაში ინციდენტებთან გამკლავების ქვეკომპონენტის (1.2) შეფასება	მაჩვენებელი	ჩამოყალიბების პროცესში (Formative)- ინციდენტებზე რეაგირების სისტემა არსებობს, თუმცა საჭიროებს დახვეწასა და შემდგომ განვითარებას.	ჩამოყალიბებული (Established) - რეაგირების სისტემა შექმნილია და პასუხისმგებლობები გაწერილია.		საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებული კვლევა

აქტივობა		აქტივობის შედეგის ინდიკატორი		დადასტურების წყარო	პასუხისმგებელი უწყება	პარტნიორი უწყება	შესრულების ვადა
2.1.1	NIS დირექტივასთან სსიპ – ციფრული მმართველობის სააგენტოს მიერ მიღებული ნორმატიული აქტების ჰარმონიზაცია	2.1.1.1	შესაბამისი ნორმატიული აქტები ჰარმონიზებულია NIS დირექტივასთან	ანალიზის დოკუმენტი	სსიპ – ციფრული მმართველობის სააგენტო;	ეროვნული უსაფრთხოების საბჭოს აპარატი; საქართველოს ეროვნული ბანკი;	2022 წ. IV კვ.
2.1.2	კრიტიკული ინფორმაციული სისტემის სუბიექტების განსაზღვრის წესისა და პროცედურების ჩამოყალიბება მათ შორის, ENISA-ს საგნობრივი რეკომენდაციების მხედველობაში მიღებით (იდენტიფიცირების მეთოდოლოგიის შემუშავება, ნუსხაში სუბიექტის შეყვანის	2.1.2.1	ჩამოყალიბებული (Established) - 2022 წლისთვის კრიტიკული ინფორმაციული სისტემის სუბიექტების განსაზღვრის მეთოდოლოგია შემუშავებულია.	საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებული	სსიპ – ციფრული მმართველობის სააგენტო; ეროვნული უსაფრთხოების საბჭოს აპარატი; სსიპ – საქართველოს ოპერატიულ-	სსიპ –კიბერუსაფრთხოების ბიურო; სახელმწიფო უსაფრთხოების სამსახური; საქართველოს ეროვნული ბანკი; საქართველოს ეკონომიკისა და მდგრადი	2021 წ.

	პროცედურის გაუმჯობესება)			კვლევა	ტექნიკური სააგენტო; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	განვითარების სამინისტრო; საქართველოს კომუნიკაციების ეროვნული კომისია; სემეკი;	
2.1.3	კიბერინციდენტების კლასიფიცირებისა და კატეგორიზაციის მეთოდოლოგიის შემუშავება/დამტკიცება და მათზე პასუხისმგებელი უწყებების იდენტიფიცირება	2.1.3.1	კიბერინციდენტების კლასიფიცირების მეთოდოლოგია შექმნილია, შეთანხმებულია, შემოწმებულია (სცენარების მეშვეობით), დანერგილია და პერიოდულად ხდება მისი გადახედვა.	საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებული კვლევა; სსიპ – საქართველოს საკანონმდებლო მაცნეს ვებგვერდი - www.matsne.gov.ge	ეროვნული უსაფრთხოების საბჭოს აპარატი	სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო; საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო უსაფრთხოების სამსახური;	2023 წ. I კვ.

2.1.4	კიბერუსაფრთხოების ოპერაციების ცენტრის/ცენტრების (CSOC) ჩამოყალიბება - 24/7	2.1.4.1	ინციდენტების მართვისა და მართვასთან დაკავშირებული კოორდინაციის ფუნქცია ხორციელდება შეთანხმებული პარამეტრების შესაბამისად.	კიბერუსაფრთხოების ოპერაციების ცენტრის/ცენტრების (CSOC) ვებგვერდები	სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო; სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)		2024 წ. IV კვ.
2.1.5						სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო; საქართველოს შინაგან საქმეთა სამინისტრო;	

	CERT/CSIRT-ებს, საქართველოს შინაგან საქმეთა სამინისტროს, კრიტიკული ინფორმაციული სისტემის სუბიექტებს, ინტერნეტ სერვის პროვაიდერებსა და სხვა პასუხისმგებელ უწყებებს შორის კიბერინციდენტებისა და კიბერსაფრთხეების შესახებ შეტყობინებისა და მათზე რეაგირების სამართლებრივი მექანიზმის შემუშავება, ინფორმაციის ურთიერთგაცვლის ერთიანი პლატფორმის შექმნა და განვითარება	2.1.5.1	ინფორმაციის ურთიერთგაცვლის ერთიანი პლატფორმა შექმნილია და მისი ფუნქციონირებისთვის საჭირო შესაბამისი სამართლებრივი მექანიზმები შემუშავებულია.	სსიპ – საქართველოს საკანონმდებლო მაცნეს ვებგვერდი - www.matsne.gov.ge	ეროვნული უსაფრთხოების საბჭოს აპარატი; სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	სახელმწიფო უსაფრთხოების სამსახური; საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო; საქართველოს კომუნიკაციების ეროვნული კომისია; სახელმწიფო ინსპექტორის სამსახური; საქართველოს ეროვნული ბანკი; სემეკი;	2023 წ. IV კვ.
2.1.6	კიბერუსაფრთხოებასთან დაკავშირებული მოვლენების განვითარების სცენარების გათვალისწინება საომარი, საგანგებო და კრიზისული სიტუაციების მართვის გეგმაში	2.1.6.1	კიბერუსაფრთხოებასთან დაკავშირებული მოვლენების განვითარების სცენარები ჩამოყალიბებულია და დანერგილია პრაქტიკაში, ასევე, შეთანხმებული პირობების თანახმად, გაიარა ტესტირება.	საომარი, საგანგებო და კრიზისული სიტუაციების მართვის გეგმა	ეროვნული უსაფრთხოების საბჭოს აპარატი	სსიპ – ციფრული მმართველობის სააგენტო; საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო უსაფრთხოების სამსახური; სსიპ –კიბერუსაფრთხოების ბიურო;	2023 წ. I კვ.

						საქართველოს თავდაცვის ძალები; საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;	
2.1.7	ევროკავშირთან ასოცირების შეთანხმებით აღებული ვალდებულებებისა და ePrivacy დირექტივის შესაბამისად, „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონში შესატანი ცვლილებების შესახებ შესაბამისი კანონპროექტის მომზადება	2.1.7.1	„ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონი ePrivacy დირექტივის მოთხოვნებთან შესაბამისობაში არის მოყვანილი	საქართველოს კომუნიკაციების ეროვნული კომისიის ვებგვერდი	საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო	საქართველოს კომუნიკაციების ეროვნული კომისია; სახელმწიფო უსაფრთხოების სამსახური; საქართველოს საგარეო საქმეთა სამინისტრო; სსიპ –კიბერუსაფრთხოების ბიურო;	2024 წ. I კვ.
2.1.8	ქსელში შიფრაციის მეთოდის (end-to-end encryption) გამოყენებაზე ტექნიკური კონტროლის განმახორციელებელი უწყების განსაზღვრა	2.1.8.1	ტექნიკური კონტროლის განმახორციელებელი უწყება გააკონტროლებს ქსელში შიფრაციის მეთოდის (end-to-end encryption) გამოყენებას.				2023 წ.

