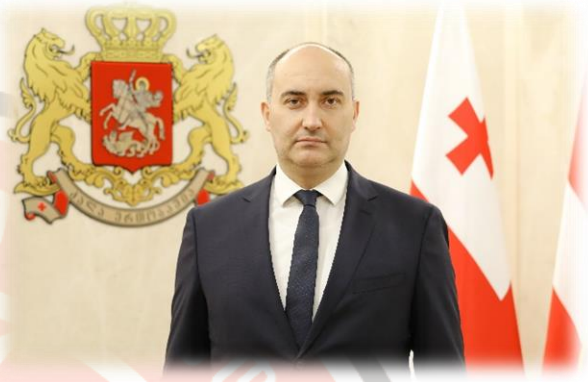
კიბერუსაფრთხოების ბიურო

საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების სტრატეგია

2021-2024

სარჩევი

თავდაცვის მინისტრის მიმართვა



საქართველოს თავდაცვის სამინისტროს საქმიანობის თითქმის ყველა ასპექტი, იქნება ეს საბრძოლო მომზადება, ოპერაციების დაგეგმვა, სამხედრო წვრთნების ჩატარება, ლოჯისტიკური უზრუნველყოფა თუ ყოველდღიური საქმიანობა, მნიშვნელოვნად არის დამოკიდებული ინფორმაციული და საკომუნიკაციო სისტემების უსაფრთხო და გამართულ ფუნქციონირებაზე. შესაბამისად, აღნიშნული სისტემების კიბერუსაფრთხოების უზრუნველყოფა მშვიდობიან, საგანგებო და საომარი ვითარების დროს, წარმოადგენს საქართველოს თავდაცვის სამინისტროს ერთ-ერთ სტრატეგიულ მიზანს.

გარდა ამისა, კიბერუსაფრთხოებას უაღრესად დიდი მნიშვნელობა ენიჭება ე.წ. ჰიბრიდულ საფრთხეებთან გამკლავების საქმეში. სწრაფი ტექნოლოგიური წინსვლისა და უსაფრთხოების სულ უფრო რთული ვითარების ფონზე, ჰიბრიდული საფრთხეები კვლავ განაგრძობენ დომინირებას. ჰიბრიდული საშუალებების ფართო მასივიდან, კიბერკომპონენტი აქტიურად გამოიყენება დივერსიებისთვის, შპიონაჟისა და ფსიქოლოგიური ოპერაციებისთვის.

ზემოაღნიშნულის გათვალისწინებით, დღის წესრიგში დგება თავდაცვის უწყების კიბერუსაფრთხოების შესაძლებლობების თანმიმდევრული განვითარების აუცილებლობა, რაც საჭიროებს კომპლექსურ დაგეგმვასა და სათანადო აღსრულებას.

კიბერუსაფრთხოების სტრატეგია, საშუალოვადიანი პერიოდისათვის, ითვალისწინებს კრიტიკულად მნიშვნელოვანი მიმართულებების გაძლიერებას, რაც საქართველოს თავდაცვის სამინისტროს კიბერშესაძლებლობების ნატოსა და ევროკავშირის სტანდარტებთან მისადაგების კუთხით ქმნის სოლიდურ წინაპირობას.

ჯუანშერ ბურჭულაძე

საქართველოს თავდაცვის მინისტრი

შესავალი

საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების სტრატეგია (შემდგომ - სტრატეგია) და სამოქმედო გეგმა წარმოადგენს საშუალოვადიან დოკუმენტს, რომელიც განსაზღვრავს საქართველოს თავდაცვის სფეროს კიბერუსაფრთხოების განვითარების მიმართულებებს, მიზნებსა და ამ მიზნების მიღწევისთვის საჭირო ამოცანებს.

სტრატეგია თავსებადია ისეთ მნიშვნელოვან კონცეპტუალურ დოკუმენტებთან, როგორიცაა, „ეროვნული უსაფრთხოების კონცეფცია“, „საფრთხეების შეფასების დოკუმენტი“, „საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგია“, „თავდაცვის სამინისტროს ხედვა 2030“ და „თავდაცვის სტრატეგიული მიმოხილვა 2021-2025” (თსმ) დოკუმენტი.

სამინისტროსა და მის სისტემაში შემავალ სტრუქტურულ ერთეულებში (შემდგომ - სამინისტრო) კიბერუსაფრთხოების გაძლიერება და პერსონალისთვის უსაფრთხო გარემოს შექმნა მოითხოვს სისტემურ მიდგომას და კიბერთავდაცვითი პოლიტიკის პროაქტიულად წარმართვას. შესაბამისად, სტრატეგია და თანმდევი სამოქმედო გეგმა, წლების განმავლობაში, ეროვნულ, უწყებრივ თუ საერთაშორისო დონეზე დაგროვილი გამოცდილების გაზიარებითა და არსებული თუ სამომავლო გამოწვევების გაანალიზების საფუძველზე, აყალიბებს სტრატეგიულ მიზნებსა და მიზნების მიღწევის აქტივობებს, რაც, საბოლოო ჯამში, აძლიერებს და სრულყოფს სამინისტროს კიბერუსაფრთხოებას.

სტრატეგიით გათვალისწინებული მიზნების მიღწევა ხელს შეუწყობს, საქართველოს თავდაცვის ძალების მიერ ოპერაციებში კიბერელემენტების უფრო ფართოდ ინტეგრირებას და გაზრდის კიბერპოტენციალს სამხედრო მიმართულებით.

