კრიტიკული ინფორმაციული უსაფრთხოების სისტემის სუბიექტებისა და ინფორმაციული უსაფრთხოების დაცვის საკითხებთან დაკავშირებული საკანონმდებლო რეგულაციები

დოქ. ოთარ ჩახუნაშვილი
პერსონალურ მოინაცემთა დაცვის სამსახურის უფროსის პირველი მოადგილე, თსუ-ის მოწვეული ლექტორი

1. შესავალი

თანამედროვე სამყაროში ტექნოლოგიების განვითარებასთან ერთად ეტაპობრივად იზრდება ინფორმაციული უსაფრთხოებისა და მონაცემების სათანადოდ დაცვის მნიშვნელობა. არსებული გამოწვევების საპასუხოდ, საქართველოში მნიშვნელოვანი საკანონმდებლო ცვლილებები და რეფორმები განხორციელდა. მათ შორის გამორჩეულია 2012 წელს ამოქმედებული ორი კანონი - „ინფორმაციული უსაფრთხოების შესახებ", რომელმაც დაარეგულირა ინფორმაციული უსაფრთხოების ორგანიზებისა და კიბერუსაფრთხოების ორგანიზების საბაზისო საკითხები და „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი, რომლითაც პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებულ ისეთ მნიშვნელოვან საკითხებთან ერთად, როგორებიცაა მონაცემთა დამუშავების პრინციპები და სამართლებრივი საფუძვლები, შემუშავდა მონაცემთა უსაფრთხოების დაცვის წესები. მითითებული კანონების დაცვის მნიშვნელობას ასევე ადასტურებს ის ფაქტიც, რომ მათი დარღვევისთვის დადგინდა ადმინისტრაციული პასუხისმგებლობა და განისაზღვრა შესაბამისი ადმინისტრაციულ სახდელები.

ინფორმაციული უსაფრთხოების შესახებ კანონმდებლობის ნაწილში აღსანიშნავია ბოლო წლებში განხორციელებული ცვლილებები და გატარებული რეფორმები, რომლის ფარგლებშიც განისაზღვრნენ კრიტიკული ინფორმაციული სისტემების სუბიექტები, რომლებიც ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით აღიჭურვნენ მთელი რიგი ვალდებულებებით და მათი შესრულების მიზნით შეიქმნა შესაბამისი საზედამხედველო მექანიზმები. შესასრულებლად სავალდებულო მოქმედებების რაოდენობისა და მოცულობის გათვალისწინებით, მათი პრაქტიკაში სათანადოდ დანერგვის მიზნით კი კანონმდებლობით განისაზღვრა შესაბამისი ვადები და ეტაპები.

ზემოაღნიშნულ საკითხებთან დაკავშირებულ რეგულაციებთან ერთად კვლევის ფარგლებში განხილული და აღწერილია დასახელებულ სფეროში მოქმედი კანონმდებლობა, მათ შორის კრიტიკული ინფორმაციული სისტემების მართვაში ჩართული უწყებების კომპეტენციები, კრიტიკული ინფორმაციული სუბიექტები, მათთვის დაწესებული ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები, აგრეთვე, რისკების მართვასთან, მონაცემთა უსაფრთხოების დაცვასთან და საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმებასთან დაკავშირებული საკითხები და სხვა საკანონმდებლო რეგულაციები.

2. კრიტიკული ინფორმაციული სისტემის სუბიექტები

საქართველოს კანონმდებლობაში ინფორმაციული უსაფრთხოების სფეროში ბოლო პერიოდში განხორციელებულ ცვლილებებსა და არსებულ სიახლეებს შორის გამოსაყოფია 2021 წლის ბოლოს მიღებული მთავრობის დადგენილება, რომლითაც დამტკიცდა პირველი, მეორე და მესამე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხა. განხორციელებული საკანონმდებლო ცვლილებების შესაბამისად, „ინფორმაციული უსაფრთხოების შესახებ" კანონი, მათ შორის, გავრცელდა ისეთ კომპანიებზე, რომელთა ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის, ეკონომიკური უსაფრთხოების, ხელისუფლების ან საზოგადოებრივი ცხოვრების შენარჩუნებისათვის.