						სსიპ –კიბერუსაფრთხოების ბიურო;		
		2.1.8.2	შემუშავებულ იქნება კრიპტოგრაფიული კონტროლის (მათ შორის, სერტიფიკატების მართვის) მეთოდოლოგია და წარედგინება სამთავრობო უწყებებსა და კრიტიკული ინფორმაციული სისტემის სუბიექტებს.	კომპეტენციის შესაბამისად, თითოეული უწყების ვებგვერდი	სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო;	სსიპ – ციფრული მმართველობის სააგენტო; სახელმწიფო უსაფრთხოების სამსახური;	2024 წ.	

ამოცანა 2.2:	კიბერდანაშაულის წინააღმდეგ ბრძოლის ეფექტიანი სისტემის განვითარება					
ამოცანის შედეგის ინდიკატორი 2.2.1:	საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებულ კვლევაში კიბერდანაშაულის ქვეკომპონენტის (4.2) შეფასება		საბაზისო	სამიზნე		დადასტურების წყარო
		წელი	2019	2024		საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებული კვლევა
		მაჩვენებელი	ჩამოყალიბების პროცესში (Formative)	ჩამოყალიბებული (Established)		

აქტივობა		აქტივობის შედეგის ინდიკატორი		დადასტურების წყარო	პასუხისმგებელი უწყება	პარტნიორი უწყება	შესრულების ვადა
2.2.1	საგამოძიებო მოქმედებების განხორციელებისას მოპოვებული ელექტრონული (მათ შორის, პერსონალური მონაცემების შემცველი) მტკიცებულებების დამუშავებისა და მათთან მოპყრობის სამართლებრივი საფუძვლების ანალიზი და შესაბამისი საკანონმდებლო ცვლილებების მომზადება	2.2.1.1	შექმნილია შესაბამისი საკანონმდებლო ცვლილებების ამსახველი დოკუმენტი და წარდგენილია უწყებებისთვის შესათანხმებლად	საკანონმდებლო ცვლილებების ამსახველი დოკუმენტის უწყებებისთვის მიწოდების დამადასტურებელი წერილი/წერილები	საქართველოს გენერალური პროკურატურა ეროვნული უსაფრთხოების საბჭოს აპარატი; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო უსაფრთხოების სამსახური; სახელმწიფო ინსპექტორის სამსახური;	2023 წ. I კვ.
2.2.2	ელექტრონული მტკიცებულებების მოპყრობისა და კიბერდანაშაულის გამოძიების პროცესის ტექნოლოგიური მხარდაჭერა	2.2.2.1	შესაბამისი რგოლები აღჭურვილი არიან კიბერდანაშაულის გამოძიებისთვის საჭირო აპარატურული და პროგრამული უზრუნველყოფით	საქართველოს შინაგან საქმეთა სამინისტროს ვებგვერდი; აპარატურული და პროგრამული	საქართველოს შინაგან საქმეთა სამინისტრო		2023 წ. IV კვ.

				უზრუნველყოფის საშუალებებით აღჭურვის დამადასტურებელი დოკუმენტაცია;			
2.2.3	კიბერდანაშაულთან დაკავშირებული ციფრული ექსპერტიზისა და კიბერსაშუალებით ჩადენილი სხვა დანაშაულების კვლევის მიზნით სპეციალური ლაბორატორიის გაძლიერება	2.2.3.1	ლაბორატორია გაძლიერებულია, დაკომპლექტებულია შესაბამისი პერსონალით და აღჭურვილია სათანადო აპარატურით.	საქართველოს შინაგან საქმეთა სამინისტროს ვებგვერდი; აპარატურული საშუალებებით აღჭურვის დამადასტურებელი დოკუმენტაცია;	საქართველოს შინაგან საქმეთა სამინისტრო;	სახელმწიფო უსაფრთხოების სამსახური; სსიპ – ციფრული მმართველობის სააგენტო; სსიპ ლევან სამხარაულის სახელობის სასამართლო ექსპერტიზის ეროვნული ბიურო;	2024 წ. III კვ.
2.2.4	კიბერსივრცეში ბავშვთა უფლებების დარღვევის (მათ შორის, ბავშვთა მიმართ სექსუალური ექსპლუატაციის) პრევენციის მიზნით, შესაბამისი საერთაშორისო-სამართლებრივი მექანიზმების შესწავლა	2.2.4.1	შესწავლილია შესაბამისი საერთაშორისო-სამართლებრივი მექანიზმები კიბერსივრცეში ბავშვთა უფლებების დარღვევის (მათ შორის, ბავშვთა მიმართ სექსუალური ექსპლუატაციის) პრევენციის მიზნით	შესაბამისი საერთაშორისო-სამართლებრივი მექანიზმების შესწავლის ანალიტიკური დოკუმენტი;	საქართველოს შინაგან საქმეთა სამინისტრო; ეროვნული უსაფრთხოების საბჭოს აპარატი; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	საქართველოს განათლების და მეცნიერების სამინისტრო; სსიპ – ციფრული მმართველობის სააგენტო; საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;	2023 წ. IV კვ.

						კომუნიკაციების ეროვნული კომისია;	
2.2.5	ელექტრონულ მტკიცებულებებთან მოპყრობისა და კიბერდანაშაულის გამოძიების პროცესში ჩართული მხარეებისთვის სახელმძღვანელო მითითებების ჩამოყალიბება	2.2.5.1	სახელმძღვანელო მითითებები დამტკიცებულია შესაბამისი უფლებამოსილი ორგანოს მიერ.	სახელმძღვანელო მითითებების დამტკიცების თაობაზე მიღებული დოკუმენტი	საქართველოს გენერალური პროკურატურა ეროვნული უსაფრთხოების საბჭოს აპარატი; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო უსაფრთხოების სამსახური;	2023 წ. III კვ.
2.2.6	კიბერდანაშაულის ტენდენციებისა და კიბერდანაშაულის მართლმსაჯულებასთან (გამოძიება, პროკურატუ რა, სასამართლო) დაკავშირებული სტატისტიკური ინფორმაციის შეგროვება და ანალიზი	2.2.6.1	საანგარიშო პერიოდში ყოველწლიურად მოხდება კიბერდანაშაულის შესახებ სტატისტიკური ინფორმაციის შეგროვება, ანალიზი და ტენდენციების გაანალიზება, რათა გამოკვეთილი ტენდენციების საფუძველზე მიღებულ იქნას რელევანტური გადაწყვეტილებები მენეჯმენტის მიერ.	საქართველოს შინაგან საქმეთა სამინისტროს საქმიანობის ყოველწლიური ანგარიშები	საქართველოს შინაგან საქმეთა სამინისტრო		2024 წ. IV კვ.
2.2.7	კიბერინციდენტებისა და კიბერდანაშაულის თაობაზე შეტყობინების არსებული	2.2.7.1	30%-ით გაზრდილია კიბერინციდენტებისა და კიბერდანაშაულის თაობაზე	კვლევა კიბერინციდენტებისა და კიბერდანაშაულის	სსიპ – ციფრული მმართველობის სააგენტო; სახელმწიფო უსაფრთხოების სამსახური;		2024 წ. III კვ.