არსებული ვითარება

სტრატეგიის შექმნის აქტუალობა განპირობებულია თავდაცვის სფეროში ინფორმაციული და საკომუნიკაციო ტექნოლოგიების განვითარებითა და კიბერშეტევების მზარდი დინამიკით. სამინისტროში მიმდინარე ინსტიტუციური ცვლილებების შედეგად, ხდება საქმიანობის ავტომატიზაცია და გაციფრულება, ინერგება მართვის ერთიანი, ცენტრალიზებული სისტემები. ეს პროცესი, ერთი მხრივ, ხელს უწყობს მართვისა და კომუნიკაციის ეფექტური მოდელების ჩამოყალიბებას, თუმცა, მეორე მხრივ, საგრძნობლად იზრდება კიბერშეტევების ალბათობა და ინფორმაციული სისტემის კომპრომეტირების რისკები.

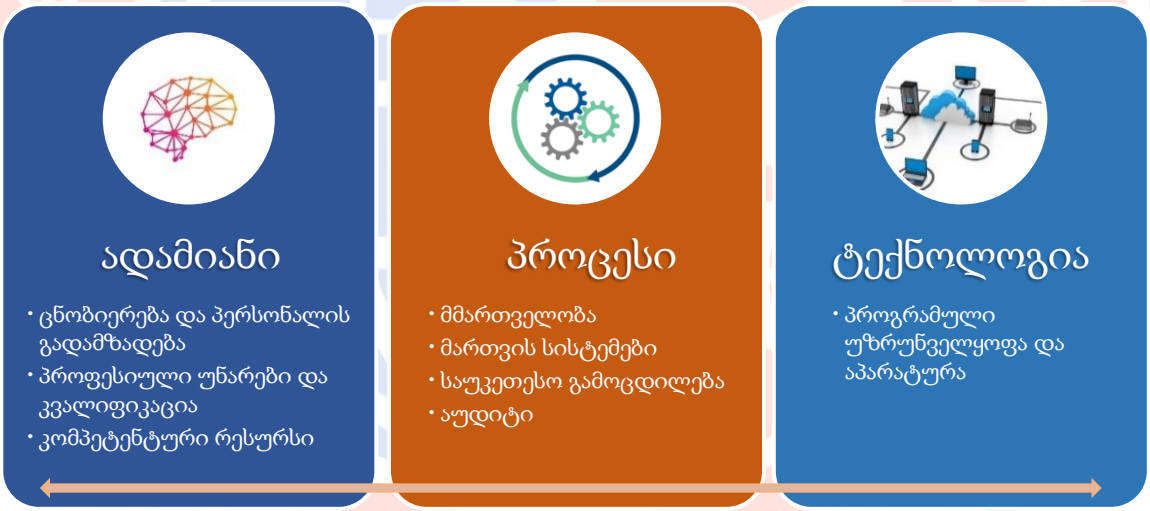
კიბერ/ინფორმაციული უსაფრთხოების სფეროში საუკეთესო პრაქტიკის გააზრებისა (ISO, NIST, CIS ა.შ) და ამ მიმართულებით სამინისტროში არსებული სიტუაციური ანალიზის საფუძველზე, გამოიკვეთა ცვლილებებისა და არსებული მიდგომების გაუმჯობესების საჭიროება, რამაც უნდა უზრუნველყოს პროცესების დაგეგმვის, მართვისა და მონიტორინგის ეფექტური და ეფექტიანი მოდელების ჩამოყალიბება.

არასათანადოდ მართული კიბერსივრცე წარმოშობს მნიშვნელოვან გამოწვევებს და სერიოზული რისკების წინაშე აყენებს სამინისტროს. კიბერთავდამსხმელების მხრიდან ინფორმაციულ სისტემებზე არასანქცირებული წვდომის შედეგად, შესაძლებელია კონფიდენციალური ინფორმაციის გადინება და სხვადასხვა სახის სადაზვერვო-დივერსიული ქმედებების განხორციელება, რაც საბოლოოდ მიზნად ისახავს საქართველოს თავდაცვისუნარიანობის დაქვეითებასა და ქვეყნის საერთაშორისო თანამეგობრობისადმი არასათანადო პარტნიორად წარმოჩენას.

2024 წლამდე განსახორციელებელი მიზნები - ადამიანი, პროცესი, ტექნოლოგია

ადამიანი საკუთარი ინტელექტუალური რესურსით ახორციელებს სხვადასხვა საქმიანობას, პროცესები ამ საქმიანობას უფრო ეფექტურს ხდიან, ტექნოლოგია კი პროცესების ავტომატიზაციის და ოპტიმიზაციის საშუალებას იძლევა. ამ დებულების ჭრილში კიბერუსაფრთხოების ვიწრო ტექნიკური მიმართულებიდან სტრატეგიული დონის სისტემამდე ტრანსფორმაცია მოითხოვს კომპლექსურ მიდგომას. სტრატეგიაში კიბერუსაფრთხოება და მასთან დაკავშირებული სტრატეგიული მიზნები განხილულია ზემოხსენებულ ურთიერთდაკავშირებულ მიმართულებათა ჭრილში.

