კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების 2025-2030 წლების სტრატეგია

კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების 2025-2030 წლების სტრატეგია

სტრატეგია და სამოქმედო გეგმა შემუშავებულია ევროკავშირის დაძმობილების პროექტის - „კიბერუსაფრთხოების შესაძლებლობების განვითარება საქართველოში“ მხარდაჭერით

2025 წელი

სარჩევი

შესავალი

წინამდებარე დოკუმენტი საქართველოში კიბერცნობიერების ამაღლების სტრატეგიას წარმოადგენს. აღნიშნული სტრატეგია, გრძელვადიან პერსპექტივაში, ქვეყანაში კიბერუსაფრთხოების შესახებ ცნობიერების ამაღლებას და შესაძლებლობების განვითარებას უზრუნველყოფს. შედეგად, საქართველოში ჩამოყალიბდება უფრო მედეგი ციფრული ეკოსისტემა და ზოგადად, გაუმჯობესდება გაციფრების მიმართულებით გადადგმული ნაბიჯები.

დოკუმენტის შემუშავებას წინ უძღოდა რელევანტურ უწყებებთან, დაინტერესებულ მხარეებთან და ექსპერტებთან გამართული არაერთი სამუშაო შეხვედრა. მათ გამოცდილებასა და პროფესიულ ცოდნაზე დაყრდნობით მომზადდა კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების სტრატეგია და მისი განხორციელების სამოქმედო გეგმა.

საზოგადოებაში ციფრული უნარების, კიბერჰიგიენის და კიბერკულტურის განვითარება უმთავრესია ქვეყნის სოციალურ, კულტურულ და ეკონომიკურ სფეროებში ციფრული ეკოსისტემის გაძლიერების, თანაბარი ხელმისაწვდომობისა და ციფრული ჩართულობის გაუმჯობესებისთვის.

კიბერუსაფრთხოების სფეროს შესახებ საზოგადოების ცნობიერების ამაღლება და შესაძლებლობების განვითარება, როგორც ციფრული მმართველობის პროცესში უსაფრთხოების კომპონენტის გაძლიერება საქართველოს მთავრობის ბოლო ათწლეულის სტრატეგიული პრიორიტეტია. აღნიშნული პრიორიტეტი ქვეყნის სხვადასხვა პოლიტიკის დოკუმენტში და სამოქმედო გეგმაშია წარმოდგენილი მიზნების, ამოცანებისა და აქტივობების სახით. ციფრული უნარების განვითარების შესახებ პირველი ცალსახა დეკლარირება მოხდა „ციფრული საქართველო: ელექტრონული საქართველოს სტრატეგია და სამოქმედო გეგმა 2014-2018" დოკუმენტში, რომლის თანახმადაც, ინფორმაციულ-საკომუნიკაციო სფეროში მდგრადი განვითარება, მიიღწევა მხოლოდ ღია და გამჭვირვალე გარემოში, ციფრული სერვისების განვითარებაზე და ინოვაციებზე ორიენტირებული კერძო სექტორის წარმომადგენლებისა და შესაბამისი ციფრული უნარების მქონე საზოგადოების ჩართულობით.

საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგიები (2013-2015 წწ., 2017-2019 წწ. და 2021-2024 წწ.) მოიცავს კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების საკითხებს და მიიჩნევა კიბერუსაფრთხოების მიმართ საზოგადოების მიდგომის ცვლილებისა და კიბერმედეგობის შენარჩუნების გარდამტეხ ეტაპად.

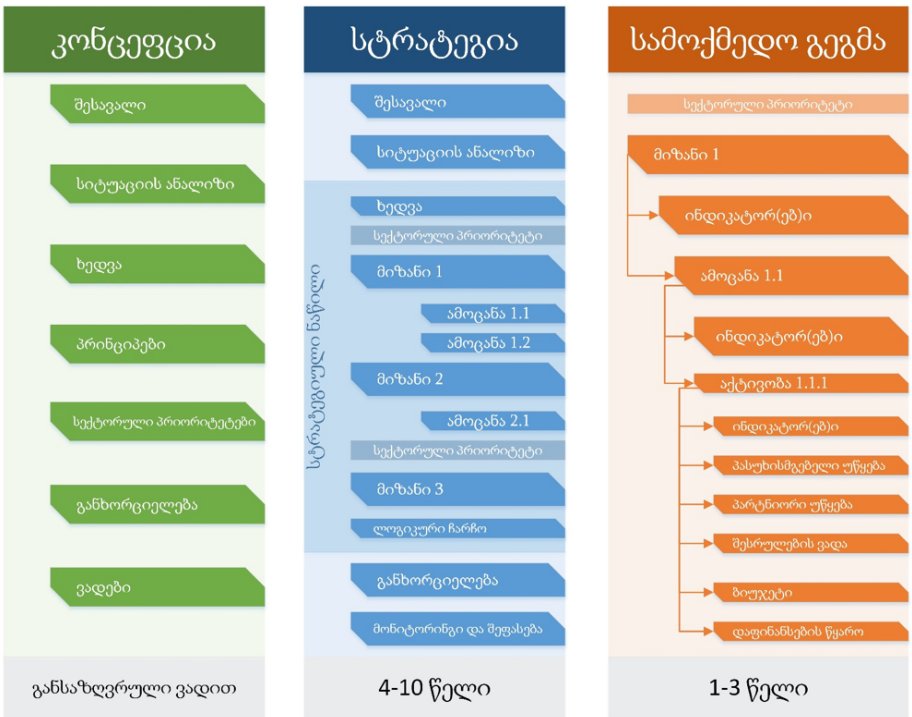
მიუხედავად იმისა, რომ გარკვეულ პოლიტიკის დოკუმენტებში, კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების საკითხები მიმოხილული იყო, არ არსებობდა დოკუმენტი, რომელიც ასახავდა „ერთიან სახელმწიფო მიდგომას", სამთავრობო ხედვასა და მიმდინარე ან სამომავლო გეგმებს, რომლებიც მიმართული იქნებოდა კიბერუსაფრთხოების სფეროში ერთიანი ძალისხმევით, მიზანმიმართულად და სტრუქტურირებულად ცნობიერების ამაღლებისკენ. სწორედ ამ მიზნით შემუშავდა კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების სტრატეგია და მისი სამოქმედო გეგმა დამოუკიდებელი სტრატეგიისა და სამოქმედო გეგმის სახით. წინამდებარე სტრატეგია წარმოადგენს საქართველოს 2021-2024 წლების ეროვნული კიბერუსაფრთხოების სტრატეგიის სამოქმედო გეგმის ერთ-ერთ აქტივობას, რომლის შემუშავებაზეც პასუხისმგებელი იყო სსიპ - ციფრული მმართველობის სააგენტო, ხოლო პარტნიორებად განსაზღვრული იყო: სსიპ - კიბერუსაფრთხოების ბიურო, სახელმწიფო უსაფრთხოების სამსახური, საქართველოს განათლებისა და მეცნიერების სამინისტრო, საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო, საქართველოს კომუნიკაციების ეროვნული კომისია, სახელმწიფო ინსპექტორის სამსახური და

საქართველოს შინაგან საქმეთა სამინისტრო. ამ აქტივობის ინდიკატორს კიბერუსაფრთხოების ეროვნული სტრატეგიის შესაბამისად წარმოადგენდა ცნობიერების ამაღლების სტრატეგიისა და მისი სამოქმედო გეგმის ტექსტებზე შეთანხმება ზემოთ მითითებულ პასუხისმგებელ და პარტნიორ უწყებებს შორის. ვინაიდან სტრატეგიის სამოქმედო გეგმით გათვალისწინებულ აქტივობებზე ზემოთ ჩამომთვლილი ორგანიზაციების გარდა სხვა უწყებებიც არის განსაზღვრული, წინამდებარე დოკუმენტი და მისი სამოქმედო გეგმა შეთანხმდა აქტივობების განხორციელებაზე პასუხისმგებელ და პარტნიორ დაწესებულებებს შორის. აღნიშნულმა უწყებებმა წერილობით დაადასტურეს სამოქმედო გეგმის განხორციელებაში მონაწილეობის მზაობა. ბოლო ასეთი დასტურის თარიღია 2025 წლის 10 ივლისი, რაც უნდა იქნეს მიჩნეული კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების 2025-2030 წლების სტრატეგიისა და მისი 2025-2030 წლების სამოქმედო გეგმის დამტკიცების თარიღად.

კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების სტრატეგია მიზნად ისახავს კომპეტენციებისა და შესაძლებლობების განვითარებას საქართველოს ციფრულ ეკოსისტემაში და კიბერუსაფრთხოების სფეროში საქართველოს მოსახლეობის ცნობიერების ამაღლებას. მოსახლეობის ცნობიერების ამაღლება და საზოგადოების ფართო ფენების კიბერკვალიფიკაციის გაზრდა, გრძელვადიან პერსპექტივაში, ქვეყანას უფრო კიბერმედეგს გახდის, განსაკუთრებით მზარდი საფრთხეების შემცველ გარემოში.

სტრატეგია და მისი სამოქმედო გეგმა აერთიანებს ამ სფეროში სხვადასხვა სამთავრობო უწყებებში მიმდინარე და დაგეგმილ ცნობიერების ამაღლების ყველა ინიციატივას ერთიან ჩარჩოში, და ხელს უწყობს სტრუქტურირებულ და კოორდინირებულ მუშაობას. დამატებით, სტრატეგია ხელს შეუწყობს სახელმწიფო და კერძო სექტორებს შორის თანამშრომლობის გაღრმავებას.

წინამდებარე სტრატეგიის სტრუქტურა ეფუძნება საქართველოს პოლიტიკის დოკუმენტების ზოგად სტრუქტურას, რომელიც ასახულია ***გამოსახულებაში №1.***



გამოსახულება №1: პოლიტიკის დოკუმენტების სტრუქტურა

სტრატეგიის განხორციელებაზე პასუხისმგებელი უწყებები

სტრატეგიის სამოქმედო გეგმით განსაზღვრული პასუხისმგებელი და პარტნიორი უწყებები:

1. საქართველოს იუსტიციის სამინისტრო;
2. საქართველოს განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტრო;
3. საქართველოს ეკონომიკის და მდგრადი განვითარების სამინისტრო;
4. საქართველოს შინაგან საქმეთა სამინისტრო;
5. საქართველოს ფინანსთა სამინისტრო;
6. საქართველოს ეროვნული უსაფრთხოების საბჭოს აპარატი;
7. სსიპ - ციფრული მმართველობის სააგენტო;
8. სსიპ - კიბერუსაფრთხოების ბიურო;
9. სსიპ - საქართველოს ოპერატიულ-ტექნიკური სააგენტო;
10. სსიპ - მასწავლებელთა პროფესიული განვითარების ეროვნული ცენტრი;
11. საქართველოს მთავრობის ადმინისტრაცია;
12. საქართველოს კომუნიკაციების ეროვნული კომისია;
13. პერსონალურ მონაცემთა დაცვის სამსახური;
14. საქართველოს ეროვნული ბანკი;
15. საქართველოს ენერგეტიკისა და წყალმომარაგების მარეგულირებელი ეროვნული კომისია.
16. სსიპ - საგანმანათლებლო დაწესებულების მანდატურის სამსახური;
17. ა(ა)იპ პროფესიული უნარების სააგენტო.

განსაზღვრული სამიზნე ჯგუფები:

- ფართო საზოგადოება, მათ შორის რეგიონებში მცხოვრები მოსახლეობა;
- კრიტიკული ინფორმაციული სისტემების სუბიექტები;
- საჯარო მოხელეები;
- მცირე და საშუალო საწარმოები;
- მედია;
- მოსწავლეები, სტუდენტები, პროფესიული საგანმანათლებლო დაწესებულებები;
- საზოგადოებრივი ორგანიზაციები;
- მასწავლებლები.