საქართველოს მთავრობის ზემოაღნიშნული დადგენილების თანახმად, კრიტიკული ინფორმაციული სისტემის სუბიექტები დაიყო 3 (სამ) კატეგორიად:

- **I კატეგორია** - სახელმწიფო და მუნიციპალური ორგანოები და სახელმწიფო საწარმოები;
- **II კატეგორია** - საქართველოს მთავრობის დადგენილებით განსაზღვრული ელექტრონული კომუნიკაციების კომპანიები;
- **III კატეგორია** - საქართველოს მთავრობის დადგენილებით განსაზღვრული კერძო კომპანიები.

აქვე აღსანიშნავია, რომ ნებისმიერ იურიდიულ პირს ან სახელმწიფო ხელისუფლების ორგანოს, რომელიც არ არის კრიტიკული ინფორმაციული სისტემის სუბიექტი, უფლება აქვს, ნებაყოფლობით აიღოს ამ კანონიდან გამომდინარე ვალდებულებები.

3. კრიტიკული ინფორმაციული სისტემების მართვაში ჩართული უწყებები

ინფორმაციული სისტემების მართვაში ჩართულია არაერთი უწყება, რომლებიც კომპეტენციის ფარგლებში უზრუნველყოფენ ქვეყანაში ინფორმაციული უსაფრთხოების სათანადო გარემოს შექმნას, მათ შორის, ხსენებული უწყებების საზედამხედველო სფეროს დაქვემდებარებული საჯარო თუ კერძო ორგანიზაციებისთვის სავალდებულოდ შესასრულებელი მითითებების დადგენის გზით.

3.1. ოპერატიულ-ტექნიკური სააგენტო

სსიპ საქართველოს ოპერატიულ-ტექნიკური სააგენტო (შემდგომში – ოპერატიულ-ტექნიკური სააგენტო) არის საქართველოს სახელმწიფო უსაფრთხოების სამსახურის მმართველობის სფეროში შემავალი საჯარო სამართლის იურიდიული პირი, რომელიც თავისი კომპეტენციის ფარგლებში უზრუნველყოფს ფარული მეთვალყურეობის ღონისძიებების განხორციელებას და სახელმწიფო უწყებებისა და დაწესებულებების საინფორმაციო-ტექნოლოგიურ უზრუნველყოფას.[1]

ოპერატიულ-ტექნიკურ სააგენტოს წამყვანი როლი აკისრია ქვეყანაში ინფორმაციული უსაფრთხოების ორგანიზებასა და უზრუნველყოფაში. აღნიშნულს ადასტურებს ის გარემოებაც, რომ „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის თანახმად, ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნები პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის განისაზღვრება ოპერატიულ-ტექნიკური სააგენტოს უფროსის ბრძანებით. ამასთან, ინფორმაციული უსაფრთხოების სფეროში მთელი რიგი საკითხები დარეგულირებულია ოპერატიულ-ტექნიკური სააგენტოს უფროსის ადმინისტრაციულ-სამართლებრივი აქტებით, რომლებიც აღწერილია მოცემული კვლევის ფარგლებში.

3.2. ციფრული მმართველობის სააგენტო

იუსტიციის სამინისტროს მმართველობის

[1] საჯარო სამართლის იურიდიული პირის საქართველოს ოპერატიულ-ტექნიკური სააგენტოს დებულების პირველი მუხლი, <https://matsne.gov.ge/ka/document/view/3625121?publication=1> [05/12/2022].

სფეროში შემავალი სსიპ ციფრული მმართველობის სააგენტო (შემდგომში - ციფრული მმართველობის სააგენტო), ოპერატიულ-ტექნიკურ სააგენტოს შემდეგ წარმოადგენს იმ ძირითად უწყებას, რომელიც უზრუნველყოფს ქვეყანაში ინფორმაციული უსაფრთხოების სათანადო გარანტიების არსებობას, მათ შორის მინიმალური მოთხოვნების განსაზღვრისა და ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების მომზადების გზით. აღნიშნული გამოიხატება იმაშიც, რომ მინიმალური უსაფრთხოების მოთხოვნები მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის განისაზღვრება ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით.