სტრატეგიის ფარგლებში ფორმულირებული მიზნები ემსახურება კიბერშესაძლებლობების ზრდას შემდეგი სამი მიმართულებით:



ადამიანი - ადამიანი წარმოადგენს კიბერუსაფრთხოების ერთ-ერთ კრიტიკულ კომპონენტს. მის მიერ ხდება ორგანიზაციული პროცესების დაგეგმვა, მართვა, მონიტორინგი და შეფასება. აღნიშნული კომპონენტი აერთიანებს ადამიანურ ფაქტორს, განურჩევლად მათი როლისა და პასუხისმგებლობისა;

პროცესი - აღნიშნული კომპონენტი მოიცავს ყველა სახის ბიზნესპროცესს, რომელიც ემსახურება ორგანიზაციის მიერ დასახული სტრატეგიული მიზნებისა და ამოცანების შესრულებას;

ტექნოლოგია - ტექნოლოგიური კომპონენტი შედგება აპარატული და პროგრამული უზრუნველყოფისგან, რაც ერთიანობაში წარმოადგენს კიბერუსაფრთხოების უზრუნველყოფის უმნიშვნელოვანეს მდგენელს.

ზემოაღნიშნული მიმართულებებით წარმატების მიღწევა დაკავშირებულია კონკრეტული აქტივობების განხორციელებასთან. შესაბამისად, კიბერუსაფრთხოების განზომილებაში არსებული ტენდენციებისა და სამინისტროს წინაშე მდგარი გამოწვევების გათვალისწინებით, 2024 წლის ბოლომდე სამინისტრო გააუმჯობესებს კიბერუსაფრთხოებას სამი მიმართულებით და ყურადღებას გაამახვილებს შემდეგი სტრატეგიული მიზნების მიღწევაზე:

1. ადამიანური კაპიტალის განვითარება;

2. პროცესების ინსტიტუციონალიზაცია და მართვის ეფექტიანობის ზრდა;

3. ტექნოლოგიური მდგრადობის უზრუნველყოფა.

მეთოდოლოგია და რესურსები

სტრატეგია ითვალისწინებს ოქსფორდის უნივერსიტეტის კიბერუსაფრთხოების გლობალური ცენტრის (The Global Cyber Security Capacity Centre), აშშ-ს ჯორჯიის შტატის ეროვნული გვარდიისა და საერთაშორისო პარტნიორი ორგანიზაციების მიერ მომზადებულ კიბერთავდაცვით რეკომენდაციებს, ასევე, ახდენს პრობლემების იდენტიფიცირებას და აყალიბებს მათი გადაჭრის მკაფიოდ ფორმულირებულ მიზნებს, ამოცანებსა და აქტივობებს.

სტრატეგიის სამოქმედო გეგმით გათვალისწინებული სამიზნე მაჩვენებლებისა და კონკრეტული აქტივობების შესრულების ეფექტიანობის გასაზომად გამოიყენება შესრულების შეფასების ინდიკატორი (KPI), რაც უზრუნველყოფს რისკებზე დაფუძნებულ დაგეგმვას, პროცესების წარმატებით ორგანიზებასა და ეფექტურ მონიტორინგს.

სტრატეგიით განსაზღვრული აქტივობების განხორციელებისთვის გამოყენებული იქნება როგორც ადამიანური, ასევე ფინანსური რესურსი. იმ აქტივობების შესრულება, რომელთა განხორციელება მოითხოვს

მატერიალურ და ფინანსურ რესურსს, მოხდება სსიპ კიბერუსაფრთხოების ბიუროსთვის გამოყოფილი საბიუჯეტო თანხებითა და პარტნიორი ქვეყნების/დონორი ორგანიზაციების ფინანსური მხარდაჭერით.

ადამიანური რესურსი

სტრატეგიაში ნახსენები მიმართულებების განხორციელება საჭიროებს სათანადოდ მომზადებულ ადამიანურ რესურსს, რაც, ღონისძიებების წარმატებული მართვით, უზრუნველყოფს საბოლოო მიზნის მიღწევას. კიბერუსაფრთხოების ბაზარზე არსებული მაღალი კონკურენციის გათვალისწინებით, კვალიფიციური კადრების მობილიზება და მათი შენარჩუნება წარმოადგენს საყოველთაო გამოწვევას, თუმცა, მიუხედავად ამისა, სამინისტროს მხარდაჭერით სსიპ კიბერუსაფრთხოების ბიურომ კადრების მოზიდვა/განვითარებაში განახორციელა სათანადო ინვესტირება, რაც ითვალისწინებს სახელფასო ბადის კონკურენტულ პირობებთან მიახლოებას და წარმატებულ საკადრო პოლიტიკას.

სსიპ კიბერუსაფრთხოების ბიურო, სტრატეგიულ პარტნიორებთან/ორგანიზაციებთან (US, UK, EST, LITH, NATO, EU) მჭიდრო და ნაყოფიერი კომუნიკაციით, თანამშრომელთა სისტემური გადამზადების გზით, ასევე უზრუნველყოფს ორგანიზაციული კომპეტენციის ზრდას. მოცემული მომენტისათვის სსიპ კიბერუსაფრთხოების ბიუროს პერსონალის კომპეტენცია შეესაბამება ისეთ საერთაშორისო სტანდარტებს როგორიცაა: ISO, NIST, SANS.

სტრატეგია ადამიანურ რესურსებში მოიაზრებს არამხოლოდ სსიპ კიბერუსაფრთხოების ბიუროს კვალიფიციურ კადრებს, არამედ სტრატეგიის მიზნებსა და აქტივობებში ჩართული სამინისტროს ადამიანურ შესაძლებლობებს, ასევე, იმ პარტნიორი ქვეყნების/ორგანიზაციების ექსპერტულ ხარისხს, რაც საჭიროა კონკრეტული მიზნისა თუ აქტივობის შესასრულებლად.