სიტუაციის ანალიზი

საქართველოში კიბერცნობიერების დონე უწყვეტად იზრდება, საზოგადოება კი სულ უფრო მეტად ითვალისწინებს კიბერჰიგიენის საბაზისო პრაქტიკას. ქვეყანაში ვითარდება კიბერუსაფრთხოების საკითხების შესწავლის კულტურა. მოსახლეობის უმრავლესობა ციფრული სერვისების გამოყენებისას უკვე დიდ ყურადღებას აქცევს უსაფრთხოების და კონფიდენციალურობის დაცვას. თუმცა, მიუხედავად ამისა, კიბერუსაფრთხოების ინსტრუმენტების სიღრმისეულად შესწავლის შესაძლებლობა კვლავ ლიმიტირებულია და შემოიფარგლება ექსპერტებით, უმაღლესი განათლებისა და შესაბამისი პროფესიული გამოცდილების მქონე მოქალაქეებით, ასევე თანამედროვე ტექნოლოგიებში კარგად გათვითცნობიერებული ახალგაზრდა თაობით. აქვე უნდა აღინიშნოს ისიც, რომ შესაბამისი პროფესიული გამოცდილების შემთხვევაში, კიბერუსაფრთხოების ინსტრუმენტების ცოდნის დონე დედაქალაქსა და რეგიონებში მცხოვრებ პირებს შორის მნიშვნელოვნად არ განსხვავდება.

საქართველოს მოსახლეობას აქვს ძირითადი ინფორმაცია კიბერუსაფრთხოების პრაქტიკების შესახებ, რომლებიც მათ შეუძლიათ გამოიყენონ თავდაცვის ან კიბერინციდენტებზე რეაგირების მიზნით, თუმცა ქვეყანაში კვლავ გამოწვევად რჩება კიბერდანაშაულის და კიბერუსაფრთხოების საკითხების შესახებ სიღრმისეული ცოდნა და შესაბამისი გამოცდილების მქონე პერსონალის დეფიციტი.

მიუხედავად იმისა, რომ საზოგადოებაში არსებობს კიბერდანაშაულის და კიბერუსაფრთხოების შესახებ ზოგადი ცოდნა და ამასთან, მუდმივად მიმდინარეობს ამ კუთხით საზოგადოების ცნობიერების ამაღლება, საზოგადოებას, დამატებით ესაჭიროება მუდმივად განახლებულ ინფორმაციაზე წვდომა და სიღრმისეული ცოდნა იმისა თუ როგორ დაიცვას თავი თანამედროვე კიბერსაფრთხეებისგან. საქართველოში მომუშავე კომპანიებმა კი, თავის მხრივ, საჭიროა გააქტიურონ სოციალური კამპანიები კიბერმედეგობის პროცესის გასაუმჯობესებლად.[1]

კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების ღონისძიებები საქართველოში სხვადასხვა დაინტერესებული მხარეების მიერ ხორციელდება: შესაბამისი მანდატის მქონე სახელმწიფო უწყებები, კერძო სექტორის წარმომადგენლები, საზოგადოებრივი ორგანიზაციები, ციფრული ელჩები, ადგილობრივი თემები, დონორი ორგანიზაციები და სხვა. ცნობიერების ამაღლების პროგრამები, კურსები, სემინარები და ონლაინ რესურსები ხელმისაწვდომია კონკრეტული საჯარო, კერძო, აკადემიური და სამოქალაქო საზოგადოების წრეებისთვის, თუმცა ამ სექტორებს შორის შეზღუდულად ან საერთოდ არ ხდება კოორდინირება.

ცნობიერების ამაღლების კამპანიებს აქვთ ერთჯერადი, სპორადული, არარეგულარული ხასიათი. ხშირ შემთხვევაში, ისინი არ განისაზღვრება სტრატეგიული გეგმით და არ არის კოორდინირებული უწყებებსა და დაინტერესებულ მხარეებს შორის, ქვეყანაში არ ხორციელდება ცნობიერების ამაღლების ერთიანი სახელმწიფო კამპანიები. როგორც წესი, ცნობიერების ამაღლების პროგრამები გათვლილია განსხვავებული სამიზნე ჯგუფებისთვის, თუმცა მათ შორის არ ხდება მიღებული ინფორმაციის ან ცოდნის გაზიარება.

კიბერცნობიერების კამპანიების არარეგულარული და არასისტემატური ხასიათი, ხშირ შემთხვევაში, გამოწვეულია არათანმიმდევრული და არასაკმარისი ფინანსური რესურსით, რაც აფერხებს ეფექტიანი და მდგრადი ეროვნული კიბერუსაფრთხოების სისტემის ჩამოყალიბებას, და გრძელვადიან პერსპექტივაში, აღნიშნული სისტემის გაძლიერების

[1] წყარო: კიბერდანაშაულის და კიბერუსაფრთხოების ბარომეტრი, რომელიც მომზადდა ევროკავშირის და ევროპის საბჭოს CyberEast და CybersecurityEast პროექტების მიერ, 2022 წლის იანვარში.

მიზნით ღონისძიებების დაგეგმვის შესაძლებლობას. კიბერუსაფრთხოების სფეროში მასშტაბური კამპანიების განსახორციელებლად როგორც საჯარო, ისე კერძო სექტორში არასაკმარისი ადამიანური კაპიტალი და ფინანსური რესურსებია. ამასთან, გასათვალისწინებელია, რომ კიბერცნობიერების პროგრამების არარეგულარული და არასისტემური ხასიათი მხოლოდ ფინანსური და ადამიანური რესურსების ნაკლებობით არ არის გამოწვეული, გამოწვევას წარმოადგენს პასუხისმგებლობების გადანაწილების და კოორდინაციის საკითხებიც. გასათვალისწინებელია, რომ ხელმძღვანელობის მხრიდან მართვის სადავეების ხელში აღება და მხარდაჭერა მნიშვნელოვანი ფაქტორია ეროვნული დონის ცნობიერების ამაღლების კამპანიების განხორციელების პროცესში.

კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების ეროვნული პოლიტიკის დოკუმენტის ხელმისაწვდომობის უზრუნველსაყოფად, ასევე ინიციატივების კოორდინირების, რესურსების სტაბილურობისა და მობილიზების მიზნით, აუცილებელია უწყებებს შორის მჭიდრო კოორდინაციის მექანიზმების არსებობა. სფეროს მოკვლევის და დაინტერესებულ მხარეებთან კონსულტაციების შემდეგ, წინასწარ განსაზღვრულ რელევანტურ უწყებებთან ერთად, სსიპ - ციფრული მმართველობის სააგენტომ შეიმუშავა წინამდებარე სტრატეგიის სამოქმედო გეგმა. სამოქმედო გეგმის ეფექტიანად განხორციელების მიზნით, საერთო რესურსების, ექსპერტული ცოდნის და უნარების გათვალისწინებით, განსაზღვრა მხარეების როლები და თანამშრომლობის პრინციპები.

საქართველოს იუსტიციის სამინისტროს სსიპ - ციფრული მმართველობის სააგენტო წარმოადგენს საქართველოს კანონმდებლობით განსაზღვრული უფლებამოსილებების ფარგლებში ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების სფეროებში მომუშავე ერთ-ერთ წამყვან სახელმწიფო უწყებას. სააგენტო ზედამხედველობას უწევს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემების სუბიექტებს და ხელს უწყობს მათი სისტემების დაცვას. სსიპ - ციფრული მმართველობის სააგენტოს ფარგლებში ფუნქციონირებს საქართველოს ეროვნული კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი (CERT.DGA.GOV.GE). სსიპ - ციფრული მმართველობის სააგენტო ქვეყანაში წამყვანი საჯარო უწყებაა კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების ღონისძიებების განხორციელების კუთხით. აღნიშნული ღონისძიებები მიზნად ისახავს საჯარო და კერძო სექტორების და ზოგადად, საზოგადოების ინფორმირებას კიბერსაფრთხეებისა და სისუსტეების შესახებ. სააგენტო კოორდინაციას უწევს ეროვნულ დონეზე ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების სფეროებში საგანმანათლებლო და ცნობიერების ამაღლების ღონისძიებებს და ამასთან მონიტორინგს უწევს აქტივობების განხორციელების პროცესს. სააგენტო საკუთარი რესურსების, ასევე საერთაშორისო პარტნიორების დახმარებით, სხვადასხვა არხების გამოყენებით სამიზნე ჯგუფებში ატარებს: კიბერუსაფრთხოების სავარჯიშოებს სახელმწიფო და კერძო სუბიექტებისთვის, კიბერფორუმებს საჯარო-კერძო პარტნიორობისთვის, მათ შორის, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის, კიბერჰიგიენის ტრენინგებს საჯარო მოხელეების, ჟურნალისტების, სტუდენტების, მოსწავლეებისა და მასწავლებლებისთვის, რომლებიც მიზნად ისახავს აუდიტორიის ონლაინ უსაფრთხოებასთან დაკავშირებული საბაზისო უნარების და ცოდნის განვითარებას. სსიპ - ციფრული მმართველობის სააგენტოს მიერ მომზადებული სასწავლო მასალები ხელმისაწვდომია ნებისმიერი დაინტერესებული პირისთვის, უსასყიდლოდ, ონლაინ ფორმატში.[2] კიბერუსაფრთხოების სფეროთი დაინტერესებული ახალგაზრდებისთვის სსიპ - ციფრული მმართველობის სააგენტო, კერძო კომპანიებთან თანამშრომლობის ფარგლებში, ორგანიზებას უწევს კონკურსებს, სტაჟირების პროგრამებს და სასწავლო კურსებს ახალგაზრდა კიბერენთუზიასტებისთვის. კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების მიზნით განხორციელებული პროგრამების შესახებ

[2] სასწავლო მოდულები ხელმისაწვდომია ბმულზე.

ინფორმაცია ხელმისაწვდომია CERT.DGA.GOV.GE-ს ოფიციალურ Facebook ვებგვერდზე. სააგენტო, ასევე ატარებს საინფორმაციო მედია კამპანიებს კიბერუსაფრთხოების უახლეს ტენდენციებზე, საფრთხეებსა და გამოწვევებზე, რომლებიც მიმართულია სამოქალაქო საზოგადოების ინფორმირებაზე. სააგენტო ავრცელებს საჯარო ინფორმაციას სხვადასხვა ტრადიციული და თანამედროვე მედია არხების, მათ შორის ბროშურების, სატელევიზიო გადაცემების, საჯარო გამოსვლების, ინტერნეტ რესურსების, სოციალური მედიის და სხვა არხების გამოყენებით. სსიპ - ციფრული მმართველობის სააგენტოს ინიციატივით შეიქმნა **კიბერუსაფრთხოების სფეროში საჯარო-კერძო თანამშრომლობის პლატფორმა (GCPPP)**. პლატფორმის მთავარი მიზანია ინფორმაციისა და გამოცდილების გაზიარება და კიბერუსაფრთხოების საუკეთესო პრაქტიკების დანერგვა როგორც ამ სფეროში განსხვავებული მანდატის მქონე ორგანიზაციებს, ისე ეროვნული დონის კრიტიკული ინფორმაციული სისტემების სუბიექტებს შორის.

საქართველოს თავდაცვის სამინისტროს სსიპ - კიბერუსაფრთხოების ბიურო, როგორც კიბერუსაფრთხოების სფეროში მოქმედი ერთ-ერთი უწყება, პასუხისმგებელია კიბერცნობიერების ამაღლებაზე საქართველოს თავდაცვის სამინისტროსა და მის დაქვემდებარებულ სტრუქტურებში, მათ შორის საგანმანათლებლო ინსტიტუტებში (ეროვნული თავდაცვის აკადემია, კადეტთა სამხედრო ლიცეუმი), სამხედრო ქვედანაყოფებში, სამოქალაქო სამსახურებში და სამინისტროს დაქვემდებარებაში მოქმედ ყველა უწყებაში.