3.3. თავდაცვის სამინისტროს სისტემაში შემავალი სსიპ კიბერუსაფრთხოების ბიურო

კიბერუსაფრთხოების ბიურო არის საქართველოს თავდაცვის სამინისტროს სისტემაში მოქმედი საჯარო სამართლის იურიდიული პირი, რომლის ძირითადი მიზანია თავდაცვის სამინისტროს კრიტიკული ინფორმაციული სისტემის სუბიექტებში შექმნა და სტაბილური, ეფექტიანი და უსაფრთხო ინფორმაციული და საკომუნიკაციო სისტემების განვითარება.

ბიურო ახორციელებს ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ქმედებების, კიბერშეტევებისა და კომპიუტერული უსაფრთხოების ინციდენტების პრევენციულ და რეაქციულ მართვას.

კიბერუსაფრთხოების ბიურო განსაზღვრავს და შეიმუშავებს თავდაცვის სფეროში ინფორმაციული უსაფრთხოების პოლიტიკას და ადგენს ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს.[2]

3.4. კომპიუტერულ ინციდენტებზე დახმარების ჯგუფები

საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, აგრეთვე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ, მასთან დაკავშირებულ სხვა საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებენ ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი (cert.ota.gov.ge), ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი (cert.dea.gov.ge) და კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი.[3]

„ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის მე-8 მუხლის მე-2 პუნქტის თანახმად კი, კიბერუსაფრთხოების პრიორიტეტულ საფრთხეებს მიეკუთვნება:

- კიბერშეტევა, რომელიც საფრთხეს უქმნის ადამიანთა სიცოცხლესა და ჯანმრთელობას, სახელმწიფო ინტერესებს ან ქვეყნის თავდაცვისუნარიანობას;
- კიბერშეტევა კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული სისტემების წინააღმდეგ;
- კიბერშეტევა, რომელიც საფრთხეს უქმნის სახელმწიფოს, ორგანიზაციის ან კერძო პირის ფინანსურ რესურსებს ან/და საკუთრების უფლებას;
- სხვა ნებისმიერი ქმედება, რომელიც, მისი ხასიათიდან, მიზნიდან, წყაროდან, მოცულობიდან ან რაოდენობიდან ან მისი აღკვეთისათვის საჭირო რესურსების ოდენობიდან გამომდინარე, კრიტიკული ინფორმაციული სისტემის ნორმალური ფუნქციონირებისათვის საკმარისი საფრთხის შემცველია.

ოპერატიულ-ტექნიკური სააგენტოს, ციფრული მმართველობის სააგენტოსა და კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფების ძირითადი მოვალეობებია: კომპიუტერული ინციდენტების დროული გამოვლენა და მათზე რეაგირება, კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა ან/და ამ კანონით გათვალისწინებულ შემთხვევებში სახელმძღვანე-

[2] <https://mod.gov.ge/ge/page/59/cyber-security-bureau> [05/12/2022].

[3] ინფორმაციული უსაფრთხოების შესახებ კანონის მე-8 მუხლის პირველი პუნქტი.

ლო მითითებების გაცემა, კომპიუტერული ინციდენტების ანალიზი და მათი შედეგების გამოსწორებისა და ზიანის მინიმუმამდე შემცირების პროცესში დახმარება და ის სხვა ვალდებულებები, რომლებიც დაკავშირებულია ინფორმაციული უსაფრთხოების მიზნებთან.

დახმარების ჯგუფების მეშვეობით ზემოაღნიშნულ უწყებებს შესაძლებლობა აქვთ შეისწავლონ კომპიუტერული ინციდენტები და განახორციელონ რეაგირება. შესწავლის შედეგად დახმარების ჯგუფი სუბიექტს წარუდგენს შესასრულებლად სავალდებულო მითითებებს, რომელიც არ შეიძლება ითვალისწინებდეს მეორე ან მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელურ სენსორზე, ან მეორე ან მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე წვდომის ვალდებულებას. კომპიუტერული ინციდენტების იდენტიფიცირების ან/და მათზე რეაგირების მიზნით ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი უფლებამოსილია ჰქონდეს წვდომა მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების ქსელურ სენსორებზე და ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე შესაბამისი სუბიექტის თანხმობით.