ფინანსური რესურსი

სამინისტრო და სსიპ კიბერუსაფრთხოების ბიურო აცნობიერებს კონტექსტს, რომ საუკეთესო ბალანსის დაცვა, კიბერუსაფრთხოების უზრუნველყოფასა და საჭირო ფინანსურ მხარდაჭერას შორის კრიტიკული მნიშვნელობისაა.

სამინისტროში მიმდინარე ინსტიტუციური განვითარების ჭრილში კიბერუსაფრთხოება წარმოადგენს სტრატეგიულ მიმართულებას, რაც სამინისტროს ხელმძღვანელობის მხარდაჭერით გამოხატულია სხვადასხვა სახის ქმედებებში. სამინისტრო აცნობიერებს სტრატეგიული ამოცანების შესრულების პასუხისმგებლობას და ძლიერი კიბერთავდაცვითი გარემოს შესაქმნელად კომპლექსურად ახორციელებს და ზრდის ფინანსურ-მატერიალურ მხარდაჭერას.

სტრატეგიაში ნახსენები მიზნებისა და ამოცანების შესასრულებლად გამოყენებულ იქნება სსიპ კიბერუსაფრთხოების ბიუროს ფინანსური სახსრები სრულად, რაც საშუალოვადიანი პერიოდისათვის ექვემდებარება ზრდას. გარდა ამისა იქ, სადაც, ამოცანის კრიტიკული მნიშვნელობიდან გამომდინარე, საჭირო იქნება დამატებითი ფინანსური რესურსების მობილიზება, საქართველოს თავდაცვის სამინისტრო უზრუნველყოფს მიმართულების/აქტივობის დაფინანსებას/თანადაფინანსებას. ამასთან, აღნიშნული მიმართულებით კრიტიკული მნიშვნელობისაა საერთაშორისო პარტნიორების პროცესში ჩართულობა და მათი ფინანსური მხარდაჭერა.

სტრატეგიის სამოქმედო გეგმაში მოყვანილია კონკრეტული აქტივობები, რომელთათვის საჭიროა საერთაშორისო პარტნიორების მხარდაჭერა. აღნიშნულის გარეშე, არსებითი რისკის ქვეშ აღმოჩნდება აქტივობის ეფექტურად განხორციელებისა და მიზნების მიღწევის საკითხი.

სტრატეგიული მიზნები

მიზანი 1 - ადამიანური კაპიტალის განვითარება (ადამიანი)

სამინისტროში არსებული კიბერინციდენტების ანალიზის საფუძველზე იკვეთება, რომ ადამიანური ფაქტორი კიბერუსაფრთხოების უზრუნველყოფაში ერთ-ერთ ყველაზე მოწყვლად რგოლს წარმოადგენს. ერთი მხრივ, არასათანადო კვალიფიკაციის და რაოდენობის ტექნიკური პერსონალი, ხოლო, მეორე მხრივ, ინფორმაციული ტექნოლოგიების უსაფრთხო გამოყენებაში მოუმზადებელი მომხმარებელი/თანამშრომელი არის ის სახიფათო კომბინაცია, რომელიც საგრძნობლად ზრდის კრიტიკული ინფორმაციული ინფრასტრუქტურის მოწყვლადობის ხარისხს.

მიზანი 1 წარმოადგენს ქმედებათა ერთობლიობას, რაც, სისტემურ მიდგომებზე დაყრდნობით, უზრუნველყოფს ადამიანური კაპიტალის განვითარებას.

ამოცანა 1.1 ადამიანური შესაძლებლობების ზრდა საგანმანათლებლო აქტივობებში ჩართულობის გზით

კიბერუსაფრთხოების ეფექტურად და ეფექტიანად უზრუნველყოფისთვის კრიტიკულად მნიშვნელოვანია შესაბამისი ცოდნისა და უნარების მქონე პერსონალი. აღნიშნული თანაბრად ეხება, როგორც უშუალოდ კიბერ/ინფორმაციული უსაფრთხოების დამგეგმავ და განმახორციელებელ პირებს, ასევე კომპიუტერული სერვისების მომხმარებლებსაც.

კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლებას და ადამიანური შესაძლებლობების ზრდაზე ორიენტირებულ აქტივობებს, კიბერუსაფრთხოების სათანადო დონეზე უზრუნველყოფისათვის სასიცოცხლო მნიშვნელობა გააჩნია. ხშირ შემთხვევაში, სწორედ ადამიანური შეცდომის შედეგად ხდება სისტემების კომპრომეტირება და უსაფრთხოების ზომების დარღვევა.

სამინისტროს მასშტაბისა და კომპლექსურობის გათვალისწინებით, დიდი ყურადღება ექცევა პერსონალის შესაბამის მომზადება-გადამზადებას. აქედან გამომდინარე, ინტერნეტ-მომხმარებელთა ცოდნის სათანადო დონის უზრუნველსაყოფად, კრიტიკული მნიშვნელობისაა, მუდმივ

ციკლზე დამყარებული, ცნობიერების ასამაღლებელი სხვადასხვა ხასიათის აქტივობები, რაც ხელს უწყობს სამინისტროს წინაშე არსებული კიბერრისკების მინიმიზაციას.