ყოველივე ზემოაღნიშნული ასახულია საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების სტრატეგიაში, რომელშიც სამინისტრო კიბერუსაფრთხოების მართვის კუთხით მიჰყვება ერთიან სახელმწიფოებრივ მიდგომას. ამასთან, სსიპ - კიბერუსაფრთხოების ბიურო აგრძელებს აქტივობებს, რომლებიც მიმართულია თავდაცვის სფეროში კიბერცნობიერების ამაღლებისკენ.

სსიპ - კიბერუსაფრთხოების ბიურო რეგულარულად ატარებს კიბერჰიგიენის კურსებს, რომლებიც მორგებულია თავდაცვის სამინისტროს თანამშრომლებზე, ამზადებს და აახლებს კიბერჰიგიენის ელექტრონულ კურსებს თავდაცვის სამინისტროს ელექტრონული სწავლების პორტალზე, რომლის გავლაც სავალდებულოა ახლად დანიშნული თანამშრომლებისთვის.

სახელმძღვანელოებისა და სარეკლამო მასალების (მათ შორის ბანერების, ბროშურების, ეკრანზე გამოსახული გაფრთხილებების და ვიდეოების) დამზადებასთან ერთად, სსიპ - კიბერუსაფრთხოების ბიურო ელექტრონული ფოსტისა და მოკლე ტექსტური შეტყობინებების გზით აწვდის შესაბამის აუდიტორიას ინფორმაციას მიმდინარე კიბერსაფრთხეების და მათგან თავდაცვის საჭირო ღონისძიებების შესახებ .

სსიპ - კიბერუსაფრთხოების ბიურო უზრუნველყოფს დაჭრილი სამხედროების ჩართულობას (რომლებსაც გავლილი აქვთ კიბერჰიგიენის ტრენერების სპეციალური სწავლება) კიბერჰიგიენის ტრენინგების ჩატარების პროცესში, რომელიც 2016 წლიდან ტარდება სამხედრო ქვედანაყოფებისთვის. სსიპ - კიბერუსაფრთხოების ბიურო მონაწილეობს ყოველწლიურ მედია სავარჯიშოს ორგანიზებაში (ღირსეული რეაგირება), რათა მედია წარმომადგენლებში ამაღლდეს კიბერუსაფრთხოებისა და მისი მნიშვნელობის შესახებ ცნობიერება.

საქართველოს სახელმწიფო უსაფრთხოების სამსახურის სსიპ - საქართველოს ოპერატიულ - ტექნიკური სააგენტო წარმოადგენს კიბერუსაფრთხოების სფეროში ერთ-ერთ წამყვან უწყებას, რომელიც პასუხისმგებელია კიბერუსაფრთხოების პოლიტიკის განხორციელებაზე, საფრთხეების პრევენციასა და მათზე რეაგირებაზე. სააგენტო ზედამხედველობს კრიტიკული ინფორმაციული სისტემების სუბიექტების პირველ და მეორე კატეგორიას და ხელს უწყობს მათი სისტემების დაცვას. ასევე, კომპეტენციის

ფარგლებში, უზრუნველყოფს ცნობიერების ამაღლებას სხვადასხვა სამიზნე ჯგუფებში. უწყება ასევე მნიშვნელოვან როლს ასრულებს საერთაშორისო სტანდარტების შესაბამისი ჩარჩო დოკუმენტების შემუშავების პროცესში და სხვადასხვა სექტორში მათი დანერგვის ხელშეწყობაში, რაც უზრუნველყოფს კიბერუსაფრთხოების ერთიანი და თანმიმდევრული მიდგომის ჩამოყალიბებას ქვეყნის მასშტაბით.

საქართველოს განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტრო აცნობიერებს კიბერუსაფრთხოების კუთხით განათლების მიღების საჭიროებას, როგორც ზოგად, ასევე, უმაღლეს საგანმანათლებლო დაწესებულებებში. განსაკუთრებით მას შემდეგ, რაც COVID-19-ის პანდემიის პერიოდში გამოიკვეთა განათლების სექტორის მაღალი დამოკიდებულება ციფრულ რესურსებზე და ონლაინ სწავლებაზე. კიბერუსაფრთხოების 2021-2024 წლების ეროვნული სტრატეგიის თანახმად, კიბერუსაფრთხოების მიმართულებით განათლების გაძლიერება არის საკვანძო საკითხი. ამავე დოკუმენტით განსაზღვრულია კონკრეტული აქტივობები დასახული მიზნების მისაღწევად. სამინისტროს ინიციატივით შემუშავდა „კიბერუსაფრთხოება თინეიჯერებისთვის“ სახელმძღვანელო. სახელმძღვანელო აერთიანებს ინფორმაციულ-საკომუნიკაციო ტექნოლოგიებს, ციფრულ მოქალაქეობას, კიბერსივრცეში ქცევის წესებსა და სხვა რელევანტურ საკითხებს. საქართველოს განათლების, მეცნიერებისა და ახალგაზრდობის სამინისტროს მასწავლებელთა პროფესიული განვითარების ეროვნული ცენტრი მუშაობს მასწავლებელთა ციფრული უნარების განვითარების მიმართულებით და იყენებს ტრენერთა ტრენინგის პრინციპს, რათა გადამზადებულმა მასწავლებლებმა შეძლონ, სახელმძღვანელოს შინაარსის შესაბამისად, საკუთარი ცოდნის მოსწავლეებისთვის გაზიარება.

საქართველოს შინაგან საქმეთა სამინისტრო როგორც სამართალდამცავი ორგანო პასუხისმგებელია კიბერდანაშაულის შემთხვევების გამოძიებაზე, უზრუნველყოფს მედია საშუალებებით კიბერდანაშაულთან და მისი შეტყობინების მექანიზმებთან დაკავშირებით ცნობიერების ამაღლებას. საქართველოს შინაგან საქმეთა სამინისტრო რეგულარულად ატარებს საინფორმაციო შინაარსის შეხვედრებს.

საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო, ქვეყანაში ტელეკომუნიკაციების, საინფორმაციო ტექნოლოგიებისა და ინოვაციების სფეროში შეიმუშავებს სახელმწიფო პოლიტიკის ძირითად მიმართულებებს. სამინისტრო უზრუნველყოფს თანამედროვე ტექნოლოგიების უწყვეტ განვითარებას და მის მაქსიმალურ ეკონომიკურ ეფექტიანობას, ქვეყნის პრიორიტეტების შესაბამისად.
სამინისტრო პასუხისმგებელია ქვეყანაში ელექტრონული კომუნიკაციების, ინოვაციური ეკოსისტემისა და საინფორმაციო ტექნოლოგიების განვითარებასა და ხელშეწყობაზე. აღნიშნული მიზნით, სამინისტრო მონაწილეობს კიბერ და საინფორმაციო უსაფრთხოების პოლიტიკის შემუშავებასა და მონიტორინგში, ახორციელებს საგანგებო ან/და საომარი მდგომარეობის დროს, მათ შორის, კიბერ ან/და საინფორმაციო შეტევების პერიოდში, საერთო სარგებლობის ელექტრონული კომუნიკაციების, საინფორმაციო ტექნოლოგიური და ფოსტის ქსელებისა და საშუალებათა ფუნქციონირების კოორდინაციას კანონმდებლობით დადგენილი წესით. საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტროს მხარდაჭერითა და თანაორგანიზებით 2019 წლიდან საქართველოშიც აღინიშნება „უსაფრთხო ინტერნეტის დღე (Safer Internet Day – SID)“, რომელიც ეძღვნება უსაფრთხო ინტერნეტ გარემოს შექმნას, სამთავრობო და არასამთავრობო სექტორის, საერთაშორისო და ადგილობრივი ორგანიზაციების, კერძო კომპანიების და ყველა დაინტერესებული პირების ჩართულობით, ღონისძიება ემსახურება მიზანს, რომ ხელი შეეწყოს ინტერნეტში უსაფრთხოების საკითხების შესახებ ინფორმირებულობის დონის ამაღლებას და პოზიტიურ ცვლილებებს ციფრულ სამყაროში. ღონისძიებაზე წარმოჩენილია ყველა დაინტერესებული მხარის მიერ უსაფრთხო

ინტერნეტის ფორმირების მიმართულებით იდენტიფიცირებული მნიშვნელოვანი საკითხები, განხორციელებული აქტივობები და სამომავლო გეგმები.

კიბერუსაფრთხოების სფეროში, საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU) ექსპერტების მიერ საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტროსთვის აღმოჩენილი ტექნიკური დახმარების შედეგად, მომზადდა ,,საქართველოში ონლაინ უსაფრთხოების შეფასების ანგარიში და რეკომენდაციები". პროექტის ფარგლებში სამინისტროს მიერ განხორციელდა კვლევა სპეციალური „ონლაინ" კითხვარების საშუალებით, რომლებიც განკუთვნილი იყო მშობლებისთვის, ბავშვებისთვის და ორგანიზაციებისთვის. განხორციელდა გამოკითხვა, ინტერნეტის უსაფრთხოდ მოხმარების მიმართულებით. კვლევის ფარგლებში გამოიკითხა 1 177 არასრულწლოვანი, 1049 მშობელი და 55 ორგანიზაცია. ექსპერტების მიერ მომზადებული დოკუმენტი განთავსდა საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტროს ვებგვერდზე, ასევე, მიეწოდა ყველა დაინტერესებულ მხარეს გამოყენებისა და გავრცელების მიზნით. ონლაინ სივრცეში ბავშვთა და მოზარდთა უსაფრთხოების მსოფლიოს საუკეთესო პრაქტიკის გაზიარების მიზნით, საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU) მიერ, სამინისტროსთან თანამშრომლობით, დღეს უკვე ქართულ ენაზეა საერთაშორისო სატელეკომუნიკაციო კავშირის „ბავშვთა ონლაინ დაცვის სახელმძღვანელო მშობლებისა და აღმზრდელებისთვის". სახელმძღვანელო შეიქმნა ITU-ს და ბავშვთა ონლაინ დაცვის საკითხებზე მომუშავე მოწინავე ორგანიზაციების ჩართულობით. სახელმძღვანელოს მიზანია უზრუნველყოს მშობლების და აღმზრდელების ცნობიერების ამაღლება ახალგაზრდა თაობის ონლაინ სამყაროსთან უსაფრთხო კავშირისთვის და დაეხმაროს მათ შესაბამისი რეკომენდაციებით, რათა ახალგაზრდა თაობის მიერ დაძლეულ იქნას ციფრული სამყაროს პოტენციური რისკები და საფრთხეები. სახელმძღვანელო განთავსდა საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტროს ვებგვერდზე, ასევე, მიეწოდა ყველა დაინტერესებულ მხარეს გამოყენებისა და გავრცელების მიზნით (მათ შორის, საქართველოს განათლებისა და მეცნიერების სამინისტროს)

საქართველოს კომუნიკაციების ეროვნული კომისია (ComCom) არის მედიაწიგნიერების განვითარებაზე პასუხისმგებელი უწყება. საზოგადოებაში მედიაწიგნიერების შესახებ ცნობიერების ამაღლებისა და მედიაპროდუქტზე წვდომის, მისი ანალიზის, კრიტიკული შეფასების, შექმნისა და გავრცელებისათვის საჭირო უნარების, დამოკიდებულებებისა და კომპეტენციების განვითარებისთვის, ComCom-ის ძირითადი გრძელვადიანი მიზნებია 1) ფორმალურ განათლებაში მედიაწიგნიერების სისტემური ინტეგრირების ხელშეწყობა, 2) მედიაწიგნიერების შესახებ ცნობიერებისა და შესაბამისი უნარების განვითარებაზე ორიენტირებული არაფორმალური განათლების საერთაშორისო პრაქტიკის ადაპტირება და განხორციელება, და 3) მაღალი სტანდარტის მედიაპროდუქტების შექმნისა და ინოვაციების განვითარების ხელშეწყობა. ზემოაღნიშნული მიზნების გათვალისწინებით, კომისია 2018 წლიდან არაერთ მნიშვნელოვან პროექტს ახორციელებს, რომლის ძირითად სამიზნე აუდიტორიას მოსწავლეები, სტუდენტები, მასწავლებლები და მშობლები წარმოადგენენ. პროექტების შერჩევის პროცესი ითვალისწინებს საერთაშორისო, მათ შორის ევროპული ქვეყნების, საუკეთესო პრაქტიკის შესწავლას და დაინტერესებულ მხარეებთან კოორდინაციით, ქართულ რეალობასთან ადაპტირებას. ამ მიზნით, ადგილობრივ დონეზე ComCom-ი აქტიურად თანამშრომლობს სამთავრობო და საერთაშორისო მხარეებთან. აღსანიშნავია, რომ 2018 წლიდან დღემდე, ComCom-ის მიერ განხორციელებულმა მედიაწიგნიერების პროექტებმა ჯამში 32,000-ზე მეტი ბენეფიციარი მოიცვა.