	მექანიზმის პოპულარიზაცია და მის შესახებ ცნობიერების ამაღლება		შეტყობინების მექანიზმის გამოყენების რიცხვი.	შესახებ შეტყობინების არსებული მექანიზმის თაობაზე	შინაგან საქმეთა სამინისტრო; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)		

ამოცანა 2.3:	ჩამოყალიბებული საკომუნიკაციო პლატფორმების გამოყენებით თანამედროვე ტენდენციების, საუკეთესო პრაქტიკისა და კიბერსაფრთხეების შესახებ ინფორმაციის გაცვლა და საერთაშორისო სტანდარტების დანერგვის ხელშეწყობა				
ამოცანის შედეგის ინდიკატორი 2.3.1:	საჯარო და კერძო ორგანიზაციებს შორის მიღწეული შეთანხმებები თანამედროვე ტენდენციების, საუკეთესო პრაქტიკისა და საერთაშორისო სტანდარტების დანერგვის შესახებ		საბაზისო	სამიზნე	დადასტურების წყარო
		წელი	2021	2024	ანგარიშები; რეკომენდაციები; შეთანხმებები;
		მაჩვენებელი	საერთაშორისო პრაქტიკის და ინფორმაციის გაცვლა არ არის სისტემატიზებული ხასიათის.	ინფორმაციის გაცვლას აქვს სისტემატიზებული/ინსტიტუციონალიზებული (ფორმალური) ხასიათი.	

აქტივობა		აქტივობის შედეგის ინდიკატორი		დადასტურების წყარო	პასუხისმგებელი უწყება	პარტნიორი უწყება	შესრულების ვადა
2.3.1		2.3.1.1	ფორუმის უფლებამოსილებები და მოქმედების სფერო განსაზღვრულია.				2023 წ.
		2.3.1.2	ფორუმის მმართველობითი ორგანო დაკომპლექტებულია.				2023 წ.
						სსიპ –კიბერუსაფრთხოების ბიურო; საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;	

	საჯარო და კერძო სექტორებს შორის კიბერუსაფრთხოების სფეროში თანამშრომლობისთვის საკომუნიკაციო პლატფორმის - კიბერუსაფრთხოების ფორუმის განვითარება	2.3.1.3	საანგარიშო პერიოდში ფორუმის მიერ, სულ მცირე, 2 რეკომენდაცია შემუშავებულია და მიწოდებულია შესაბამისი უწყებებისათვის.	ფორუმის ჩატარების დამადასტურებელი დოკუმენტაცია: წესდება, დღის წესრიგი, მონაწილეთა სია	სსიპ – ციფრული მმართველობის სააგენტო	შინაგან საქმეთა სამინისტრო; სახელმწიფო უსაფრთხოების სამსახური; საქართველოს კომუნიკაციების ეროვნული კომისია; სახელმწიფო ინსპექტორის სამსახური; ეროვნული უსაფრთხოების საბჭოს აპარატი;	2024 წ.
	საფრთხის შემცველი	2.3.2.1	მეთოდოლოგიის შემუშავებაზე პასუხისმგებელი უწყება განსაზღვრულია	საფრთხის შემცველი პროგრამული	ეროვნული უსაფრთხოების საბჭოს	სსიპ –კიბერუსაფრთხოების ბიურო; სსიპ – ციფრული მმართველობის სააგენტო; საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო უსაფრთხოების სამსახური;	2023 წ.

2.3.2	პროგრამული უზრუნველყოფის სიის (ე.წ. შავი სია) წარმოება და ინფორმაციის ხელმისაწვდომობა	2.3.2.2	საფრთხის შემცველი პროგრამული უზრუნველყოფის სია (ე.წ. შავი სია) ხელმისაწვდომია ყველა კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის.	უზრუნველყოფის სიის (ე.წ. შავი სია) წარმოებისა და ხელმისაწვდომობის დამადასტურებელი ინფორმაციული რესურსები.	აპარატი;	სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო; სახელმწიფო ინსპექტორის სამსახური; საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო; კომუნიკაციების ეროვნული კომისია;	2023 წ.
2.3.3	სამართალდამცავ და სახელმწიფო უსაფრთხოების სექტორში საჯაროდ ხელმისაწვდომი (open source) პროგრამული საშუალებების დანერგვა	2.3.3.1	სამართალდამცავ და სახელმწიფო უსაფრთხოების სექტორში სახელმწიფო კრიტიკული სისტემის სუბიექტთა საინფორმაციო და საკომუნიკაციო სისტემები, სადაც ეს შესაძლებელია, მთლიანად ეყრდნობა საჯაროდ ხელმისაწვდომ პროგრამულ სამუალებებს.	სამართალდამცავ და სახელმწიფო უსაფრთხოების სექტორში საჯაროდ ხელმისაწვდომი (open source) პროგრამული საშუალებების დანერგვის დამადასტურებელი დოკუმენტაცია	სახელმწიფო უსაფრთხოების სამსახური	საქართველოს შინაგან საქმეთა სამინისტრო; სსიპ – ციფრული მმართველობის სააგენტო;	2024 წ. III კვ.
			შიფრაციის (end-to-end encryption) და	შიფრაციის (end-to-end			

2.3.4	ქსელში შიფრაციის (end-to-end encryption) და კრიპტოგრაფიული კონტროლის ერთიანი სტანდარტის/ჩარჩოს შემუშავება და მისი დანერგვის ხელშეწყობა	2.3.4.1	კრიპტოგრაფიული კონტროლის ჩარჩო შემუშავებული და შეთანხმებულია შესაბამის უწყებებთან.	encryption) და კრიპტოგრაფიული კონტროლის ჩარჩოს უწყებებისათვის გაგზავნის დამადასტურებელი დოკუმენტი	სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო;	სსიპ –კიბერუსაფრთხოების ბიურო; სსიპ – ციფრული მმართველობის სააგენტო;	2024 წ. III კვ.
		2.3.4.2	2.3.4.1-ში განსაზღვრულ სამოქმედო გეგმაში მითითებული აქტივობების 70% შესრულდა.	შესრულების მონიტორინგის შედეგების ამსახველი დოკუმენტაცია (შესრულების ანგარიში).			
2.3.5	სახელმწიფო შესყიდვების პროცესსა და „მიწოდების ჯაჭვში“ (supply chain) ინფორმაციული ტექნოლოგიებისა და სისტემების, ასევე, სხვა პროდუქტებისა და მომსახურებების მიმართ ინფორმაციული და კიბერუსაფრთხოების მოთხოვნების გათვალისწინების შესახებ კვლევა და რეკომენდაციების შემუშავება	2.3.5.1	კვლევა ჩატარებულია;	საჯარო და კერძო სექტორის წარმომადგენლებისათვის რეკომენდაციების მიცემის დამადასტურებელი დოკუმენტაცია	ეროვნული უსაფრთხოების საბჭოს აპარატი	სსიპ – ციფრული მმართველობის სააგენტო; სახელმწიფო უსაფრთხოების სამსახური; სსიპ –კიბერუსაფრთხოების ბიურო; საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო ინსპექტორის სამსახური; საქართველოს განათლებისა და მეცნიერების სამინისტრო; სახელმწიფო შესყიდვების სააგენტო;	2023 წ.
		2.3.5.2	რეკომენდაციები კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ იქნა გამოყენებული პრაქტიკაში.				