კიბერუსაფრთხოების ცვალებადი გარემოს კვალდაკვალ, საჭიროა მაღალი კვალიფიკაციისა და ცოდნის მქონე კიბერსპეციალისტები, რომლებიც საერთაშორისო სტანდარტების გათვალისწინებითა და სათანადო ცოდნაზე დაყრდნობით დაგეგმავენ და სისრულეში მოიყვანენ უსაფრთხოებაზე ორიენტირებულ სხვადასხვა სახის ამოცანებს.

ამოცანა 1.2 სხვადასხვა სახის კიბერსავარჯიშოებსა და პროექტებში მონაწილეობით დარგის სპეციალისტების ტექნიკური უნარ-ჩვევების გაძლიერება

ინფორმაციული ტექნოლოგიების სწრაფი განვითარების პარალელურად ასიმეტრიულად იზრდება კიბერშეტევათა რიცხვი. ცვალებად კიბერგარემოში, მოწინააღმდეგის მიერ პერმანენტულად მიმდინარეობს კიბერშეტევითი ტაქტიკის, ტექნიკისა და პროცედურების ცვლა. შესაბამისად, მნიშვნელოვანია, რომ კიბერუსაფრთხოების სპეციალისტები უწყვეტ რეჟიმში მონაწილეობდნენ სხვადასხვა სახის ღონისძიებებში, რომლებიც გამიზნულია როგორც პრაქტიკული კიბერთავდაცვითი უნარ-ჩვევების გამომუშავებაზე, ასევე მსოფლიოში მიმდინარე საუკეთესო პრაქტიკების საოპერაციო გარემოში დანერგვაზე.

კიბერუსაფრთხოების ტექნიკური ჯგუფის პრაქტიკული უნარ-ჩვევების გაძლიერებისთვის საჭიროა მაღალი დონის კიბერსწავლებებში ჩართულობა. აღნიშნული ღონისძიებები წარმოადგენს კომპეტენციის ზრდის საუკეთესო საშუალებას, რაც რეალურ დროში კიბერკრიზისული სცენარების სიმულირებით, ხელს უწყობს შესაძლებლობების ზრდას.

მნიშვნელოვანია ყურადღება გამახვილდეს კიბერუსაფრთხოების საკითხებზე ორიენტირებულ სხვადასხვა სახის პროექტებზე. პროექტებში აქტიური მონაწილეობა, ერთი მხრივ, ხელს უწყობს საუკეთესო გამოცდილების გაზიარებას და ორგანიზაციული შესაძლებლობების ზრდას, ხოლო, მეორე მხრივ, იძლევა მიღებული ცოდნისა და გამოცდილების ყოველდღიურ რეალობაში გამოყენების საშუალებას.

მიზანი 2: პროცესების ინსტიტუციონალიზაცია და მართვის ეფექტიანობის ზრდა (პროცესი)

სამინისტროს ფარგლებში მიმდინარე ზოგიერთი პროცესი საჭიროებს გაუმჯობესებასა და ინსტიტუციურ დახვეწას. ფრაგმენტული დაგეგმვა და მართვა არასათანადო მიმართულებით წარმართავს პროცესებს, რაც, თავის მხრივ, აისახება კონკრეტული მიზნისა თუ ამოცანის შესრულების შედეგიანობაზე.

მიზანი 2 ითვალისწინებს პროცესების გაძლიერებას/სრულყოფას და რისკების ანალიზის საფუძველზე ადეკვატურ განახლებას, დაგეგმვასა და აღსრულებას.

ამოცანა 2.1. რისკებზე დაფუძნებული დაგეგმვით მართვის ოპტიმიზაციის უზრუნველყოფა

პროცესების პროაქტიულად დაგეგმვას კრიტიკული მნიშვნელობა ენიჭება ქვეყნის თავდაცვისუნარიანობის განმტკიცების საქმეში. შესაბამისად, მნიშვნელოვანია ცხადად და მკაფიოდ ჩამოყალიბებული სხვადასხვა კიბერსაოპერაციო გეგმებისა თუ სცენარების არსებობა, რაც საომარი თუ კრიზისული სიტუაციის დროს კიბერელემენტების აქტიური და ეფექტური გამოყენებისათვის სათანადო წინაპირობას შექმნის.

თავდაცვის სფეროში კიბერ და ინფორმაციული უსაფრთხოების უზრუნველყოფის ერთ-ერთი უმნიშვნელოვანესი მიმართულებაა ინფორმაციული უსაფრთხოების სტანდარტების დანერგვა. სტანდარტები, საერთაშორისოდ აღიარებული უსაფრთხოების ნორმების შესაბამისად, ინფორმაციული აქტივების უსაფრთხოების გაძლიერების და რისკებისა და ინციდენტების მართვის საშუალებას იძლევა.

ინფორმაციული აქტივების, რისკების მართვის მეთოდოლოგიის, ასევე, სხვა მნიშვნელოვანი წესების, პოლიტიკებისა თუ სამართლებრივი დოკუმენტების შემუშავება და დანერგვა კიდევ უფრო აამაღლებს თავდაცვის სფეროს ინფრასტრუქტურის დაცულობის ხარისხს. გარდა ამისა, ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვა თავდაცვის სფეროს სუბიექტებში, წარმოადგენს კიბერუსაფრთხოების განმტკიცების მხარდამჭერ მნიშვნელოვან ფაქტორს.

არანაკლებ მნიშვნელოვანია ინფორმაციული და საკომუნიკაციო სისტემების პერიოდული შეფასება/აუდიტი. მოწყვლადი ადგილების დროული აღმოჩენის და მათზე ადეკვატური რეაგირების შემთხვევაში, შესაძლებელია თავიდან იქნას აცილებული ქსელური ინფრასტრუქტურის ფუნქციონირების შეფერხება და სისტემის მთლიანობის დარღვევა.