კომუნიკაციების კომისია 2022 წლიდან ახორციელებს "ციფრული მხარდაჭერის პროგრამას". პროგრამის მიზანს შერჩეული მუნიციპალიტეტებისა და სოფლად მცხოვრები მოსახლეობის ციფრული ცნობიერების ამაღლება, მათთვის ინტერნეტის მიზნობრივად გამოყენების სწავლება და ციფრულ ეკონომიკაში ჩართულობის ხელშეწყობა წარმოადგენს.

პროგრამა მოიცავს ციფრული წიგნიერებისა და ინტერნეტის უსაფრთხო გამოყენების საკითხებზე სემინარებს, რომელიც ემსახურება პროგრამის ბენეფიციარების ცნობიერების ამაღლებას ისეთ საკითხებზე, როგორიცაა: ინფორმაციის მოძიება, ელ-ფოსტის გამოყენება, გუგლის რუკითა და თარჯიმნით სარგებლობა, ონლაინ საკომუნიკაციო საშუალებების გამოყენება, ინტერნეტში უსაფრთხო ნავიგაცია, ნამდვილი და ყალბი ინფორმაციის ამოცნობა და სხვა. გარდა თემატური სემინარებისა, პროგრამა მოიცავს საინფორმაციო შეხვედრებს სახელმწიფო ელექტრონული სერვისების და ინტერნეტის მომხმარებელთა უფლებების შესახებ. პროგრამის ფარგლებში 230 სოფელსა და დასახლებულ პუნქტში სულ ჩატარდა 600 სემინარი და გადამზადდა 8000-მდე ადამიანი.

კომუნიკაციების კომისიის ერთ-ერთი მთავარი ამოცანა, ქვეყანაში მედიაწიგნიერების განვითარების პროცესში, მეტი დაინტერესებული მხარის ჩართვა და აქტიური კოორდინაციის ხელშეწყობაა. სწორედ ამ მიზანს ემსახურება მედიაწიგნიერების ონლაინ პლატფორმა - www.mediatsigniereba.ge, რომელიც საქართველოში მედიაწიგნიერების მიმართულებით მომუშავე საჯარო, საერთაშორისო და არასამთავრობო ორგანიზაციებისა თუ უწყებებისთვის ერთიან ონლაინ სივრცეს, ერთგვარ ჰაბს წარმოადგენს. ეს არის ვებპლატფორმა, რომელიც მედიაწიგნიერების შესახებ არსებულ საგანმანათლებლო რესურსებსა და პროექტებზე წვდომას ნებისმიერი დაინტერესებული პირისათვის უზრუნველყოფს. პლატფორმაზე განთავსებული საინფორმაციო სტატიები და საგანმანათლებლო რესურსები ისეთ თემებს ეხება, როგორიცაა კიბერჰიგიენა, ინტერნეტსაფრთხეები, სოციალური მედია, ხელოვნური ინტელექტი და სხვა.

პერსონალურ მონაცემთა დაცვის სამსახური და მისი ცნობიერების ამაღლების კამპანიები სასიცოცხლოდ მნიშვნელოვანია ონლაინ გარემოში პერსონალურ მონაცემთა დაცვისთვის. პერსონალურ მონაცემთა დაცვის სამსახური საზოგადოების ცნობიერების ამაღლების მიზნით აქტიურად იყენებს სხვადასხვა საკომუნიკაციო არხსა და საშუალებას, სამსახურის მიერ აქტიურად გამოიყენება სოციალური ქსელები, ტრადიციული მედია, პირისპირი შეხვედრების ფორმატი, ვიზუალური, ვიდეო თუ აუდიომასალა. სამსახური აქტიურად ათავსებს საინფორმაციო პლაკატებს მათ შორის საზოგადოებრივ ტრანსპორტსა და სკოლებში. პერიოდულად იბეჭდება საინფორმაციო ბროშურები, რომელიც თემატურად რიგდება სხვადასხვა სამიზნე აუდიტორიასთან. საჯარო მოხელეებისთვის არსებობს მონაცემთა დაცვის კურსები, რომლებიც ორიენტირებულია მათ სპეციალურ საჭიროებებზე, როგორიც არის მოქმედება მონაცემთა დაცვის პრინციპების გათვალისწინებით, სამსახური აქტიურად მართავს ცნობიერების ამაღლების მიმართულებით საინფორმაციო კამპანიებს, მათ შორის – ლექცია/ტრენინგების, პერსონალურ მონაცემთა დაცვის ოფიცერთა გადამზადების კურსებისა და რეგიონული შეხვედრების სახით. სამსახურის ელექტრონულ სასწავლო პლატფორმაზე elearning.pdps.ge დაინტერესებულ პირებს შესაძლებლობა აქვთ მიიღონ საბაზისო ცოდნა პერსონალურ მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული ყველა ძირითადი ინსტიტუტის შესახებ და გაიგონ, თუ რა წესები უნდა დაიცვან პერსონალური მონაცემების კანონიერად დამუშავებისთვის. პერსონალურ მონაცემთა დაცვის სამსახური, საკანონმდებლო მანდატის ფარგლებში, მოქალაქეებს, კომპანიებს და სახელმწიფო უწყებებს სთავაზობს საკონსულტაციო მომსახურებებს. დამატებით, მოქმედებს საინფორმაციო ხასიათის პლატფორმები („Facebook“, „linkedin“, „X“, „YouTube“), რომელიც გულისხმობს მონაცემების დამუშავების დარღვევების, პარლამენტის ყოველწლიური ანგარიშების, კითხვა-პასუხის ღონისძიებების და დიალოგების

წარმოებას, სოციალურ მედიაარხებსა და სოციალურ ქსელებში სამსახურის მიერ შექმნილ გვერდებზე მთელი წლის განმავლობაში სისტემატურად ქვეყნდება სამსახურის გადაწყვეტილებები, „მსოფლიო პრაქტიკა“, განცხადებები და რელიზები, ხოლო კვარტალურად — სამსახურის მიერ გაწეული საქმიანობის ანგარიშები და სტატისტიკური მონაცემები. ასევე, მოქმედია ორი რუბრიკა სახელწოდებებით: „DataTech“ ანალიტიკა და „Datanewsroom“. პერსონალურ მონაცემთა დაცვის საკითხებით დაინტერესებული პირებისთვის მუდმივად ქვეყნდება სახელმძღვანელო რეკომენდაციები და გაიდლაინები. სამსახურს, ოფიციალურ ვებგვერდზე შემუშავებული აქვს ონლაინ აპლიკაცია „ციფრული მრჩეველი“, რომლის მიზანია ორგანიზაციებისთვის მორგებული, კონკრეტულ საჭიროებებზე ადაპტირებული სახელმძღვანელო რეკომენდაციების შემუშავება.

საქართველოს მთავრობის ადმინისტრაცია წარმოადგენს საჯარო სამსახურის რეფორმის მაკოორდინირებელ უწყებას, რომელიც მუშაობს საჯარო დაწესებულების ორგანიზაციული მოწყობის სტანდარტიზებასა და საჯარო სამსახურში ადამიანური კაპიტალის მართვის პროცესების სტრატეგიულ განვითარებაზე. 2025 წლის 1-ელ აპრილამდე, აღნიშნული ხორციელდებოდა სსიპ - საჯარო სამსახურის ბიუროს მიერ. „საქართველოს მთავრობის სტრუქტურის, უფლებამოსილებისა და საქმიანობის წესის შესახებ“ საქართველოს კანონში განხორციელებული ცვლილების შესაბამისად, 2025 წლის 1-ლი აპრილიდან ლიკვიდირდა სსიპ - საჯარო სამსახურის ბიურო, ხოლო მის უფლებამონაცვლედ განისაზღვრა საქართველოს მთავრობის ადმინისტრაცია.

საჯარო სამსახურის რეფორმის იმპლემენტაციის მხარდაჭერის პროცესში, საჯარო სამსახურის ბიურომ შექმნა საჯარო მოხელეებთან საკომუნიკაციო არაერთი პლატფორმა, რომელთა გამოყენებითაც უზრუნველყოფდა პროფესიული საჯარო მოხელეების ცნობიერების ამაღლებას და ინფორმირებულობას სხვადასხვა თემაზე. 2021-2023 წლების განმავლობაში, ბიურო რეგულარულად ატარებდა საჯარო მოხელეთა ფორუმებს, მათ შორის, რამდენიმე დაეთმო კიბერუსაფრთხოების საკითხებსაც. აღნიშნულ შეხვედრებში მონაწილეობა მიიღო ცენტრალური ხელისუფლებისა და ადგილობრივი თვითმმართველობის ორგანოებში დასაქმებულმა 700-ზე მეტმა წარმომადგენელმა. ამასთანავე, საჯარო სამსახურის ბიურო, სსიპ - ციფრული მმართველობის სააგენტოსთან თანამშრომლობით, ჩართული იყო საჯარო მოხელეების ცნობიერების ამაღლების პროცესში, რომლის ფარგლებშიც აქტიურად ეწეოდა კიბერუსაფრთხოების ონლაინ კურსის პოპულარიზაციას. თანამშრომლობის ფორმატში დაგეგმილი კამპანიის შედეგად, 2024 წლის განმავლობაში, აღნიშნული კურსი გაიარა ცენტრალურ საჯარო დაწესებულებებში დასაქმებულმა 400-ზე მეტმა მოხელემ.

საქართველოს მთავრობის ადმინისტრაცია, როგორც სსიპ - საჯარო სამსახურის ბიუროს უფლებამონაცვლე, საჯარო მოხელეების უწყვეტი პროფესიული განვითარების უზრუნველსაყოფად, შეიმუშავებს ახალ ხედვებსა და ინიციატივებს, რომლებიც მორგებულია თანამედროვე გამოწვევებზე. საჯარო მოხელეთა პროფესიული განვითარების ხელშესაწყობად, საქართველოს მთავრობის ადმინისტრაცია განახორციელებს საჯარო სამსახურის ბიუროს მიერ შექმნილი სწავლების ერთიანი ელექტრონული პლატფორმის ადმინისტრირებას. მოცემული პლატფორმა შესაძლებლობას მისცემს პროფესიულ საჯარო მოხელეებსა და სხვა დაინტერესებულ პირებს გაიარონ ტრენინგ პროვაიდერების მიერ შეთავაზებული სხვადასხვა კურსი, მათ შორის კიბერჰიგიენის მიმართულებითაც. „პროფესიული საჯარო მოხელის პროფესიული განვითარების საჭიროებების განსაზღვრის წესის, პროფესიული განვითარების სტანდარტისა და წესის დამტკიცების შესახებ“ საქართველოს მთავრობის N242

დადგენილების შესაბამისად, აღნიშნული, თავის მხრივ, წარმოადგენს მოხელის პროფესიული განვითარების არააკრედიტებულ სავალდებულო საბაზისო პროგრამას. ამ მიმართულებით, მთავრობის ადმინისტრაცია გეგმავს ერთიან ელექტრონულ პლატფორმაზე, ბმულის მეშვეობით, განათავსოს სსიპ - ციფრული მმართველობის სააგენტოს მიერ შემუშავებული ონლაინ კურსი და უზრუნველყოს მისი ხელმისაწვდომობა. ეს აქტივობა, დამატებით, ხელს შეუწყობს სსიპ - ციფრული მმართველობის სააგენტოს მიერ შემუშავებული სასწავლო კურსის პოპულარიზაციასაც.