2.3.6	საინფორმაციო და საკომუნიკაციო ტექნოლოგიების მომწოდებელთა და მომსახურების გამწევ კომპანიათა ე.წ. შავის სიის შემუშავება და მისი რეგულარული განახლება	2.3.6.1	განისაზღვრება კრიტერიუმები ე.წ. შავი სიის ფორმირებისთვის, რომელზე დაყრდნობითაც საქართველოს მთავრობა დაამტკიცებს საინფორმაციო და საკომუნიკაციო ტექნოლოგიების მომწოდებელთა და მომსახურების გამწევ კომპანიათა ნუსხას, რომლებთანაც კომერციული ურთიერთობა აეკრძალებათ კრიტიკული საინფორმაციო სისტემების სუბიექტებს.	www.matsne.gov.ge	ეროვნული უსაფრთხოების საბჭოს აპარატი; სსიპ –კიბერუსაფრთხოების ბიურო; სახელმწიფო უსაფრთხოების სამსახური; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	სსიპ – ციფრული მმართველობის სააგენტო;	2024 წ. III კვ.
2.3.7	ინფორმაციული უსაფრთხოების ექსპერტთა კლუბის/ ფორუმის განვითარება	2.3.7.1	ფორუმი იკრიბება წელიწადში, სულ მცირე, 4-ჯერ, ფორუმის წესდების შესაბამისად.	ფორუმის წესდება; ფორუმის დღის წესრიგი; დამსწრე პირთა სია; სსიპ – ციფრული მმართველობის სააგენტოს ვებგვერდი;	სსიპ – ციფრული მმართველობის სააგენტო	სსიპ –კიბერუსაფრთხოების ბიურო; სახელმწიფო უსაფრთხოების სამსახური; საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო ინსპექტორის სამსახური;	2024 წ. IV კვ.
		2.3.7.2	ფორუმის მუშაობაში, სულ მცირე, წელიწადში ერთხელ მონაწილეობს მოწვეული სტუმარი/დარგის ექსპერტი.				
	კიბერუსაფრთხოების სფეროში არსებული კურსების საერთაშორისო დონეზე აკრედიტება		სსიპ – ციფრული მმართველობის სააგენტოს ფარგლებში არსებულ სამ კურსს (100%) აქვს				

2.3.8		2.3.8.1	საერთაშორისო აკრედიტაცია	სასერტიფიკატო კურსების აკრედიტაციის დამადასტურებელი დოკუმენტაცია	სსიპ – ციფრული მმართველობის სააგენტო	სსიპ –კიბერუსაფრთხოების ბიურო; საქართველოს შინაგან საქმეთა სამინისტრო;	2024 წ. IV კვ.

ამოცანა 2.4:	ეროვნული კიბერუსაფრთხოების მიზნების განსაზღვრა

ამოცანის შედეგის ინდიკატორი 2.4.1:			საბაზისო	სამიზნე	დადასტურების წყარო
		წელი	2021	2023	
	ეროვნული კიბერუსაფრთხოების მიზნების განსაზღვრის მეთოდოლოგია შემუშავებულია.	მაჩვენებელი	ეროვნული კიბერუსაფრთხოების მიზნები არ არის ჩამოყალიბებული განსაზღვრული მეთოდოლოგიის მიხედვით.	ეროვნული კიბერუსაფრთხოების მიზნები განსაზღვრულია შემუშავებული მეთოდოლოგიის მიხედვით.	www.matsne.gov.ge

აქტივობა		აქტივობის შედეგის ინდიკატორი		დადასტურების წყარო	პასუხისმგებელი უწყება	პარტნიორი უწყება	შესრულების ვადა
2.4.1	ეროვნული კიბერუსაფრთხოების მიზნების განსაზღვრის მიდგომის (მეთოდოლოგიის) ჩამოყალიბება	2.4.1.1	მეთოდოლოგია ჩამოყალიბებულია და დადასტურებულია დაინტერესებული მხარეების მიერ.	მეთოდოლოგიის დოკუმენტი	სსიპ – ციფრული მმართველობის სააგენტო	სსიპ –კიბერუსაფრთხოების ბიურო; საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო	2022 წ. II კვ.

						უსაფრთხოების სამსახური; ეროვნული უსაფრთხოების საბჭოს აპარატი;	
2.4.2	ეროვნული კიბერუსაფრთხოების მიზნების ჩამოყალიბება	2.4.2.1	ჩამოყალიბებულია ეროვნული კიბერუსაფრთხოების მიზნები	კიბერუსაფრთხოების ეროვნული სტრატეგია	ეროვნული უსაფრთხოების საბჭოს აპარატი	სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო; საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო უსაფრთხოების სამსახური;	2022 წ. III კვ.
						სსიპ –კიბერუსაფრთხოების ბიურო;	

2.4.3	ეროვნული კიბერუსაფრთხოების ინდექსის და შესაბამისი კითხვარის შემუშავება.	2.4.3.1	შემუშავებულია ეროვნული კიბერუსაფრთხოების ინდექსის ფორმატი, თემები და მიმართულებები, კვლევის კითხვარი.	ეროვნული კიბერუსაფრთხოების ინდექსის დოკუმენტი, კითხვარი.	სსიპ – ციფრული მმართველობის სააგენტო	საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო უსაფრთხოების სამსახური; ეროვნული უსაფრთხოების საბჭოს აპარატი;	2022 წ. II კვ.
		2.4.3.2	კვლევა ჩატარებულია	კვლევის ანგარიში	სსიპ – ციფრული მმართველობის სააგენტო	სსიპ –კიბერუსაფრთხოების ბიურო; საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო უსაფრთხოების სამსახური; ეროვნული უსაფრთხოების საბჭოს აპარატი;	2022 წ. IV კვ.

		2.4.3.3	კიბერუსაფრთხოების ეროვნული სტრატეგია შესამბისობაშია ინდექსის კვლევის შედეგებთან და მიზნებთან.	კიბერუსაფრთხოების ეროვნული სტრატეგია	ეროვნული უსაფრთხოების საბჭოს აპარატი	სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო; საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო უსაფრთხოების სამსახური;	2023 წ. II კვ.

ამოცანა 2.5:	კიბერუსაფრთხოების სფეროში კვლევითი საქმიანობის მხარდაჭერა და გაძლიერება				
ამოცანის შედეგის ინდიკატორი 2.5.1:	საქართველოში კიბერუსაფრთხოების მიმართულებით კვლევითი საქმიანობის ხარისხი		საბაზისო	სამიზნე	დადასტურების წყარო
		წელი	2021	2024	საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი
		მაჩვენებელი	კიბერუსაფრთხოების სფეროში კვლევითი საქმიანობა ხორციელდება მცირე მოცულობით,	ჩამოყალიბებულია საჯარო-კერძო პარტნიორობა, რომლის ფარგლებშიც	

				თუმცა საჭიროებს დახვეწასა და შემდგომ განვითარებას.	რეგულარულად და სისტემურად ხორციელდება კვლევები		ჯგუფის მიერ განხორციელებული კვლევა
აქტივობა		აქტივობის შედეგის ინდიკატორი		დადასტურების წყარო	პასუხისმგებელი უწყება	პარტნიორი უწყება	შესრულების ვადა
2.5.1	კვლევებისა და განვითარების ცენტრის შექმნა და ორგანიზაციულ დონეზე გამართვა	2.5.1.1	ცენტრი შექმნილია და გააჩნია ყველა ორგანიზაციული, ტექნიკური და ფინანსური შესაძლებლობა კვლევების განსახორციელებლად	ამონაწერი ცენტრის რეგისტრაციის შესახებ, ცენტრის სტრატეგია და სამოქმედო გეგმა.	ეროვნული უსაფრთხოების საბჭოს აპარატი	სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო; სახელმწიფო უსაფრთხოების სამსახური; შინაგან საქმეთა სამინისტრო;	2023 წ. IV კვ.
2.5.2	კიბერუსაფრთხოების მიმართულებით კვლევითი საქმიანობის განხორციელება	2.5.2.1	ჩატარებული კვლევების რაოდენობა	ცენტრის ვებგვერდი	ეროვნული უსაფრთხოების საბჭოს აპარატი	სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო; სახელმწიფო უსაფრთხოების სამსახური; შინაგან საქმეთა სამინისტრო;	2023 წ. I კვ.