3.5. შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულთან ბრძოლის სამმართველო

საქართველოს შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტის დაქვემდებარებაში ფუნქციონირებს კიბერდანაშაულთან ბრძოლის სამმართველო, რომლის მთავარი ამოცანაა კიბერდანაშაულის წინააღმდეგ ბრძოლა, მისი პრევენცია, გამოვლენა და აღკვეთა. აქვე აღსანიშნავია, რომ საქართველოს სისხლის სამართლის კოდექსის XXXV თავი ითვალისწინებს მთელ რიგ კიბერდანაშაულებს (კომპიუტერულ სისტემაში უნებართვო შეღწევა[4], კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება[5] და ა.შ.) რომლის ჩადენის შემთხვევაშიც დადგენილია შესაბამისი სისხლისსამართლებრივი პასუხისმგებლობები, ხოლო აღნიშნული დანაშაულების გამოძიება სწორედ შინაგან საქმეთა სამინისტროს კომპეტენციას წარმოადგენს.

3.6. საქართველოს ეროვნული ბანკი

კიბერუსაფრთხოების მიმართულებით კომერციული ბანკების დარგობრივ მარეგულირებელს საქართველოს ეროვნული ბანკი წარმოადგენს. „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის თანახმად, კომერციული ბანკი, რომელიც არ არის კრიტიკული ინფორმაციული სისტემის სუბიექტი, ხელმძღვანელობს ეროვნული ბანკის მიერ დადგენილი წესებითა და მოთხოვნებით.

საგულისხმოა, რომ კომერციული ბანკების მიმართ ინფორმაციული უსაფრთხოების პოლიტიკისა და ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების დამატებით სტანდარტებსა და მოთხოვნებს ადგენს ეროვნული ბანკი[6], რომელიც ასევე უფლებამოსილია მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკებს მოსთხოვოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების განსახილველად წარდგენა და განახორციელოს კანონის შესაბამისად დადგენილი დამატებითი სტანდარტებისა და მოთხოვნების მიმართ შესასრულებლად სავალდებულო მითითებების ან/და რეკომენდაციების გაცემა.[7]

---

4 საქართველოს სისხლის სამართლის კოდექსის 284-ე მუხლი.

5 ამავე კოდექსის 285-ე მუხლი.

6 „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის მე-4 მუხლის მე-6 პუნქტი

7 ამავე მუხლის მე-5 პუნქტი.

ამასთან, ეროვნული ბანკის პრეზიდენტის ბრძანების შესაბამისად დამტკიცებულია კიბერუსაფრთხოების ჩარჩო[8], რომლის შესაბამისად, ეროვნული ბანკი კომერციულ ბანკებს უწევს ზედამხედველობას, რათა დააკმაყოფილონ ინფორმაციული უსაფრთხოების მათთვის განსაზღვრული მინიმალური სტანდარტი.

3.7. ეროვნული უსაფრთხოების საბჭო

ეროვნული უსაფრთხოების საბჭო ეროვნული უსაფრთხოების საკითხებზე უმაღლესი დონის გადაწყვეტილებების მისაღებად შექმნილი საქართველოს პრემიერ-მინისტრის უშუალო დაქვემდებარებაში არსებული სათათბირო ორგანოა. საბჭო ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვის სფეროში მთავარ მაკოორდინირებელ ერთეულს წარმოადგენს. მას საქართველოს პრემიერ-მინისტრი ხელმძღვანელობს.[9]