საქართველოს ენერგეტიკისა და წყალმომარაგების მარეგულირებელი ეროვნული კომისია - როგორც საქართველოს ენერგო სექტორის მარეგულირებელი ორგანო და ერთ-ერთი მთავარი დაინტერესებული მხარე, ხელს უწყობს ენერგო სექტორში კიბერუსაფრთხოების გაძლიერებას. როგორც ენერგო სექტორის კრიტიკული ინფორმაციული სისტემის სუბიექტი, საქართველოს ენერგეტიკისა და წყალმომარაგების მარეგულირებელი ეროვნული კომისია ყოველთვის წარმოადგენს კიბერთავდასხმების მთავარ სამიზნეს. ამასთან , სრული გაციფრულების პროცესში, სექტორი კიდევ უფრო მოწყვლადი ხდება. ენერგეტიკის ინფრასტრუქტურა სასიცოცხლოდ მნიშვნელოვანი კომპონენტია ნებისმიერი ქვეყნის ეკონომიკისა და ეროვნული უსაფრთხოებისთვის, შესაბამისად, უმნიშვნელოვანესია ყველა აუცილებელი ზომის მიღება ამ სისტემის კიბერსაფრთხეებისგან დასაცავად. აღნიშნული მიუთითებს იმაზე, რომ აუცილებელია განსაკუთრებული ყურადღება დაეთმოს კრიტიკულ ინფრასტრუქტურას მმართველ კომპანიებში, ასევე მომხმარებლებში ცნობიერების ამაღლებას. ამჟამად მზადდება კიბერუსაფრთხოების საგანმანათლებლო პროგრამა, რომელიც მორგებული იქნება საქართველოს ენერგეტიკისა და წყალმომარაგების მარეგულირებელი ეროვნული კომისიის სასწავლო ცენტრის სტუდენტებზე. სასწავლო ცენტრმა უკვე ჩაატარა რამდენიმე აქტივობა ამ მიმართულებით. კერძოდ, ჩატარდა კიბერჰიგიენის ტრენინგი ენერგო სექტორის კომპანიების წარმომადგენლებისთვის და იმ სტუდენტებისთვის, რომლებიც დაინტერესებულნი იყვნენ ამ კურსით. საქართველოს ენერგეტიკისა და წყალმომარაგების მარეგულირებელი ეროვნული კომისია აქტიურად მონაწილეობს ენერგო ინფრასტრუქტურის კიბერსაფრთხეების წინააღმდეგ მედეგობის გაძლიერებასთან დაკავშირებულ აქტივობებში.

კერძო სექტორის კომპანიები, სამოქალაქო საზოგადოების ორგანიზაციები და ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების ვენდორები დამატებით ახორციელებენ კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების ღონისძიებებს და ხელს უწყობენ მათი პროდუქტებისა და გადაწყვეტილებების საზოგადოებისთვის გაცნობას. კომერციულ ბანკებს და ინტერნეტ მომსახურების პროვაიდერებს (ISPs) აქვთ კიბერცნობიერების ინიციატივები, რომლებიც მზადდება და ინერგება მათი მომხმარებლებისთვის. კიბერუსაფრთხოებისა და ინფორმაციულ - საკომუნიკაციო ტექნოლოგიების ინოვაციების რეგიონული კონფერენცია (GITI), რომელიც წარმოადგენს ყოველწლიურ ღონისძიებას ციფრული მმართველობის და კიბერუსაფრთხოების საკითხებზე, იმართება სხვადასხვა დაინტერესებული მხარეების ჩართულობით ინფორმაციულ-საკომუნიკაციო ტექნოლოგიებისა და კიბერუსაფრთხოების მნიშვნელობის განხილვის მიზნით.

ზოგადი დასკვნის სახით უნდა აღინიშნოს, რომ მიზანმიმართული, კონსოლიდირებული, ყოვლისმომცველი და კარგად კოორდინირებული ცნობიერების ამაღლების ეროვნული დონის პროგრამები და კამპანიები, რომლებიც უზრუნველყოფილია საკმარისი რესურსით, ხელმძღვანელობის მკაფიო ხედვით, მანდატით, სამუშაოს შესრულების ზუსტი ინდიკატორებით და შედეგების გაზომვის შესაძლებლობებით არის ის მკაფიო საჭიროებები და მნიშვნელოვანი მიმართულებები, რომლებსაც უნდა დაეყრდნოს აღნიშნული სტრატეგია და განხორციელდეს მისი სამოქმედო გეგმით.

ხედვა

ინფორმირებულობა არის ერთ-ერთი მთავარი ფაქტორი საზოგადოების დაცვისთვის. მიზანმიმართული ზომების, ინიციატივების და სტრუქტურული განვითარების გზით ხდება მოლოდინების, კომპეტენციების და შესაძლებლობების განვითარება, გაძლიერება და უწყვეტი გაუმჯობესება. შედეგად, გაძლიერდება საზოგადოების კიბერმედეგობის მაჩვენებელი და სამიზნე ჯგუფები შეძლებენ კიბერუსაფრთხოების მომავალ გამოწვევებთან გამკლავებას. ამასთან, მათი როლი ქართულ ციფრულ ეკოსისტემაში უფრო აქტიური გახდება.

მიზნები და ამოცანები

მიზანი 1: სიღრმისეული აღქმა

კიბერუსაფრთხოების სფეროში ცნობიერების დაბალი დონით გამოწვეული პრობლემის აღქმა.

ამოცანა 1.1. კიბერსაფრთხეების და მათი ნეგატიური შედეგების შესახებ ინფორმირებულობის გაზრდის ხელშეწყობა

სამიზნე ჯგუფების უმრავლესობა სათანადოდ ვერ აღიქვამს პრობლემის რეალურად არსებობას და იმას, თუ რა ზიანის მოტანა შეუძლია ამ პრობლემას საზოგადოებისთვის.

პრობლემის აღქმა ზეგავლენას ახდენს ყველა სამიზნე ჯგუფზე. თუმცა, დაინტერესებული მხარეების მრავალფეროვნების გათვალისწინებით, პრობლემის განმარტება, აღწერილობა და მისი გადმოცემის გზები მნიშვნელოვნად განსხვავდება სამიზნე ჯგუფების მიხედვით:

სამიზნე ჯგუფი	პრობლემური საკითხები
ფართო საზოგადოება, მათ შორის რეგიონებში მცხოვრები მოსახლეობა	კიბერუსაფრთხოება ხშირად არ აღიქმება მნიშვნელოვან საკითხად. საფრთხეები, რომლებმაც შეიძლება გამოიწვიოს პერსონალური მონაცემების დაკარგვა ან მათთვის ზიანის მიყენება, მეტწილად უცნობია, ან საკმარისად არ არის აღქმული. პრობლემის არასათანადოდ აღქმა, მისთვის ნაკლები ყურადღების დათმობა, ხშირად გამოწვეულია საბაზისო ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების გამოყენების სათანადო უნარების არ ქონით და ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების/კიბერუსაფრთხოების სფეროსთან დაკავშირებული ტერმინოლოგიების ცოდნის დაბალი დონით მოსახლეობაში.
კრიტიკული ინფორმაციული სისტემების სუბიექტები	კრიტიკული ინფორმაციული სისტემების სუბიექტების უმრავლესობა სათანადოდ აღიქვამს კიბერსაფრთხეებს, თუმცა ყველაფერი მაინც დამოკიდებულია აღნიშნული სექტორის სიმწიფეზე. ხშირად კომპანიები მეტწილად ორიენტირებული არიან მხოლოდ საკუთარ საფრთხეებზე და იმ გავლენაზე, რომელსაც ეს საფრთხე იწვევს. მაგრამ, ისინი ვერ აცნობიერებენ თუ რა გავლენა შეიძლება ჰქონდეს კიბერინციდენტს ეროვნულ დონეზე. ხშირად, კიბერუსაფრთხოებასთან დაკავშირებული საკითხები აღიქმება როგორც უშუალოდ ინფორმაციულ-

	საკომუნიკაციო ტექნოლოგიების და არა ოპერაციული დონის პრობლემა.
სახელმწიფო/საჯარო მოხელეები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში. თუმცა, დამატებით გასათვალისწინებელია ის ფაქტორი, რომ საჯარო მოხელეები ხშირად მუშაობენ კონფიდენციალურ მონაცემებთან და იყენებენ სამთავრობო სისტემებს, თუმცა ვერ აცნობიერებენ მათ მნიშვნელობას და არ იციან თუ როგორ დაიცვან ისინი.
მცირე და საშუალო საწარმოები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში. დამატებით გასათვალისწინებელია, რომ ორგანიზაციასთან და მის საქმიანობასთან დაკავშირებული საფრთხეები ან უცნობია, ან არ არის სათანადოდ აღქმული. შესაბამისად, არ არის მიღებული შესაბამისი ზომები.
მედია	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში. დამატებით გასათვალისწინებელია, რომ ჟურნალისტები კონკრეტულად კიბერუსაფრთხოების და ტექნოლოგიური მიმართულებების გაშუქებაზე არ მუშაობენ (მუშაობენ ზოგადი მიმართულებით) და ხშირად დიდად დაინტერესებულნი არც არიან ამ საკითხებით.
მოსწავლეები და სტუდენტები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში. დამატებით გასათვალისწინებელია, რომ ეს ჯგუფი დროის უმეტეს ნაწილს ონლაინ სივრცეში ატარებს და ყველაზე ხშირად აწყდება შემდეგ საფრთხეებს: • ონლაინ დაშინება • კიბერბულინგი • კიბერგრუმინგი • მონაცემების ქურდობა • კიბერდანაშაული პრობლემის აღქმის დონე დაბალია და ხშირად მხარდაჭერა მშობლების და მასწავლებლების მხრიდანაც მწირია (რადგან, მათაც, თავის მხრივ, აქვთ ცოდნის ნაკლებობა).
მასწავლებლები	მასწავლებლები უშუალოდ მუშაობენ მოსწავლეებთან, რომლებიც დიდ დროს ატარებენ ონლაინ სივრცეში. მათ აქვთ ცოდნის ნაკლებობა კიბერუსაფრთხოების საკითხებზე, რაც თავის მხრივ ხელს უშლის მათ ეფექტიანად დაეხმარონ მოსწავლეებს.
საზოგადოებრივი ორგანიზაციები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების და მცირე და საშუალო საწარმოების შემთხვევაში.

➢ **პრობლემის და მისი შედეგების ურთიერთკავშირის აღქმა**

ამოცანა 1.2. არსებული მდგომარეობის შესახებ ცნობიერების დონის გაზრდის ხელშეწყობა

კიბერუსაფრთხოების სფეროში არსებული სიტუაციის შესახებ არასაკმარისი ინფორმირებულობა იწვევს კომუნიკაციის ხარვეზს უწყებებს შორის და საზოგადოებაში, რესურსების არაეფექტიან გამოყენებას და სხვადასხვა უწყების მიერ განხორციელებული აქტივობების არაეფექტიანობას.