2.5.3	აღმოსავლეთ პარტნიორობის წევრ სახელმწიფოებთან / შესაბამის კვლევით ორგანიზაციებთან ინსტიტუციური თანამშრომლობა ერთობლივი პროექტების განხორციელების მიზნით	2.5.3.1	რეგიონული მასშტაბის კვლევითი პროექტების რაოდენობა	ცენტრის ვებგვერდი;	სსიპ – ციფრული მმართველობის სააგენტო; ეროვნული უსაფრთხოების საბჭოს აპარატი; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	სსიპ –კიბერუსაფრთხოების ბიურო; სახელმწიფო უსაფრთხოების სამსახური; შინაგან საქმეთა სამინისტრო; საქართველოს ეროვნული ბანკი;	2023 წ. II კვ.

მიზანი 3:	კიბერშესაძლებლობების განვითარება ძლიერი ადამიანური რესურსითა და სათანადო ტექნიკური უზრუნველყოფის საშუალებებით				მდგრადი განვითარების მიზნებთან (SDGs) კავშირი
გავლენის ინდიკატორი 3.1:	ადამიანური რესურსების ცოდნის, უნარების, გამოცდილებისა და ტექნიკური შესაძლებლობების დონე		საბაზისო	სამიზნე	დადასტურების წყარო
		წელი	2021	2024	საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებული კვლევა
		მაჩვენებელი	ადამიანური რესურსების ცოდნის, უნარების, გამოცდილებისა და ტექნიკური შესაძლებლობების დონე არ არის კიბერუსაფრთხოების ცვალებადი გარემოს ადეკვატური.	ადამიანური რესურსები აღჭურვილია შესაბამისი ტექნიკური საშუალებებით კიბერუსაფრთხოების სფეროში სერვისების მიწოდებისთვის.	
ამოცანა 3.1:	დარგის სპეციალისტების ცოდნისა და კვალიფიკაციის ამაღლება				
ამოცანის შედეგის ინდიკატორი 3.1.1:	საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებულ კვლევაში პროფესიონალთა კიბერგანათლების ქვეკომპონენტის (3.3) შეფასება		საბაზისო	სამიზნე	დადასტურების წყარო
		წელი	2019	2024	საქართველოში არსებული კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებული კვლევა
		მაჩვენებელი	საწყისი ეტაპი (Start-up)	ჩამოყალიბების პროცესში (Formative)	

აქტივობა		აქტივობის შედეგის ინდიკატორი		დადასტურების წყარო	პასუხისმგებელი უწყება	პარტნიორი უწყება	შესრულების ვადა
3.1.1	კრიტიკული ინფრასტრუქტურების კიბერუსაფრთხოების სპეციალისტებისთვის ცოდნისა და კვალიფიკაციის ეროვნული ჩარჩოს მომზადება (skill pipeline)	3.1.1.1	კიბერუსაფრთხოების სპეციალისტთა ცოდნისა და კვალიფიკაციის ჩარჩო მომზადებული და წარდგენილია კრიტიკული ინფრასტრუქტურებისათვის.	კიბერუსაფრთხოების სფეროში ადამიანური რესურსების მიმართ დადგენილი საკვალიფიკაციო მოთხოვნების დამადასტურებელი დოკუმენტი	ეროვნული უსაფრთხოების საბჭოს აპარატი; სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	სსიპ –კიბერუსაფრთხოების ბიურო; სსიპ – ციფრული მმართველობის სააგენტო; სახელმწიფო უსაფრთხოების სამსახური; საქართველოს შინაგან საქმეთა სამინისტრო; საჯარო სამსახურის ბიურო;	2023 წ. II კვ.
3.1.2	სსიპ – ციფრული მმართველობის სააგენტოს, სახელმწიფო უსაფრთხოების სამსახურის, სსიპ –კიბერუსაფრთხოების ბიუროს, საქართველოს	3.1.2.1	კიბერუსაფრთხოების სპეციალისტების 70 %	მონაწილეთა სია; ტრენინგების კურიკულუმი;	სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო; სახელმწიფო უსაფრთხოების სამსახური;	სსიპ თავდაცვის ინსტიტუციური	2024 წ. IV კვ.

	შინაგან საქმეთა სამინისტროს კიბერუსაფრთხოების სპეციალისტების გადამზადება/სწავლება		დატრენინგდა/გადამზადდა	სსიპ – ციფრული მმართველობის სააგენტოს ვებგვერდი	საქართველოს შინაგან საქმეთა სამინისტრო; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	აღმშენებლობის სკოლა;	
3.1.3	სახელმწიფო უსაფრთხოების სამსახურისა და სხვა ეროვნული უსაფრთხოების უწყებების შესაბამისი თანამშრომლებისთვის შიდა (in-house) კიბერ სასწავლო-საგანმანათლებლო ბაზის შექმნა და განვითარება	3.1.3.1	კიბერუსაფრთხოებასთან დაკავშირებული სპეციალური სასწავლო დისციპლინები შემუშავებული და დანერგილია.	სასწავლო-საგანმანათლებლო მასალები	სახელმწიფო უსაფრთხოების სამსახური		2024 წ. III კვ.

3.1.4	სავარჯიშოების ჩატარება კიბერუსაფრთხოების სფეროს სპეციალისტებისთვის (მაგ. CyberExe, CyberCube, იუმს შესავალი, იუმს-ის რისკების მართვა, იუმს-ის აუდიტი)	3.1.4.1	კიბერუსაფრთხოების სპეციალისტების ცოდნისა და კვალიფიკაციის ჩარჩოს საფუძველზე, მომზადდა სატრენინგო პროგრამა კიბერუსაფრთხოების სპეციალისტებისათვის და ჩატარდა, სულ მცირე, 3 სავარჯიშო	ტრენინგების კურიკულუმი; მონაწილეთა სია;	სსიპ – ციფრული მმართველობის სააგენტო	სსიპ –კიბერუსაფრთხოების ბიურო; სახელმწიფო უსაფრთხოების სამსახური;	2024 წ.
		3.1.4.2	ტრენინგებსა და სავარჯიშოებში კიბერუსაფრთხოების სფეროს სპეციალისტთა მონაწილეობა გაიზარდა, სულ მცირე, 20 %-ით.	სსიპ – ციფრული მმართველობის სააგენტოს ვებგვერდი			
3.1.5	ეროვნული დონის სამხედრო სავარჯიშოებში/სწავლებებში კიბერუსაფრთხოების კომპონენტის ინტეგრირება	3.1.5.1	კიბერუსაფრთხოების კომპონენტი სრულად ინტეგრირებულია ეროვნული დონის ყველა სტრატეგიული ხასიათის სამხედრო სავარჯიშოსა და სწავლებაში.	პრესრელიზი; თავდაცვის სამინისტროს ვებგვერდი;	სსიპ –კიბერუსაფრთხოების ბიურო	სსიპ – ციფრული მმართველობის სააგენტო; სახელმწიფო უსაფრთხოების სამსახური; საქართველოს შინაგან საქმეთა სამინისტრო;	2024 წ. IVკვ.
3.1.6	CYBER RANGE-პლატფორმის შექმნა	3.1.6.1	საანგარიშო პერიოდისთვის, პარტნიორების მხარდაჭერით, პლატფორმა შექმნილი და ფუნქციონალურია	თავდაცვის სამინისტროს ვებგვერდი, მონაწილეთა სია	სსიპ –კიბერუსაფრთხოების ბიურო	პარტნიორი ქვეყნები / საერთაშორისო ორგანიზაციები; სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო; სსიპ – ციფრული მმართველობის სააგენტო; სახელმწიფო ინსპექტორის სამსახური; საქართველოს კომუნიკაციების ეროვნული კომისია; საქართველოს ეროვნული ბანკი; სემეკი;	2024 წ.