ამოცანა 2.2 კვლევა და ანალიზი

განვითარების ტემპიდან გამომდინარე და კიბერუსაფრთხოების ეფექტურად უზრუნველყოფისათვის, მიზანშეწონილია სამინისტროში სხვადასხვა სახისა და მიზნობრიობის კვლევისა და ანალიზის წარმართვა.

თავდაცვის სფეროს კიბერ/ინფორმაციული უსაფრთხოების გარემოს შეფასების მიზნით, უნდა ჩატარდეს პერიოდული შეფასება, რაც გამოავლენს მმართველობითი მოდელების სისუსტეებს და დააყენებს აუცილებელი ცვლილებების ინიცირების საკითხს.

საჭიროა რეგულარულად განხორციელდეს კიბერსივრცეში არსებული და პოტენციური რისკების კვლევა. საფრთხეების გაცნობიერება და მათი პოტენციური ზემოქმედების შეფასება, ხელს შეუწყობს უსაფრთხოების ზომების გაძლიერებას. საფრთხეების ანალიზისა და რისკების კვლევის შედეგების საფუძველზე, გამოწვევების დაძლევის მიზნით უნდა მოხდეს პრევენციული ზომების შემუშავება და გატარება. ამ მხრივ, სფეროში არსებული სიახლეების კვლევა და ანალიზი, ხელს შეუწყობს სამინისტროს კიბერშესაძლებლობების განვითარებას და ამ მიმართულებით საუკეთესო პრაქტიკის დანერგვას.

მითითებული სტრატეგიული მიმართულებით პროცესების დახვეწა, ასევე საჭიროებს არსებული საკანონმდებლო ბაზის სიღრმისეულ ანალიზს და საერთაშორისოდ აღიარებულ ნორმებთან თავსებადობის გზით მის სრულყოფასა და გაძლიერებას.

მიზანი 3: ტექნოლოგიური მდგრადობის უზრუნველყოფა (ტექნოლოგია)

სამინისტროს, ისევე როგორც მთელი ქვეყნის წინაშე, დგას გარდაუვალი გაციფრულების პროცესი, რომელიც საგრძნობლად ამარტივებს საქმისწარმოებას და ეფექტიანობის სხვა დონეზე გადაჰყავს პროცესები. მეორე მხრივ, სამინისტროს მუშაობის სპეციფიკიდან გამომდინარე, სხვადასხვა მართვის სისტემები სულ უფრო მეტად ექცევა კიბერსფეროს გავლენის ქვეშ, რაც საჭიროებს თანამედროვე ტექნოლოგიის აქტიური გამოყენებით ადეკვატურ დაცულობას.

მიზანი 3 სამინისტროში თანამედროვე კიბერთავდაცვითი ინფრასტრუქტურის ინტეგრირებითა და თანმდევი პროცესების უზრუნველყოფით ითვალისწინებს უსაფრთხოების უზრუნველყოფას და პროაქტიული კიბერთავდაცვითი მექანიზმების შექმნას.

ამოცანა 3.1 კიბერშესაძლებლობების განმტკიცება მაღალი დონის ტექნიკური/პროგრამული უზრუნველყოფის საშუალებებით

თავდაცვის სფეროში კიბერუსაფრთხოების სათანადო დონეზე უზრუნველყოფისთვის, აუცილებელი პირობაა ტექნოლოგიური შესაძლებლობების პერმანენტული განვითარება/განახლება. სფეროში არსებული უახლესი ტექნოლოგიების ინტეგრაციით, სამინისტრო შეძლებს დასახული პრიორიტეტების ეფექტიან და დროულ განხორციელებას.

კიბერთავდაცვითი შესაძლებლობების განვითარებისთვის ძირითადი საყრდენი ახალი ტექნოლოგიების დანერგვაა, რისთვისაც გამოყოფილი უნდა იყოს შესაბამისი რესურსები, ხოლო პერსონალი სათანადოდ მომზადებული. სამინისტროს კიბერუსაფრთხოების არქიტექტურაში ინოვაციური მიდგომებისა და უახლესი ტექნიკური/პროგრამული შესაძლებლობების დანერგვა, საფრთხის შემცველი ქმედებების პრევენციის შესაძლებლობას იძლევა.

სსიპ კიბერუსაფრთხოების ბიურომ, სამინისტროს კრიტიკული ინფორმაციული სისტემების უსაფრთხოების უზრუნველსაყოფად, უნდა გაატაროს პროაქტიული ღონისძიებები, რაც, სათანადოდ აღჭურვილ

გარემოში, ინფრასტრუქტურის მონიტორინგისა და ეფექტური რეაგირების გზით, გაზრდის სამინისტროს მდგრადობას.

კიბერუსაფრთხოების პროაქტიულად უზრუნველყოფისათვის, ასევე კრიტიკულად მნიშვნელოვანია, ინციდენტების შესახებ ინფორმაციის გაცვლა, როგორც ეროვნულ, ასევე საერთაშორისო დონეზე. შესაბამისად, საჭიროა კვლავ გაგრძელდეს და განვითარდეს ამგვარ პლატფორმებში სსიპ კიბერუსაფრთხოების ბიუროს აქტიური ჩართულობა.