კიბერუსაფრთხოების სფეროში არსებული სიტუაციის შესახებ ინფორმაციის ნაკლებობა გავლენას ახდენს ყველა სამიზნე ჯგუფზე, თუმცა დაინტერესებული მხარეების მრავალფეროვნების გათვალისწინებით საჭირო ინფორმაცია განსხვავდება სამიზნე ჯგუფების მიხედვით:

სამიზნე ჯგუფი	პრობლემური საკითხები
ფართო საზოგადოება, მათ შორის რეგიონებში მცხოვრები მოსახლეობა	არ არის სათანადოდ აღქმული და ფართოდ გავრცელებული ინფორმაცია იმ კიბერსაფრთხეების შესახებ, რომლებიც იწვევს პერსონალური მონაცემების დაკარგვას ან ზიანს აყენებს მომხმარებელს. ასევე, მარტივად გასაგებ ენაზე არ არის ხელმისაწვდომი ინფორმაცია სხვადასხვა სამიზნე ჯგუფების შესაბამის საფრთხეებზე და მათი თავიდან აცილების გზებზე.
კრიტიკული ინფორმაციული სისტემების სუბიექტები	კრიტიკული ინფორმაციული სისტემების სუბიექტები არ არიან სათანადოდ ინფორმირებულები საფრთხეების (Threat Intelligence) შესახებ.
სახელმწიფო/საჯარო მოხელეები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში.
მცირე და საშუალო საწარმოები	კონკრეტულად მცირე და საშუალო საწარმოებზე ორიენტირებული საფრთხეებისგან თავდაცვის მიზნით მარტივად გასაგებ (იმის გათვალისწინებით, რომ მცირე და საშუალო საწარმოებს ძირითადად არ ჰყავთ კიბერ/ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების ექსპერტები) და გამოსაყენებელ ინფორმაციასა და რესურსებზე ხელმისაწვდომობის ნაკლებობა.
მედია	ჟურნალისტებს ხშირად არ აქვთ პირველადი წყაროსგან მიღებული ზუსტი ინფორმაცია არსებული სიტუაციის შესახებ, რომელსაც მარტივად დაამუშავებენ და გამოიყენებენ ფართო საზოგადოებაში ინფორმაციის გასავრცელებლად.
მოსწავლეები და სტუდენტები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში. დამატებით გასათვალისწინებელია, ამ სამიზნე ჯგუფისთვის სპეციფიკური საფრთხეები: • ონლაინ დაშინება • კიბერბულინგი • კიბერგრუმინგი • მონაცემების ქურდობა • კიბერდანაშაული
მასწავლებლები	მასწავლებლებს არ აქვთ ინფორმაცია თანამედროვე კიბერსაფრთხეების შესახებ განსაკუთრებით იმ საფრთხეების შესახებ, რომლებიც უშუალოდ მათ

	მოსწავლეებს ეხება (ონლაინ დაშინება, კიბერბულინგი, ონლაინ ექსპლუატაცია, მონაცემების ქურდობა). მათ არ აქვთ საკმარისი ცოდნა, რომ მოახდინონ მსგავსი პრობლემების პრევენცია ან ეფექტიანად მართვა.
საზოგადოებრივი ორგანიზაციები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების და მცირე და საშუალო საწარმოების შემთხვევაში.

➢ **სახელმწიფოს მხრიდან, კიბერუსაფრთხოების ზოგად ტენდენციებზე, საფრთხეებსა და არსებულ სიტუაციაზე ინფორმაციის გაზიარების გზით საზოგადოებაში ცნობიერების დონის ამაღლება.**

მიზანი 2: კომპეტენციების ზრდა

კომპეტენციების მუდმივი გაუმჯობესება ხელს უწყობს ცნობიერების ამაღლების აქტივობების ჩატარებას ყველა სამიზნე ჯგუფში. ამგვარად, ძლიერდება საზოგადოების კიბერსივრცეში მიზანმიმართულ ან შემთხვევით განვითარებულ ინციდენტებთან გამკლავების უნარი.

ამოცანა 2.1. კიბერუსაფრთხოების სფეროში ჩარჩო დოკუმენტების გაუმჯობესება

პოლიტიკის დოკუმენტების შემუშავების სტანდარტებთან შეუსაბამობა შედეგად იწვევს იმას, რომ შემუშავებული დოკუმენტები ხშირად დუბლირდება და ერთმანეთთან წინააღმდეგობაში მოდის.

სამიზნე ჯგუფი	პრობლემური საკითხები
ფართო საზოგადოება, მათ შორის რეგიონებში მცხოვრები მოსახლეობა	საზოგადოების ფართო ნაწილისთვის არ არის ხელმისაწვდომი ციფრულ სივრცეში უსაფრთხოდ ნავიგაციისთვის, მარტივად გასაგებ ენაზე დაწერილი კიბერჰიგიენის პრინციპები და საუკეთესო პრაქტიკები, რომლითაც მოქალაქეებს შეუძლიათ იხელმძღვანელონ. სახელმძღვანელო პრინციპები უნდა მოიცავდეს მარტივად განსახორციელებელ ინსტრუქციებს რა “შეიძლება” და რა “არ შეიძლება” ციფრული მოწყობილობების გამოყენებისას.
მცირე და საშუალო საწარმოები	დეფიციტურია მცირე და საშუალო საწარმოებისთვის განკუთვნილი, მარტივად გასაგები საბაზისო ინფორმაცია. რთულად ხელმისაწვდომია კიბერჰიგიენის და ციფრული უნარების ჩარჩოები, სახელმძღვანელოები და საუკეთესო პრაქტიკები. მნიშვნელოვანია, რომ ჩარჩოები და სახელმძღვანელოები, მათ შორის პოლიტიკის დოკუმენტები, პროცესები და ტექნიკური რეკომენდაციები (რომლებიც შეეხება კორპორაციულ ინფრასტრუქტურას, მობილურ მოწყობილობებს, ინტერნეტს, მონაცემთა დაცვას და სხვა საკითხებს) მარტივად დასანერგი იყოს საწარმოების ციფრული ცხოვრების თითოეულ ეტაპზე.
კრიტიკული ინფორმაციული სისტემების სუბიექტები	ქვეყანაში კიბერუსაფრთხოების კუთხით კომპანიების და კრიტიკული ინფორმაციული სისტემების სუბიექტების უმრავლესობისთვის განკუთვნილი საჭირო ჩარჩოების, სტანდარტების და საუკეთესო პრაქტიკების დეფიციტია. მნიშვნელოვანია ჩარჩო დოკუმენტები და

	სახელმძღვანელოები მოიცავდნენ მათი დანერგვისთვის მარტივ და გასაგებ ინსტრუქციას, ინფორმაციული უსაფრთხოების მართვის პრაქტიკულ ჩარჩოს (ISMS), დანერგვის ინსტრუქციებს, პროცესების აღწერას და ტექნიკურ რეკომენდაციებს (რომლებიც შეეხება კორპორაციულ ინფრასტრუქტურას, მობილურ მოწყობილობებს, ინტერნეტს, მონაცემთა დაცვას და სხვა საკითხებს).
სახელმწიფო/საჯარო მოხელეები	იგივე პრაქტიკაა, რაც მცირე და საშუალო საწარმოების შემთხვევაში.
მედია	იგივე პრაქტიკაა, რაც მცირე და საშუალო საწარმოების შემთხვევაში.
მოსწავლეები და სტუდენტები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში, თუმცა ყურადღება მახვილდება ახალგაზრდების კონკრეტულ საჭიროებებზე, რომლებიც დიდ დროს ატარებენ ონლაინ და სოციალურ მედიაში.
მასწავლებლები	მასწავლებლებისთვის არ არის ხელმისაწვდომი სპეციალიზებული ჩარჩოები და სახელმძღვანელოები, რომლებიც მათ დაეხმარებოდა კიბერუსაფრთხოების საკითხების ინტეგრირებაში საგანმანათლებლო პროცესში. მნიშვნელოვანია არსებობდეს პედაგოგიური მიდგომების და მეთოდოლოგიების სტანდარტი, რომლითაც მასწავლებლები შეძლებენ მოსწავლეებისთვის კიბერუსაფრთხოების საბაზისო პრინციპების სწავლებას.
საზოგადოებრივი ორგანიზაციები	იგივე პრაქტიკაა, რაც მცირე და საშუალო საწარმოების შემთხვევაში.

➢ ეფექტიანი აქტივობების განხორციელება კიბერუსაფრთხოების სფეროში ცნობიერების დონის ამაღლების მიმართულებით მოიცავს ან სულ მცირე შესაძლებლობის ფარგლებში ითვალისწინებს ფართოდ მისაღებ ჩარჩოებს, სახელმძღვანელოებს, საუკეთესო ან კარგ პრაქტიკებს.

ამოცანა 2.2. კიბერუსაფრთხოების სფეროში მარტივად გასაგები, ერთიანი პრაქტიკების შემუშავება

კიბერუსაფრთხოების შეუსაბამო პრაქტიკები ხელს უწყობს ახალი სისუსტეების წარმოქმნას და ზოგადად, ასუსტებს ქვეყნის მედეგობას კიბერსაფრთხეების მიმართ.

სამიზნე ჯგუფი	პრობლემური საკითხები
ფართო საზოგადოება, მათ შორის რეგიონებში მცხოვრები მოსახლეობა	იხილეთ ამოცანა 2.1
მცირე და საშუალო საწარმოები	იხილეთ ამოცანა 2.1
კრიტიკული ინფორმაციული სისტემების სუბიექტები	იხილეთ ამოცანა 2.1
სახელმწიფო/საჯარო მოხელეები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში (მომხმარებლის პერსპექტივიდან).

მედია	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში (მომხმარებლის პერსპექტივიდან).
მოსწავლეები და სტუდენტები	იხილეთ ამოცანა 2.1
მასწავლებლები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში. დამატებით, იმის გათვალისწინებით, რომ მასწავლებლები ხშირად სარგებლობენ ციფრული ტექნოლოგიებით საკლასო ოთახში, მათთვის აუცილებელია საგანმანათლებლო კონტექსტზე მორგებული კიბერუსაფრთხოების პრაქტიკების ფლობა.
საზოგადოებრივი ორგანიზაციები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში (მომხმარებლის პერსპექტივიდან).

➢ **ინფორმაციულ - საკომუნიკაციო ტექნოლოგიებით სარგებლობისას საერთო, საფრთხეებზე მორგებული პრაქტიკების შემუშავება.**

ამოცანა 2.3. კიბერუსაფრთხოების უნარების განვითარების ხელშეწყობა

თანამშრომლები, რომელთაც არ აქვთ ინფორმაციულ-საკომუნიკაციო ტექნოლოგიებით სარგებლობის სათანადო ცოდნა და უნარები, ვერ დაიცავენ თავს კიბერსაფრთხეებისგან სამუშაო სივრცეში .