ეროვნული უსაფრთხოების საბჭო 2019 წელს შეიქმნა. მისი ფუნქციონირების სამართლებრივი საფუძველი განსაზღვრულია საქართველოს კანონით „ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ". აღნიშნული კანონის შესაბამისად, ეროვნული უსაფრთხოებისა და სახელმწიფო ინტერესებისთვის საფრთხის შემცველ საკითხებზე საქართველოს პრემიერ-მინისტრის ინფორმირებისა და მის მიერ მისაღები პოლიტიკური გადაწყვეტილებების მომზადების, სტრატეგიულ დონეზე ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის მიზნით იქმნება ეროვნული უსაფრთხოების საბჭო, რომელსაც ხელმძღვანელობს საქართველოს პრემიერ-მინისტრი.[10]

ამავე კანონის მე-3 მუხლის თანახმად, ინფორმაციული უსაფრთხოება წარმოადგენს ეროვნული უსაფრთხოების პოლიტიკის ერთ-ერთ უმნიშვნელოვანეს მიმართულებას. შესაბამისად, საბჭოს ფუნქციებში შედის ინფორმაციული უსაფრთხოების პოლიტიკის იმპლემენტაციის კოორდინაციაც.

ამასთან, აღსანიშნავია, რომ ეროვნული უსაფრთხოების საბჭოს აპარატის ერთ-ერთი სტრუქტურული ერთეულია ინფორმაციული და კიბერუსაფრთხოების საკითხთა დეპარტამენტი[11], რომლის ფუნქციას ინფორმაციული უსაფრთხოების/კიბერუსაფრთხოების სფეროში ერთიანი სახელმწიფო პოლიტიკის დაგეგმვის და კოორდინაციის განხორციელება და ამავე კომპეტენციის ფარგლებში, საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგიის სამოქმედო გეგმით გათვალისწინებული ღონისძიებების იმპლემენტაციის მონიტორინგი და შესრულების კოორდინაციის უზრუნველყოფა წარმოადგენს. აგრეთვე, დეპარტამენტი, შესაბამის სექტორულ უწყებასთან შეთანხმებით, შესაძლოა ჩაერთოს კონკრეტული კომპიუტერული ინციდენტის მართვის პროცესში იმ შემთხვევაში, თუ შესაძლებელია მოცემული მოვლენის მავნე შედეგების სამომავლო ესკალაცია.

4. თავდაცვის სფეროში არსებული პოლიტიკის დოკუმენტები

4.1. საქართველოს ეროვნული უსაფრთხოების კონცეფცია

საქართველოს ეროვნული უსაფრთხოების კონცეფცია[12] თავდაცვის სფეროში ერთ-ერთი მნიშვნელოვანი დოკუმენტია, რომელიც საქართველოს ეროვნულ ინტერესად კიბერუსაფრთხოებას განამტკიცებს. კონცეფციის მიხედვით, „საქართველოსთვის მეტად მნიშვნელოვანია ინფორმაციული სივრცის უსაფრთხოება და ელექტრონული ინფორმაციის დაცულობა. ინფორ-

[8] „კომერციული ბანკების კიბერუსაფრთხოების მართვის ჩარჩოს დამტკიცების შესახებ" საქართველოს ეროვნული ბანკის პრეზიდენტის 2019 წლის 22 მარტის №56/04 ბრძანება. <https://matsne.gov.ge/ka/document/view/4515476?publication=1> [05/12/2022].

[9] <https://nsc.gov.ge/ka/საბჭო/საბჭოს-შესახებ> [05/12/2022].

[10] „ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ". საქართველოს კანონის მე-19[1] მუხლი.

[11] <https://nsc.gov.ge/ka/საბჭოს-აპარატი/დეპარტამენტები> [05/12/2022].

[12] <https://mod.gov.ge/uploads/2018/pdf/NSC-GEO.pdf> [05/12/2022].

მაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად იზრდება მათზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულება. ამის გათვალისწინებით, დიდი მნიშვნელობა ენიჭება კიბერდანაშაულთან ბრძოლას და კიბერსივრცეში დივერსიული აქტებისგან თავდაცვას."