						ეროვნული დონის კრიტიკული ინფორმაციული სისტემის სუბიექტები;	
3.1.7	კიბერრეზერვის პროექტის ინსტიტუციური განვითარება	3.1.7.1	საანგარიშო პერიოდისთვის ჩამოყალიბებულია რეზერვის მართვის ოპტიმალური მოდელი; გაწერილია რეზერვის კონცეფცია / ხედვა; შექმნილია / განახლებულია შესაბამისი საკანონმდებლო ბაზა	კიბერრეზერვთან დაკავშირებული ღია დოკუმენტები (კონცეფცია და ა.შ.)	სსიპ –კიბერუსაფრთხოების ბიურო; ეროვნული გვარდია;	საქართველოს თავდაცვის სამინისტრო; ეროვნული დონის კიბერაქტორები; ეროვნული დონის კრიტიკული ინფორმაციული სისტემის სუბიექტები;	2024 წ. IV კვ.
3.1.8	სპეციალური სატრენინგო პროგრამების დახვეწა გამომძიებლებისთვის ელექტრონული მტკიცებულებების მოპყრობისა და კიბერდანაშაულის გამოძიების პროცესში	3.1.8.1	სპეციალური სატრენინგო პროგრამები გამომძიებლებისთვის დანერგილია და გადამზადებულია გამომძიებელთა ჯგუფი.	სასწავლო-სატრენინგო მასალები	საქართველოს შინაგან საქმეთა სამინისტრო; სახელმწიფო უსაფრთხოების სამსახური;		2024 წ. III კვ.
3.1.9	საომარი, საგანგებო და კრიზისული სიტუაციების დროს კიბერუსაფრთხოებასთან დაკავშირებულ მოვლენათა განვითარების სცენარების გათვალისწინებით სავარჯიშოების ჩატარება (მათ შორის, კრიტიკული	3.1.9.1	საომარი, საგანგებო და კრიზისული სიტუაციების დროს კიბერუსაფრთხოებასთან დაკავშირებულ მოვლენათა განვითარების სცენარების გათვალისწინებით სავარჯიშოები ტარდება	შესაბამისი უწყებების ინფორმაციული რესურსები; სავარჯიშოების	ეროვნული უსაფრთხოების საბჭოს აპარატი	სახელმწიფო უსაფრთხოების სამსახური; სსიპ – ციფრული მმართველობის სააგენტო;	2024 წ. II კვ.

	ინფორმაციული სისტემების სუბიექტების ჩართულობით) და მათი შედეგების ანალიზი		ყოველწლიურად.	ჩატარების დამადასტურებელი მასალები.		სსიპ –კიბერუსაფრთხოების ბიურო; საქართველოს თავდაცვის ძალები;	

ამოცანა 3.2:	ეროვნული კიბერ შესაძლებლობების გაძლიერება ტექნიკური უზრუნველყოფის საშუალებებით					
ამოცანის შედეგის ინდიკატორი 3.2.1:			საბაზისო	სამიზნე	დადასტურების წყარო	
		წელი	2021	2024	„SAFE“[1]-ის ანგარიში; საერთაშორისო დახმარების პროექტების ანგარიშები	
	უფლებამოსილ სახელმწიფო უწყებათა ტექნოლოგიური შესაძლებლობების დონე	მაჩვენებელი	უფლებამოსილ სახელმწიფო უწყებებს აქვთ ინციდენტების მართვისთვის საჭირო მწირი ტექნოლოგიური შესაძლებლობები.	უფლებამოსილ სახელმწიფო უწყებებს აქვთ ინციდენტების მართვისთვის აუცილებელი თანამედროვე ტექნოლოგიური შესაძლებლობები.		

აქტივობა	აქტივობის შედეგის ინდიკატორი	დადასტურების წყარო	პასუხისმგებელი უწყება	პარტნიორი უწყება	შესრულების ვადა

3.2.1	უფლებამოსილი სახელმწიფო უწყებებისთვის ტექნიკური შესაძლებლობების შექმნა/განვითარება კრიტიკული ინფორმაციული სისტემების სუბიექტების ინფრასტრუქტურებში კიბერინციდენტებისა და კიბერსაფრთხეების მართვის მიზნით	3.2.1.1	იდენტიფიცირებული და მოთხოვნილი ინფრასტრუქტურული პროდუქტები შეძენილია და ინტეგრირებულია.	ინფრასტრუქტურული პროდუქტებით აღჭურვის დამადასტურებელი დოკუმენტაცია	სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო; სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	საქართველოს შინაგან საქმეთა სამინისტრო;	2024 წ. IV კვ.
3.2.2	კიბერთავდაცვითი შესაძლებლობების განვითარების მიზნით თავდაცვის სფეროში კიბერუსაფრთხოების ლაბორატორიის შექმნა	3.2.2.1	ლაბორატორია სრულად არის აღჭურვილი მოთხოვნილი ტექნიკური და პროგრამული საშუალებებით.	თავდაცვის სამინისტროს ვებგვერდი	სსიპ –კიბერუსაფრთხოების ბიურო		2022 წ. IVკვ.

მიზანი 4:	კიბერუსაფრთხოების საერთაშორისო ასპარეზზე საქართველოს, როგორც უსაფრთხო და დაცული ქვეყნის როლის გაძლიერება				მდგრადი განვითარების მიზნებთან (SDGs) კავშირი
გავლენის ინდიკატორი 4.1:	საქართველოს მიღწევები საერთაშორისო ასპარეზზე		საბაზისო	სამიზნე	დადასტურების წყარო
		წელი	2021	2024	ITU-ს გლობალური ინდექსი
		მაჩვენებელი	კიბერუსაფრთხოების გლობალურ დღის წესრიგში საქართველო არ არის მნიშვნელოვანი კონტრიბუტორი.	საქართველო პარტნიორი სახელმწიფოებისა და საერთაშორისო ორგანიზაციების მიერ აღიარებულია უსაფრთხო, დაცულ და სანდო ქვეყნად.	
გავლენის ინდიკატორი 4.2:	ITU-ს გლობალურ ინდექსში საქართველოს პოზიცია	მაჩვენებელი	2018 - ITU-ს გლობალურ ინდექსში საქართველო მსოფლიოს მასშტაბით არის მე-18, ხოლო რეგიონში (ევროპაში) - მე-9 ადგილზე.	ITU-ს გლობალურ ინდექსში საქართველო დაწინაურდა.	