სამიზნე ჯგუფი	პრობლემური საკითხები
ფართო საზოგადოება, მათ შორის რეგიონებში მცხოვრები მოსახლეობა	საზოგადოება არ არის ინფორმირებული თუ როგორ უნდა მოხდეს ისეთი საფრთხეების იდენტიფიცირება და პრევენცია როგორიც არის საზიანო პროგრამები, სპამი, თაღლითობა და სხვა. აქედან გამომდინარე, სამიზნე ჯგუფი უფრო მოწყვლადია და ხშირად ხდება კიბერდანაშაულის მსხვერპლი. აღნიშნული განსაკუთრებით მნიშვნელოვანია საბაზისო განათლების მქონე, ხანდაზმული და სოფლად მაცხოვრებელი პირების შემთხვევაში. ამ ჯგუფებისთვის აუცილებელია მოიძებნოს განსხვავებული ფორმატები, რომლებიც მათი საჭიროებების დაკმაყოფილებას უზრუნველყოფს.
მცირე და საშუალო საწარმოები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში (მომხმარებლის პერსპექტივიდან). რაც შეეხება მართვას, ინფორმაციული ტექნოლოგიების და ინფორმაციული უსაფრთხოების სისტემების მართვა ხშირად წარმოადგენს პრობლემას. ამ სამიზნე ჯგუფში გამოწვევას წარმოადგენს კომპეტენციების, კიბერუსაფრთხოების საბაზისო ჩარჩოების ცოდნის და მათი დანერგვის საკითხი.
კრიტიკული ინფორმაციული სისტემების სუბიექტები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში (მომხმარებლის პერსპექტივიდან). მართვის კუთხით, ხშირად, პრობლემას წარმოადგენს ინფორმაციული უსაფრთხოების სისტემების მართვის უნარების საუკეთესო პრაქტიკებთან (ISMS) შესაბამისობა. გამოწვევას წარმოადგენს, ასევე კანონით გათვალისწინებული მინიმალური მოთხოვნების სწორად აღქმა და დანერგვა.
სახელმწიფო/საჯარო მოხელეები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში (მომხმარებლის პერსპექტივიდან). მართვის კუთხით, იგივე

	პრაქტიკაა, რაც მცირე და საშუალო საწარმოების შემთხვევაში.
მედია	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში (მომხმარებლის პერსპექტივიდან). მედიის შემთხვევაში აღნიშნული პრობლემა იწვევს შესაბამისი ინფორმაციის და მედია დაფარვის შეუძლებლობას. მართვის კუთხით, იგივე პრაქტიკაა, რაც მცირე და საშუალო საწარმოების შემთხვევაში.
მოსწავლეები და სტუდენტები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში, თუმცა განსაკუთრებული ყურადღება მახვილდება იმ უნარებზე, რომლებიც აუცილებელია ახალგაზრდა თაობისთვის, რომლებიც დროის უმეტეს ნაწილს ატარებენ ონლაინ და სოციალურ მედიაში. ამ ჯგუფისთვის დაინტერესებულ მხარეს დამატებით წარმოადგენენ მშობლები, რომლებსაც არ აქვთ საბაზისო ცოდნა თუ როგორ უზრუნველყონ ისეთი გარემო საკუთარი შვილებისთვის (განსაკუთრებით მცირეწლოვანი ბავშვებისთვის), რომელიც დაიცავს მათ ონლაინ ექსპლუატაციის და სხვა საფრთხეებისგან (შინაარსის გაფილტვრა, კონტროლი).
მასწავლებლები	აუცილებელია მასწავლებლები ფლობდნენ კიბერუსაფრთხოების უნარებს პირადი სარგებლობისთვის, ასევე პედაგოგიურ უნარებს კიბერუსაფრთხოების საკითხების სწავლებისთვის. მათ უნდა შეძლონ სწავლების პროცესში უსაფრთხო ციფრული გარემოს შექმნა და მოსწავლეებში კიბერუსაფრთხოების კულტურის დანერგვა. მნიშვნელოვანია, რომ მასწავლებლებმა გაიუმჯობესონ შესაბამისი უნარები, რათა ეფექტიანად მოახდინონ კიბერბულინგის და სხვა ონლაინ საფრთხეების იდენტიფიცირება და მართვა.
საზოგადოებრივი ორგანიზაციები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში (მომხმარებლის პერსპექტივიდან). მართვის კუთხით, იგივე პრაქტიკაა, რაც მცირე და საშუალო საწარმოების შემთხვევაში.

➢ **კიბერუსაფრთხოების მედეგობის გაზრდის მიზნით ციფრული უნარების განვითარება სხვადასხვა სამიზნე ჯგუფებში.**

ამოცანა 2.4. დაგეგმილი აქტივობების განხორციელების მიზნით რესურსების გაზრდის ხელშეწყობა

კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების მიზნით განსაზღვრული რესურსების სიმწირე, ხშირ შემთხვევაში, იწვევს იმას, რომ მიმდინარე აქტივობები და

პროექტები სრულად ვერ სრულდება. შესაბამისად, ძირითადი გამოწვევები და პრობლემები გადაუჭრელი რჩება.

სამიზნე ჯგუფი	პრობლემური საკითხები
ფართო საზოგადოება, მათ შორის რეგიონებში მცხოვრები მოსახლეობა	-
მცირე და საშუალო საწარმოები	მცირე და საშუალო საწარმოებს ხშირად არ აქვთ რესურსები კიბერუსაფრთხოების მიზნებისთვის. საუკეთესო შემთხვევაში, უსაფრთხოების საკითხები იმართება ინფორმაციული და საკომუნიკაციო ტექნოლოგიების სპეციალისტების მიერ, მაგრამ ხშირ შემთხვევაში, კომპანიებში ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების გამოყენების კუთხითაც არის პრობლემები. ამასთან, დეფიციტია იმ ადამიანური კაპიტალის, რომელსაც შესაბამისი ცოდნის საფუძველზე შეუძლია კომპანიის თანამშრომლების ცნობიერების დონის ამაღლებაზე იზრუნოს.
კრიტიკული ინფორმაციული სისტემების სუბიექტები	ხშირად, კრიტიკული ინფორმაციული სისტემების სუბიექტებსაც კი არ ჰყავთ შესაბამისი უნარების მქონე ექსპერტები როგორც რაოდენობრივი, ასევე პროფესიული თვალსაზრისით. მხოლოდ რამდენიმე სექტორს (მაგ. საბანკო სექტორი) აქვს საკმარისი რესურსი, რომელიც უზრუნველყოფს კიბერუსაფრთხოების საუკეთესო პრაქტიკების შესაბამისად მართვას. დანარჩენები, დამოკიდებული არიან გარე მხარდაჭერაზე, მაგ. სერვის პროვაიდერებზე, რომელთაც ხშირ შემთხვევაში თავადაც აქვთ კიბერუსაფრთხოების კუთხით მსგავსი პრობლემები.
სახელმწიფო/საჯარო მოხელეები	იგივე პრაქტიკაა, რაც მცირე და საშუალო საწარმოების შემთხვევაში.
მედია	იგივე პრაქტიკაა, რაც მცირე და საშუალო საწარმოების შემთხვევაში.
მოსწავლეები და სტუდენტები	-
მასწავლებლები	მასწავლებლებს ხშირად არ აქვთ წვდომა სპეციალიზებულ რესურსებზე, რომლებიც განკუთვნილია საგანმანათლებლო პროცესისთვის. მათ უნდა ჰქონდეთ წვდომა სასწავლო მასალებზე, სახელმძღვანელოებსა და ციფრულ ინსტრუმენტებზე, რომლებიც დაეხმარებათ მოსწავლეებისთვის კიბერუსაფრთხოების საკითხების სწავლებაში.
საზოგადოებრივი ორგანიზაციები	იგივე პრაქტიკაა, რაც მცირე და საშუალო საწარმოების შემთხვევაში.

➢ **ცნობიერების ამაღლების მიზნით განსაზღვრული აქტივობების განხორციელებისთვის შესაბამისი დაფინანსების გამოყოფა, ხარჯებსა და სარგებელს შორის ოპტიმალური წონასწორობის დაცვის და პასუხისმგებლობების გათვალისწინებით.**

მიზანი 3: კომუნიკაციის გაუმჯობესება

კომუნიკაცია სხვადასხვა სამიზნე ჯგუფებს შორის საკვანძო ფაქტორია თანმიმდევრული ცნობიერების ჩარჩოს ჩამოყალიბებისთვის.

ამოცანა 3.1. კიბერუსაფრთხოების სფეროში მომუშავე ორგანიზაციების განვითარების ხელშეწყობა

ისეთი უწყებების არსებობა, რომლებიც დაეხმარებიან დაინტერესებულ მხარეებს კიბერუსაფრთხოების სისტემის გაძლიერებაში, ხოლო ორგანიზაციებს - კიბერუსაფრთხოების სფეროში ცოდნის გაღრმავებაში; აღნიშნული, თავის მხრივ, განსხვავებული პერსპექტივების ინტეგრაციას და ყოვლისმომცველი საკომუნიკაციო ქსელის ჩამოყალიბებას შეუწყობს ხელს.

სამიზნე ჯგუფი	პრობლემური საკითხები
ფართო საზოგადოება, მათ შორის რეგიონებში მცხოვრები მოსახლეობა	არ არსებობს ორგანიზაცია, რომელსაც აქვს საკმარისი რესურსი, ხელი შეუწყოს კიბერუსაფრთხოების კუთხით საზოგადოების ცოდნის ამაღლებას. ასევე, არ არსებობს ინიციატივები, რომლებიც ხელს შეუწყობს მოქალაქეებს, თემის დონეზე გაავრცელოს ცოდნა კიბერუსაფრთხოების მიმართულებით.
მცირე და საშუალო საწარმოები	არ არის განსაზღვრული ორგანიზაცია, რომელიც დაეხმარება მცირე და საშუალო საწარმოებს კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების და საჭიროებების დაკმაყოფილების კუთხით.
კრიტიკული ინფორმაციული სისტემების სუბიექტები	-
სახელმწიფო/საჯარო მოხელეები	-
მედია	-
მოსწავლეები და სტუდენტები	არ არსებობს ოფიციალური უწყება, რომელიც მუშაობს მოსწავლეების და სტუდენტების კიბერბულინგის, კიბერჩაგვრის, ონლაინ ექსპლუატაციის და სხვა საკითხებზე.
მასწავლებლები	არ არსებობს სპეციალიზებული უწყება, რომელიც მასწავლებლებს დაეხმარება უსაფრთხო საგანმანათლებლო გარემოს შექმნაში.
საზოგადოებრივი ორგანიზაციები	არ არის განსაზღვრული ორგანიზაცია, რომელიც ორიენტირებული იქნება კიბერუსაფრთხოების საკითხებზე, და რომელიც დახმარებას აღმოუჩენს საზოგადოებრივ ორგანიზაციებს კიბერუსაფრთხოების კუთხით.

➢ **მჭიდრო, უწყვეტი და მდგრადი თანამშრომლობის უზრუნველყოფა სამთავრობო, საზოგადოებრივ ორგანიზაციებსა და ინტერესთა ჯგუფებს შორის, რადგან ისინი წარმოადგენენ მნიშვნელოვან პარტნიორებს კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების სტრატეგიის დანერგვის პროცესში.**

ამოცანა 3.2. კომუნიკაციის პლატფორმების განვითარების ხელშეწყობა

კიბერუსაფრთხოების ცნობიერების ამაღლების მიზნით შექმნილი კომუნიკაციის პლატფორმები ხელს უწყობს ინფორმაციის გაცვლას და ორგანიზაციებს შორის სინერგიას.

სამიზნე ჯგუფი	პრობლემური საკითხები
ფართო საზოგადოება, მათ შორის რეგიონებში მცხოვრები მოსახლეობა	არ არსებობს პლატფორმა, რომლის მეშვეობითაც ფართო საზოგადოება მიიღებს რჩევას თუ როგორ მოემზადოს კიბერ თავდასხმის და თაღლითობისთვის. ასეთი პლატფორმები მორგებული უნდა იყოს კონკრეტულ ჯგუფებზე, მაგალითად ხანდაზმული და ახალგაზრდა ადამიანები (იხ. „მოსწავლეები და სტუდენტები“).
მცირე და საშუალო საწარმოები	არ არსებობს პლატფორმა, სადაც მცირე და საშუალო საწარმოები მიიღებენ რჩევას თუ როგორ მოემზადონ კიბერთავდასხმისა და თაღლითობისთვის.
კრიტიკული ინფორმაციული სისტემების სუბიექტები	არ არსებობს სანდო საკომუნიკაციო პლატფორმა, სადაც შესაძლებელი იქნება ინციდენტებთან დაკავშირებული ცოდნის გაცვლა.
სახელმწიფო/საჯარო მოხელეები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში (მომხმარებლის პერსპექტივიდან).
მედია	იგივე პრაქტიკაა, რაც მცირე და საშუალო საწარმოების შემთხვევაში.
მოსწავლეები და სტუდენტები	არ არსებობს პლატფორმა, სადაც მოსწავლეები, სტუდენტები და მათი მშობლები მიიღებენ რეკომენდაციებს თუ როგორ მოემზადონ კიბერთავდასხმისა და თაღლითობისთვის, და სადაც ყურადღება გამახვილებული იქნება კიბერბულინგზე, ჩაგვრაზე, კიბერგრუმინგზე, ონლაინ ექსპლუატაციასა და სხვა მსგავს საკითხებზე.
მასწავლებლები	მასწავლებლებისთვის არ არსებობს სპეციალიზებული პლატფორმა, სადაც მათ შესაძლებლობა ექნებათ გაეცნონ კარგ პრაქტიკებს, დაამყარონ კავშირი კიბერუსაფრთხოების ექსპერტებთან ან მიიღონ მითითებები, როგორ უნდა დაეხმარონ მოსწავლეებს კიბერუსაფრთხოების საკითხებში.
საზოგადოებრივი ორგანიზაციები	იგივე პრაქტიკაა, რაც მცირე და საშუალო საწარმოების შემთხვევაში.