ამასთან, კონცეფციის თანახმად, საქართველოს უსაფრთხოების პოლიტიკის ერთ-ერთი ძირითადი მიმართულება სათანადო კიბერუსაფრთხოების პოლიტიკის არსებობაა. ამავე დოკუმენტის მიხედვით: „საქართველოს მიზანია, შექმნას ინფორმაციული უსაფრთხოების ისეთი სისტემა, რომლის დროსაც ნებისმიერი კიბერთავდასხმის საზიანო შედეგები მინიმუმამდე იქნება შემცირებული და ასეთი თავდასხმის შემდეგ უმოკლეს დროში გახდება შესაძლებელი ინფორმაციული ინფრასტრუქტურის ფუნქციონირების სრული აღდგენა. საქართველო დიდ მნიშვნელობას ანიჭებს საიდუმლო ინფორმაციის უსაფრთხოების უზრუნველყოფას და სახელმწიფოს საინფორმაციო სისტემების დაცვას. იგი ქმნის შესაბამის საკანონმდებლო ბაზას და ინფრასტრუქტურას, რომელიც აუცილებელია ინფორმაციული ტექნოლოგიების გასაუმჯობესებლად და ინფორმაციის დაცულობის უზრუნველსაყოფად."

4.2. საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგია და სამოქმედო გეგმა

კიბერუსაფრთხოების უზრუნველყოფის მიზნით, მნიშვნელოვანია, ქვეყანაში უზრუნველყოფილ იქნას სათანადო კოორდინაცია და თანამშრომლობა ჩართულ და დაინტერესებულ უწყებებს/მხარეებს შორის, შემუშავებულ იქნას შესაბამისი სტრატეგია და კონკრეტული სამოქმედო გეგმა სტრატეგიით განსაზღვრული მიზნების განსახორციელებლად.[13]

საქართველოს მთავრობის დადგენილებით 2021 წლის 30 სექტემბერს მიღებულ იქნა საქართველოს კიბერუსაფრთხოების 2021–2024 წლების ეროვნული სტრატეგია და დამტკიცდა სამოქმედო გეგმა. საგულისხმოა, რომ ის რიგით მესამე დოკუმენტია და მის მიღებამდე მოქმედებდა 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". კიბერუსაფრთხოების ეროვნული სტრატეგიის თანახმად, აღნიშნული დოკუმენტების არსებობა 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.[14]

სამოქმედო გეგმით განსაზღვრულ აქტივობებს შორის კვლევის მიზნებისთვის გამოსარჩევია კრიტიკული ინფრასტრუქტურების კიბერუსაფრთხოების სპეციალისტებისთვის ცოდნისა და კვალიფიკაციის ეროვნული ჩარჩოს მომზადება (skill pipeline), რაც გეგმის მიხედვით უნდა შესრულდეს 2023 წელს. ამასთან, 2024 წლის მე-4 კვარტალში უნდა დასრულდეს უფლებამოსილი სახელმწიფო უწყებებისთვის ტექნიკური შე-

[13] European Union Agency for Cybersecurity (ENISA), A Governance Framework for National Cybersecurity Strategies, 2023, 6 < https://www.enisa.europa.eu/publications/a-governance-framework-for-national-cybersecurity-strategies/@@download/fullReport> [05/12/2022].

[14] „საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ" საქართველოს მთავრობის.
2021 წლის 30 სექტემბრის №482 დადგენილება <https://matsne.gov.ge/ka/document/view/5263611?publication=1> [05/12/2022].

საძლებლობების შექმნა/განვითარება კრიტიკული ინფორმაციული სისტემების სუბიექტების ინფრასტრუქტურებში კიბერინციდენტებისა და კიბერსაფრთხეების მართვის მიზნით.

5. ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები

კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია მიიღოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები, რომლებიც ემსახურება „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის დებულებათა აღსრულებას და განსაზღვრავს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკას.

ინფორმაციული უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს. ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები დგინდება სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO), აშშ-ის სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტის (NIST) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილი სტანდარტებისა და მოთხოვნების მხედველობაში მიღების გზით, პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის – ოპერატიულ-ტექნიკური სააგენტოს უფროსის ბრძანებით, ხოლო მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის – ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით.[15]

საკითხის მნიშვნელობიდან გამომდინარე, მოქმედი კანონმდებლობა კრიტიკული ინფორმაციული უსაფრთხოების სისტემის სუბიექტებს ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დანერგვისთვის უწესებს შესაბამის ვადებს და ეტაპებს. ორგანიზაციებს აღნიშნული ვალდებულება აკისრიათ საქართველოს მთავრობის 2021 წლის 31 დეკემბრის №646 დადგენილებით განსაზღვრული წესით შესაბამისი კატეგორიის სუბიექტად განსაზღვრისთანავე და მათ კანონმდებლობის მოთხოვნათა გათვალისწინებით უნდა დანერგონ მინიმალური მოთხოვნები, ეტაპობრივად შეზღუდული დროის განმავლობაში.