სტრატეგიული მიზნების მიღწევის გზები

კიბერუსაფრთხოების სწრაფი განვითარებისა და ამ განზომილებაში არარსებული საზღვრების გათვალისწინებით, რთულია ინდივიდუალურ რეჟიმში გამოწვევებზე სრულფასოვანი რეაგირება. შესაბამისად, მჭიდრო თანამშრომლობასა და კიბერინციდენტების შესახებ ინფორმაციის გაცვლას დიდი მნიშვნელობა ენიჭება.

სტრატეგია სხვადასხვა დონეზე თანამშრომლობას განიხილავს არა როგორც მიზნად, არამედ სტრატეგიული მიზნების მიღწევის საშუალებად / გზად.

შიდაუწყებრივ, ეროვნულ და **საერთაშორისო** დონეზე თანამშრომლობა არის ის ძირითადი საშუალება, რომლის აქტიური და ეფექტური გამოყენებითაც მოხდება სტრატეგიაში მოყვანილი სტრატეგიული მიზნებისა და აქტივობების შესრულება. კერძოდ, სამინისტროს კიბერშესაძლებლობების ზრდა და დასავლურ სტანდარტებთან მიახლოება.

შიდაუწყებრივი თანამშრომლობა

სტრატეგიული მიზნების მიღწევის ერთ-ერთ კრიტიკულად მნიშვნელოვან გზას, შიდაუწყებრივ დონეზე თანამშრომლობა წარმოადგენს. აღნიშნული კომპონენტი განსაკუთრებულ ხასიათს იძენს როდესაც, ორგანიზაციული მოწყობის გათვალისწინებით, მართვა მოითხოვს კომპლექსურ მიდგომას და საჭიროებს სხვადასხვა ქვეუწყებების აქტიურ თანამონაწილეობას.

სამინისტროში შემავალი სტრუქტურული ერთეულები ქმნიან ერთიან სისტემას, რომელიც ინფორმაციული ტექნოლოგიებისა და კომუნიკაციების სისტემებით მჭიდროდ არიან ერთმანეთთან დაკავშირებული.

სამინისტროში შემავალი კრიტიკული ინფორმაციული სისტემების კიბერ/ინფორმაციულ უსაფრთხოებას, უზრუნველყოფს სსიპ კიბერუსაფრთხოების ბიურო, რომელიც აღნიშნული ამოცანის შესასრულებლად მჭიდრო თანამშრომლობაშია საქართველოს თავდაცვის ძალების გენერალური შტაბის J-6 კავშირგაბმულობისა და ინფორმაციული სისტემების და სამინისტროს საინფორმაციო ტექნოლოგიების დეპარტამენტებთან. თანამშრომლობა მოიცავს როგორც ქსელური

ინფრასტრუქტურის, ასევე, სამინისტროში არსებული სხვადასხვა სახის აპლიკაციების კიბერუსაფრთხოებით უზრუნველყოფას.

ამასთანავე, სასიცოცხლო მნიშვნელობა ენიჭება სამინისტროს მის სისტემაში მოქმედ საჯარო სამართლის იურიდიულ პირებთან და სხვა, რელევანტურ სტრუქტურულ ერთეულებთან მჭიდრო კომუნიკაციასა და თანამშრომლობას, ვინაიდან ისინი ერთიანი სისტემის ნაწილია და მათ წინააღმდეგ მომხდარი კიბერშეტევები პირდაპირ კავშირშია სამინისტროს ერთიანი ინფორმაციული და საკომუნიკაციო სისტემის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის ხელყოფასთან.

არასათანადო დონეზე თანამშრომლობის შემთხვევაში, სამინისტროს ექმნება მნიშვნელოვანი გამოწვევები, რადგან მიუხედავად ცალკეული სტრუქტურული ერთეულების ეფექტიანი საქმიანობისა, თუ პროცესები არ დაიგეგმა და განხორციელდა ერთიანი სურათის გააზრებით, რთული იქნება თავდაცვის კომპლექსური სისტემის კიბერუსაფრთხოებით უზრუნველყოფა.

ეროვნული დონის თანამშრომლობა

ეროვნულ დონეზე თანამშრომლობის არსებული ფორმატი, უზრუნველყოფს კიბერსაფრთხეებზე რეაგირებას და ინფორმაციის გაზიარებას. ამ პროცესში ჩართულია სხვადასხვა სახელმწიფო დონის კიბერაქტორი და არ ხდება ფუნქციების დუბლირება. ეს უწყებებია: ეროვნული უსაფრთხოების საბჭო (პრემიერ მინისტრის სათათბირო ორგანო ეროვნული უსაფრთხოების საკითხებზე), სსიპ ციფრული მმართველობის სააგენტო (საქართველოს იუსტიციის სამინისტრო), სსიპ ოპერატიულ-ტექნიკური სააგენტო (საქართველოს სახელმწიფო უსაფრთხოების სამსახური), სსიპ კიბერუსაფრთხოების ბიურო (საქართველოს თავდაცვის სამინისტრო), კიბერდანაშაულთან ბრძოლის სამმართველო (საქართველოს შინაგან საქმეთა სამინისტრო).

კიბერსივრცეში არსებულ გამოწვევებზე ადეკვატური რეაგირებისა და ეროვნული კიბერუსაფრთხოების სათანადოდ უზრუნველყოფისათვის, მნიშვნელოვანია უწყებათაშორისი თანამშრომლობის განვითარება სხვადასხვა მიმართულებით, რათა ეროვნული უსაფრთხოების მექანიზმი ფუნქციონირებდეს როგორც ერთიანი სისტემა და არა როგორც ცალკეული

კომპონენტების მექანიკური ერთიანობა. ეროვნული კიბერუსაფრთხოების დაგეგმვის და განხორციელების ერთიანი სამთავრობო მიდგომა, უზრუნველყოფს არსებული რესურსების კოორდინირებული ძალისხმევით გამოყენებას.