➢ ეფექტიანი საკომუნიკაციო პლატფორმების განვითარება, რომლებიც ხელს შეუწყობს კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების კუთხით დაინტერესებულ მხარეებს შორის თანამშრომლობის დამყარებას და შენარჩუნებას.

ამოცანა 3.3. საკონტაქტო პირების/ პუნქტების შექმნა/გაძლიერება

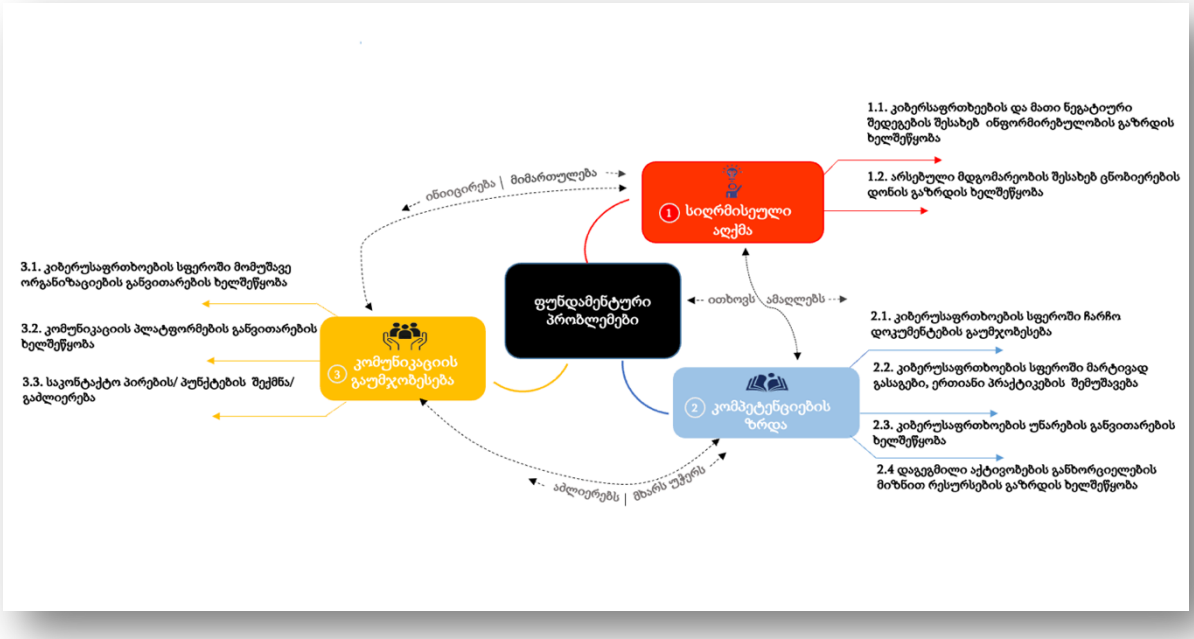
წინასწარ განსაზღვრული ინფორმაცია საკონტაქტო პირების შესახებ, სადაც შესაძლებელია პრობლემების დაფიქსირება, ხელს უწყობს კიბერუსაფრთხოების ვითარების კონტროლს და აჩენს დაცულობის და თავდაჯერებულობის განცდას საზოგადოებაში.

სამიზნე ჯგუფი	პრობლემური საკითხები
ფართო საზოგადოება, მათ შორის რეგიონებში მცხოვრები მოსახლეობა	მოქალაქეები იშვიათად აფიქსირებენ კიბერინციდენტებს, ან თაღლითობის შემთხვევებს, რაც განპირობებულია სახელმწიფო ინსტიტუტების მიმართ ნდობის ნაკლებობით. ხშირად საზოგადოებამ არც კი იცის თუ ვის, ან როგორ

	მიმართოს. მარტივად ხელმისაწვდომი, სანდო კონტაქტების არსებობა ხელს შეუწყობს მოქალაქეებს სწორად დააფიქსირონ კიბერინციდენტები და მიიღონ შესაბამისი მხარდაჭერა.
მცირე და საშუალო საწარმოები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში.
კრიტიკული ინფორმაციული სისტემების სუბიექტები	კანონმდებლობით განსაზღვრულია შემთხვევების დაფიქსირების ვალდებულება, მაგრამ ხშირად ზუსტი პროცედურები არ არის ცნობილი, ან არ ხდება მათი გათვალისწინება.
სახელმწიფო/საჯარო მოხელეები	იგივე პრაქტიკაა, რაც ფართო საზოგადოების შემთხვევაში.
მედია	მედიას არ ჰყავს კონკრეტული საკონტაქტო პირი, რომელიც მიაწვდის ინფორმაციას კიბერუსაფრთხოების საკითხებზე. შესაბამისად, არსებული მდგომარეობით არ ხდება მედიის, როგორც საზოგადოებისთვის ინფორმაციის მიწოდების საშუალების გამოყენება.
მოსწავლეები და სტუდენტები	მწირია სანდო პლატფორმების და კონტაქტების რაოდენობა (ბარიერების გარეშე და ემპათიით გამსჭვალული), სადაც მსხვერპლი შეძლებს დანაშაულის დაფიქსირებას.
მასწავლებლები	მასწავლებლებს არ ჰყავთ კონკრეტული საკონტაქტო პირები, ვისაც შეიძლება მიმართონ ინციდენტების შემთხვევაში.
საზოგადოებრივი ორგანიზაციები	იგივე პრაქტიკაა, რაც საზოგადოების შემთხვევაში.

- **ინსტიტუციურ დონეზე, კიბერუსაფრთხოების საკითხებზე, სხვადასხვა სამიზნე ჯგუფზე მორგებული საკონტაქტო პირების გამოყოფა, რომელთა ვინაობაც ცნობილი იქნება შესაბამისი სამიზნე ჯგუფებისთვის.**

შედეგად, ლოგიკური ჩარჩოს შესაბამისად, ყალიბდება ქვემოთ მოცემული სტრუქტურა



გამოსახულება №2: ლოგიკური ჩარჩო კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების სტრატეგიისთვის

სტრატეგიის შემუშავების და განხორციელების პროცესი

კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების სტრატეგიის შემუშავების პროცესი:

გამოსახულება №3: ცნობიერების ამაღლების სტრატეგიის შემუშავება

დოკუმენტის **მომზადების** ეტაპზე, კიბერუსაფრთხოების ეროვნულ სტრატეგიაზე დაყრდნობით განისაზღვრა დაინტერესებული მხარეები და უწყებები. ასევე, განისაზღვრა ის სამიზნე ჯგუფები, რომლისთვისაც მნიშვნელოვანია კიბერუსაფრთხოების სფეროში ცოდნის გაღრმავება. მეორე ეტაპზე განხორციელდა არსებული სიტუაციის **ანალიზი**. ამავე ეტაპზე თავი მოეყარა ყველა უწყების მიერ დაგეგმილ აქტივობას, ღონისძიებას, ინიციატივას და პროექტს. **დაგეგმვის** ეტაპზე გაანალიზდა აქტივობები, განისაზღვრა სტრატეგიის მიზნები და ამოცანები. აღნიშნული აქტივობები პასუხისმგებელი და პარტნიორი უწყებების ჩართულობით მოერგო სამიზნე ჯგუფებს. აქტივობების **შეფასების** ეტაპზე დაიდენტიფიცირდა ის ღონისძიებები, რომელთა განხორციელებაც დახარჯული რესურსის და მოსალოდნელი შედეგების გათვალისწინებით ყველაზე ეფექტიანი იქნება საქართველოში. **განხორციელების** ეტაპზე სამოქმედო გეგმით განსაზღვრული აქტივობები ხორციელდება პასუხისმგებელი უწყების მიერ, პარტნიორი ორგანიზაციების მხარდაჭერით. საბოლოო, **მონიტორინგის** ეტაპზე, ფასდება შესრულების ინდიკატორები, რომლებიც განსაზღვრავს აქტივობების შესრულების სტატუსს და მის წარმატებას.

აქტივობების შესრულების მონიტორინგის შესახებ ინფორმაცია შესაძლებელია მიეწოდოს ყველა დაინტერესებულ მხარეს.

ცნობიერების ამაღლების სტრატეგია უნდა შეესაბამებოდეს კიბერუსაფრთხოების ეროვნული სტრატეგიის მოთხოვნებს და უნდა გადაიხედოს მისი განახლების ციკლის შესაბამისად. რაც შეეხება სამოქმედო გეგმას, დოკუმენტი გადახედვას ექვემდებარება წელიწადში ერთხელ.

მონიტორინგი და შეფასება

კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების სტრატეგიას თან ერთვის სამოქმედო გეგმა. სტრატეგია, მიზნები და ამოცანები, რომლებიც განსაზღვრულია წინამდებარე დოკუმენტით უნდა გადაიხედოს საჭიროების შესაბამისად.

სამოქმედო გეგმა წარმოადგენს სტრატეგიის განხორციელების სამუშაო გეგმას. ის განსაზღვრავს კონკრეტულ ზომებს, რომლებიც უნდა გატარდეს ყველა დაინტერესებული მხარის მიერ. სამოქმედო გეგმით გათვალისწინებულია, ასევე, აქტივობების შესრულების ინდიკატორები, რომლის მიხედვითაც განხორციელდება სტრატეგიის შესრულების მონიტორინგი და შეფასება.

განხორციელება

კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების 2025-2030 წლების სტრატეგიის შესრულებას კოორდინაციას უწევს საქართველოს იუსტიციის სამინისტროს სსიპ - ციფრული მმართველობის სააგენტო.

წინამდებარე სტრატეგიის განხორციელების მთავარ მექანიზმს წარმოადგენს თანდართული სამოქმედო გეგმა, რომელიც განსაზღვრავს კონკრეტულ შესასრულებელ მიზნებს, პასუხისმგებელ უწყებებს და შესაბამის რესურსებს. სამოქმედო გეგმის შესრულება წარმოადგენს ამავე დოკუმენტით განსაზღვრული პასუხისმგებელი უწყებების ვალდებულებას. თუმცა პარტნიორმა უწყებებმა, მათი კომპეტენციის ფარგლებში, ხელი უნდა შეუწყონ პასუხისმგებელ უწყებებს სამოქმედო გეგმით განსაზღვრული აქტივობების შესრულების პროცესში. პასუხისმგებელი უწყება უფლებამოსილია შექმნას სამუშაო ჯგუფი, რომელიც პარტნიორ უწყებებს ან/და სხვა პასუხისმგებელ უწყებებს ჩართავს აქტივობების განხორციელების პროცესში.

კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების 2025-2030 წლების სტრატეგიაში და მის სამოქმედო გეგმაში ცვლილებები ხორციელდება სტრატეგიის შესრულების პროგრესის წარმატებისა და განხორციელების პროცესში იდენტიფიცირებული გამოწვევების შესაბამისად.

სტრატეგიის სამოქმედო გეგმის განხორციელება ძირითადად დაგეგმილია სახელმწიფო ბიუჯეტიდან, თუმცა დამატებით შესაძლებლობად, ასევე განიხილება დონორი ორგანიზაციების ფინანსური მხარდაჭერაც.

დოკუმენტის დასასრული