ამოცანა 4.1:	კიბერსაფრთხეებსა და ინციდენტებთან დაკავშირებულ ინფორმაციაზე წვდომის ზრდა და საერთაშორისო მხარდაჭერის/თანამშრომლობის გაძლიერება					
ამოცანის შედეგის ინდიკატორი 4.1.1:	საქართველოს კიბერინციდენტებთან დაკავშირებულ ინფორმაციაზე წვდომისა და მხარდაჭერის საკითხზე საქართველოსა და პარტნიორ ქვეყნებს/საერთაშორისო ორგანიზაციებს შორის თანამშრომლობის ხარისხი		საბაზისო	სამიზნე		დადასტურების წყარო
		წელი	2021	2024		შესაბამისი სახელმწიფო უწყებების ანგარიშები
		მაჩვენებელი	დღეის მდგომარეობით, საქართველოსა და პარტნიორ ქვეყნებს/ საერთაშორისო ორგანიზაციებს შორის თანამშრომლობა არ არის საკმარისად ინტენსიური.	საქართველოსა და პარტნიორ ქვეყნებს/ საერთაშორისო ორგანიზაციებს შორის თანამშრომლობა გაღრმავებულია.		

აქტივობა		აქტივობის შედეგის ინდიკატორი		დადასტურების წყარო	პასუხისმგებელი უწყება	პარტნიორი უწყება	შესრულების ვადა
4.1.1	NATO-ს MISP პლატფორმის ეროვნულ დონეზე ინტეგრაცია	4.1.1.1	პლატფორმა ხელმისაწვდომია და ხორციელდება ინფორმაციის მიმოცვლა ეროვნული დონის აქტორებსა და NATO-ს შორის.	პრესრელიზი	სსიპ –კიბერუსაფრთხოების ბიურო;	სსიპ – ციფრული მმართველობის სააგენტო; სახელმწიფო უსაფრთხოების სამსახური; შინაგან საქმეთა სამინისტრო; საქართველოს ეროვნული ბანკი;	2024 წ.

4.1.2	საერთაშორისო CSIRT-ებთან (US CERT; DFN CERT) თანამშრომლობით ინციდენტების შესახებ ინფორმაციის მიღება	4.1.2.1	თანამშრომლობის ინტენსივობა გაზრდილია და საქართველოს გაფორმებული აქვს მემორანდუმი, სულ მცირე, US CERT-სა და DFN CERT-თან.	ანგარიშები, ერთობლივი პროექტები; მემორანდუმები/შეთანხმებები;	სსიპ – ციფრული მმართველობის სააგენტო;	სსიპ –კიბერუსაფრთხოების ბიურო; სახელმწიფო უსაფრთხოების სამსახური;	2024 წ. IV კვ.
ამოცანა 4.2:	საერთაშორისო კიბერსწავლებებსა და კიბერსავარჯიშოებში ჩართულობის უზრუნველყოფა და ცოდნისა და გამოცდილების გაზიარება კიბერუსაფრთხოების გლობალურ დღის წესრიგში წვლილის შეტანისთვის						
ამოცანის შედეგის ინდიკატორი				საბაზისო	სამიზნე		დადასტურების წყარო
4.2.1:	პარტნიორ სახელმწიფოებსა და საერთაშორისო ორგანიზაციებთან თანამშრომლობითი ურთიერთობების ხარისხი, რაც გამოიხატება მაღალი დონის მნიშვნელოვან საერთაშორისო ღონისძიებებში მონაწილეობაში.		წელი	2021	2024		ღონისძიებებში მონაწილეობის დამადასტურებელი ინფორმაცია/მასალები
			მაჩვენებელი	საქართველოს წარმომადგენლები ხშირად არასრულად, ad-hoc საფუძველზე და არარეგულარული ფორმით არიან წარმოდგენილნი საერთაშორისო ფორმატის სხვადასხვა ღონისძიებაში.	კიბერუსაფრთხოების სფეროში მომუშავე სხვადასხვა უწყების წარმომადგენლებს (სპეციალისტებს) მონაწილეობა ექნებათ მიღებული, სულ მცირე, 10 საერთაშორისო სავარჯიშოსა და კიბერსწავლებაში და 10 საერთაშორისო ღონისძიებაში/შეხვედრაში.		

აქტივობა		აქტივობის შედეგის ინდიკატორი		დადასტურების წყარო	პასუხისმგებელი უწყება	პარტნიორი უწყება	შესრულების ვადა
4.2.1	NATO-ს მიერ ორგანიზებულ კიბერსწავლება Cyber Coalition -ში მონაწილეობა	4.2.1.1	საქართველოს წარმომადგენლები ყოველწლიურად მონაწილეობენ Cyber Coalition-ში	მოწვევის წერილი;	სსიპ –კიბერუსაფრთხოების ბიურო;	სსიპ – ციფრული მმართველობის სააგენტო; სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო; სახელმწიფო უსაფრთხოების სამსახური;	2021-2024 წწ.
4.2.2	ლიეტუვის შეიარაღებული ძალების მიერ ორგანიზებულ კიბერსწავლება Amber Mist - ში მონაწილეობა	4.2.2.1	საქართველოს წარმომადგენლები ყოველწლიურად მონაწილეობენ Amber Mist - ში	მოწვევის წერილი;	სსიპ –კიბერუსაფრთხოების ბიურო;		2021-2024 წწ.
4.2.3	CCDCOE-ს მიერ ორგანიზებულ კიბერსწავლება Locked Shields - ში მონაწილეობა	4.2.3.1	საქართველოს წარმომადგენელი ყოველწლიურად მონაწილეობს კიბერსწავლება Locked Shields - ში	მოწვევის წერილი;	სსიპ –კიბერუსაფრთხოების ბიურო;		2021-2024 წწ.
4.2.4	Paintball-ში მონაწილეობა	4.2.4.1	საქართველოს წარმომადგენლე ბი, წელიწადში სულ მცირე ერთხელ, მონაწილეობენ Paintball-ში (აშშ)	მოწვევის წერილი; რეგისტრაციის დამადასტურებელი დოკუმენტი;	სსიპ –კიბერუსაფრთხოების ბიურო;		2024 წ. IV კვ.
4.2.5	Cyber Europe-ში მონაწილეობა	4.2.5.1	საანგარიშო პერიოდში საქართველოს წარმომადგენლებ მა, სულ მცირე, სამჯერ მიიღეს მონაწილეობა Cyber Europe-ში.	ღონისძიებებში მონაწილეობის დამადასტურებელი ინფორმაცია/მასალები	სსიპ – ციფრული მმართველობის სააგენტო; სსიპ –კიბერუსაფრთხოების ბიურო; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო;	2024 წ. IV კვ.