სამინისტრო იზიარებს ერთიან სამთავრობო მიდგომას, რომელიც გულისხმობს კრიტიკული ინფორმაციული სისტემების სუბიექტების, კერძო სექტორის, აკადემიური წრეებისა და ინფორმაციული საზოგადოების ჩართულობას ქვეყნის კიბერუსაფრთხოების განვითარების საქმეში.

ეროვნულ დონეზე გაღრმავებული თანამშრომლობით, შესაძლებელი იქნება კიბერუსაფრთხოებასთან დაკავშირებული მოვლენების განვითარების სცენარების შემუშავება მშვიდობიანი, საგანგებო და საომარი მდგომარეობის დროისათვის. კიბერუსაფრთხოების სფეროში სახელმწიფოს ერთიანი ძალისხმევის ორგანიზება, ასევე ხელს შეუწყობს კიბერსივრცეში არსებული საფრთხეების პრევენციასა და კიბერინციდენტების შედეგად მიღებული ზიანის მინიმუმამდე შემცირებას.

საერთაშორისო თანამშრომლობა

თანამედროვე სამყაროში კიბერსივრცე აქტიურად გამოიყენება პოლიტიკური, სამხედრო, ეკონომიკური და სხვა მიზნების მისაღწევად. ტექნოლოგიების განვითარებასთან ერთად, რთულდება კიბერსივრცეში არსებული რისკების მართვა და პრევენცია, მეტადრე მაშინ, როდესაც კიბერსფეროს არ გააჩნია დადგენილი საზღვრები.

ეროვნული კიბერუსაფრთხოების განსამტკიცებლად და გლობალური უსაფრთხოების უზრუნველყოფაში წვლილის შესატანად, ერთ-ერთ კრიტიკულად მნიშვნელოვან კომპონენტს წარმოადგენს საერთაშორისო დონეზე თანამშრომლობის გამყარება და საუკეთესო გამოცდილების გაზიარება.

სტრატეგიულ პარტნიორებთან ორმხრივ და მრავალმხრივ ფორმატში თანამშრომლობა ხელს უწყობს სამინისტროს კიბერშესაძლებლობების

ზრდას. ნატოსა და ევროკავშირთან მჭიდრო ალიანსი, უზრუნველყოფს სამინისტროს კიბერსპეციალისტების ჩართულობას სხვადასხვა სახის საგანმანათლებლო პროგრამებში, კიბერწვრთნებში, სემინარებსა თუ კონფერენციებში, რაც ჯამში ზრდის სამინისტროს დასავლურ სტანდარტებთან თავსებადობას.

დასკვნა

ეს დოკუმენტი სტრატეგიულად მნიშვნელოვან განაცხადს წარმოადგენს, რომლის სისრულეში მოყვანაც სამინისტროს საშუალებას მისცემს, ჯეროვნად და ეფექტიანად იყოს მომზადებული დღევანდელ მსოფლიოში არსებულ კიბერგამოწვევებთან გასამკლავებლად.

განსაზღვრული პრიორიტეტების გათვალისწინებითა და სამიზნე მაჩვენებლების მიღწევის გზით, შესაძლებელი იქნება შემდგომ წლებში კიდევ უფრო მდგრადი ინფორმაციული და საკომუნიკაციო ინფრასტრუქტურის შექმნა.

მოცემული სტრატეგიის მიზნების და სამოქმედო გეგმის აქტივობების სამი მიმართულებით კლასიფიკაცია (ადამიანი, პროცესი, ტექნოლოგია), შესაძლებლობას იძლევა კიდევ უფრო ნათელი გახდეს ამ კომპონენტების ურთიერთკავშირი და მნიშვნელობა. შესაბამისი ელემენტების გაძლიერებით, მივაღწევთ ყველა იმ სტრატეგიულ მიზანს, რომელიც სასიცოცხლოდ მნიშვნელოვანია სამინისტროს კიბერსივრცისკენ მიმართული დამაზიანებელი ქმედებების პრევენციისა და საქართველოს თავდაცვის ძალებში კიბერუსაფრთხოების კომპონენტის ინტეგრირების საქმეში.

ნაკისრი ვალდებულებების შესრულება, მნიშვნელოვან წვლილს შეიტანს სამინისტროს ნატოსა და ევროკავშირის სტანდარტებთან თავსებადობის საქმეში და გაზრდის საერთაშორისო თანამშრომლობის ხარისხს როგორც სტრატეგიულ, ასევე ტაქტიკურ და ოპერაციულ დონეზე, რაც პოზიტიურად აისახება ეროვნული უსაფრთხოების დღის წესრიგზე.

ამრიგად, სამინისტრო აცნობიერებს, გლობალური სტრატეგიული უსაფრთხოების კონტექსტში, კიბერუსაფრთხოების საკითხების სიმწვავეს და კიბერსაფრთხეებთან გამკლავებისთვის კოორდინირებული ქმედებების მნიშვნელობას. შესაბამისად, გამოყოფს იმ სტრატეგიულ მიმართულებებს და განვითარების პრიორიტეტულ გზებს, რასაც უნდა დავეყრდნოთ მომდევნო წლების განმავლობაში.