4.2.6	EuroDIG-სა და IGF-ში მონაწილეობა	4.2.6.1	საანგარიშო პერიოდში საქართველოს წარმომადგენლებ მა, სულ მცირე, სამჯერ მიიღეს მონაწილეობა EURODIG-ში		სსიპ – ციფრული მმართველობის სააგენტო; საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	საქართველოს კომუნიკაციების ეროვნული კომისია;	2024 წ. IV კვ.
		4.2.6.2	საანგარიშო პერიოდში საქართველოს წარმომადგენლებ მა, სულ მცირე, ორჯერ მიიღეს მონაწილეობა IGF-ში.	ღონისძიებებში მონაწილეობის დამადასტურებელი ინფორმაცია/მასალები			
4.2.7	UN GGE-ს სამუშაო შეხვედრებში მონაწილეობა	4.2.7.1	საანგარიშო პერიოდში საქართველოს წარმომადგენლებ მა, სულ მცირე, ერთხელ მიიღეს მონაწილეობა UN GGE-ს სამუშაო შეხვედრაში.	ღონისძიებებში მონაწილეობის დამადასტურებელი ინფორმაცია/მასალები	სსიპ – ციფრული მმართველობის სააგენტო;	საქართველოს საგარეო საქმეთა სამინისტრო; სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო;	2024 წ. IV კვ.
4.2.8	OSCE CBM მექანიზმში მონაწილეობის მიღება	4.2.8.1	საანგარიშო პერიოდში საქართველოს წარმომადგენლებ მა მონაწილეობა მიიღეს OSCE CBM მექანიზმის ყველა სამუშაო შეხვედრაში.	ღონისძიებებში მონაწილეობის დამადასტურებელი ინფორმაცია/მასალები	სსიპ – ციფრული მმართველობის სააგენტო;	საქართველოს საგარეო საქმეთა სამინისტრო; სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტო;	2024 წ. IV კვ.

ამოცანა 4.3:	საერთაშორისო ორმხრივი და მრავალმხრივი ფორმატის პარტნიორობის გაძლიერება

ამოცანის შედეგის ინდიკატორი 4.3.1:			საბაზისო	სამიზნე	დადასტურების წყარო
		წელი	2021	2024	ჩატარებული რეგიონული ღონისძიებების შესახებ ინფორმაციული რესურსები
	საქართველოს როლი რეგიონში	მაჩვენებელი	საქართველოს მიერ არ არის ინიცირებული რეგიონული თანამშრომლობითი პროექტები.	საქართველო ატარებს კიბერუსაფრთხოების სფეროში რეგიონულ ღონისძიებებს, სულ მცირე, წელიწადში ორჯერ.	

აქტივობა		აქტივობის შედეგის ინდიკატორი		დადასტურების წყარო	პასუხისმგებელი უწყება	პარტნიორი უწყება	შესრულების ვადა
4.3.1	საერთაშორისო პარტნიორების დახმარებით, საქართველოს კიბერუსაფრთხოების რეგიონულ ჰაბად ჩამოყალიბების კონცეფციის შემუშავება და	4.3.1.1	რეგიონულ ჰაბად ჩამოყალიბების კონცეფცია შემუშავებულია და უწყებათა მიერ შეთანხმებულია.	რეგიონული ჰაბის შესახებ შეთანხმება წევრ ქვეყნებს შორის	ეროვნული უსაფრთხოების საბჭოს აპარატი;	ეროვნული დონის კიბერაქტორები; შესაბამისი სახელმწიფო უწყებები; საქართველოს კომუნიკაციების ეროვნული კომისია; საქართველოს ეროვნული ბანკი; სემეკი; ეროვნული დონის კრიტიკული ინფორმაციული სისტემის სუბიექტები;	2024 წ.
		4.3.1.2	რეგიონული მასშტაბის, სულ მცირე, 1 პროექტი	პროექტის			

	ინიცირება		ინიცირებულია რეგიონული ჰაბის ფარგლებში.	დოკუმენტაცია		სამოქალაქო სექტორი; პარტნიორი ქვეყნები / საერთაშორისო ორგანიზაციები;	
4.3.2	კიბერუსაფრთხოების სფეროში საქართველოს მიღწევებისა და წარმატებული რეფორმების საერთაშორისო თანამეგობრობისათვის გაზიარება	4.3.2.1	საქართველოს წარმომადგენლებ მა მონაწილეობა მიიღეს, სულ მცირე, 5 საერთაშორისოდ აღიარებულ ღონისძიებაში (მაგ.: Cyber UK 2020).	ღონისძიებებში მონაწილეობის დამადასტურებელი ინფორმაცია/მასალები	ეროვნული უსაფრთხოების საბჭოს აპარატი;	ეროვნული დონის კიბერაქტორები; საქართველოს საგარეო საქმეთა სამინისტრო;	2024 წ. IV კვ.
	კიბერუსაფრთხოების საერთაშორისო ინდექსებში საქართველოს მიღწევებისა და რეფორმების წარმოჩენა	4.3.3.1	საანგარიშო პერიოდში ITU-ს გლობალურ ინდექსში საქართველო რეგიონის ლიდერი ქვეყანაა	ITU-ს გლობალური ინდექსი			

					სსიპ – ციფრული მმართველობის სააგენტო;	ეროვნული დონის კიბერაქტორები;	
4.3.3		4.3.3.2	კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებული კვლევის საფუძველზე, შესაძლებლობათა სიმწიფის მოდელის მიხედვით, საქართველოს შესაძლებლობები, სულ მცირე, ერთი პუნქტით გაუმჯობესდა თითოეული მიმართულებით.	კიბერუსაფრთხოების მდგომარეობის შესახებ ოქსფორდის შემფასებელი ჯგუფის მიერ განხორციელებული კვლევის ანგარიში	ეროვნული უსაფრთხოების საბჭოს აპარატი; (კომპეტენციის შესაბამისად, თითოეული წარმოადგენს წამყვან უწყებას)	საქართველოს საგარეო საქმეთა სამინისტრო; საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;	2024 წ. IV კვ.
4.3.4	საერთაშორისო კიბერფორუმ-ინტერმარიუმის ჩატარება	4.3.4.1	საანგარიშო პერიოდისთვის კიბერფორუმ-ინტერმარიუმის რეპუტაცია გაზრდილია, მასში დამატებით სამი ახალი საერთაშორისოდ აღიარებული, პროფილური ორგანიზაციის ჩართულობით.	მოწვევის წერილი, მონაწილეთა სია; რეგისტრაციის დამადასტურებელი დოკუმენტი;	სსიპ –კიბერუსაფრთხოების ბიურო;	ეროვნული დონის კიბერაქტორები;	2021-2024 წწ.

4.3.5	რეგიონალური კიბერთავდაცვის ცენტრში (RCDC-ლიეტუვა) გაწევრიანება	4.3.5.1	სსიპ – კიბერუსაფრთხოების ბიურო (საქართველოს წარმომადგენლობა) გაწევრიანებულია ცენტრში და მონაწილეობას იღებს დაგეგმილ ღონისძიებებში	ურთიერთთან ამშრომლობის მემორანდუმი	სსიპ –კიბერუსაფრთხოების ბიურო;		2022 წ.
4.3.6	საქართველოს კიბერუსაფრთხოების ფორუმის განვითარება	4.3.6.1	საანგარიშო პერიოდისთვის, საქართველოს კიბერუსაფრთხოების ფორუმის რეპუტაცია გაზრდილია, მასში დამატებით საერთაშორისოდ აღიარებული აქტორების ჩართულობით.	მონაწილეთა სია, რეგისტრაციის დამადასტურებელი დოკუმენტი.	ეროვნული უსაფრთხოების საბჭოს აპარატი	ეროვნული დონის კიბერაქტორები; შესაბამისი სახელმწიფო უწყებები; საქართველოს კომუნიკაციების ეროვნული კომისია; საქართველოს ეროვნული ბანკი; სემეკი; ეროვნული დონის კრიტიკული ინფორმაციული სისტემის სუბიექტები; სამოქალაქო სექტორი; პარტნიორი ქვეყნები/საერთაშორისო ორგანიზაციები.	2021-2024 წწ.

[1] EU4 Security, Accountability and Fight against Crime in Georgia (SAFE)