კერძოდ, პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებისთვის, ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვა ხორციელდება ორ ეტაპად:

ა) პირველი ეტაპი - მოიცავს თვრამეტ თვეს საქართველოს კანონმდებლით დადგენილი წესით ორგანიზაციის პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტად განსაზღვრიდან;

ბ) მორე ეტაპი - მოიცავს ექვს თვეს პირველი ეტაპის დასრულებიდან.[16]

ოპერატიულ-ტექნიკური სააგენტოს უფროსის 2021 წლის 21 დეკემბრის №35 ბრძანებით დამტკიცებული „პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების" მე-4 და მე-5 მუხლების თანახმად, ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვის პირველ ეტაპზე ორგანიზაციამ უნდა უზრუნველყოს:

- ორგანიზაციის კონტექსტის განსაზღვრა, რაც მოიცავს ორგანიზაციის და მისი საქმიანობის კონტექსტის განსაზღვრას, დაინტერესებული მხარეების საჭიროებების და მოლოდინების განსაზღვრას, ინფორმაციული უსაფრთხოების მართვის სისტემის ფარგლების განსაზღვრას, ინფორმაციული უსაფრთხოების მართვის სისტემის დაფუძნებას, შენარჩუნებას და განგრძობად გაუმჯობესებას;
- ორგანიზაციის მენეჯმენტის მიერ განსახორციელებელი ქმედებების აღსრულებას, რაც მოიცავს მენეჯმენტის მხრიდან ინფორმაციული უსაფრთხოების მართვის სისტემის მხარდაჭერის დემონსტრირებას, ინფორმაციული უსაფრთხოების პოლიტიკების დამტკიცებას, ორგანიზაციული როლების, პასუხისმგებლობების და უფლებამოსილებების განსაზღვრას;

[15] „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის მე-4 მუხლის მე-2 პუნქტი.

[16] ოპერატიულ-ტექნიკური სააგენტოს უფროსის 2021 წლის 21 დეკემბრის №35 ბრძანებით დამტკიცებული პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების მე-3 მუხლი.

- დაგეგმვა, რაც მოიცავს ინფორმაციული უსაფრთხოების რისკების შეფასებას, ინფორმაციული უსაფრთხოების რისკების მოპყრობას, ინფორმაციული უსაფრთხოების მიზნების და მათი მიღწევის დაგეგმვას;
- სათანადო მხარდაჭერა, რაც მოიცავს შესაბამისი რესურსების გამოყოფას, კომპეტენციის და ცნობიერების დონის ამაღლებას, კომუნიკაციას და დოკუმენტაციის მართვას;
- ოპერირება, რაც მოიცავს ოპერაციულ დაგეგმვას და კონტროლს, ინფორმაციული უსაფრთხოების რისკების შეფასებას დაგეგმილი ინტერვალებით და ინფორმაციული უსაფრთხოების რისკების მოპყრობის გეგმის აღსრულებას.

ხოლო, ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვის მეორე ეტაპზე ორგანიზაციამ უნდა უზრუნველყოს:

- ინფორმაციული უსაფრთხოების მართვის სისტემის შეფასება, რაც მოიცავს ინფორმაციული უსაფრთხოების მართვის სისტემის მონიტორინგს, გაზომვას, ანალიზს და შეფასებას, დაგეგმილი პერიოდულობით შიდა აუდიტის განხორციელებას, დაგეგმილი პერიოდულობით მენეჯმენტის მიერ ინფორმაციული უსაფრთხოების მართვის სისტემის გადახედვას მისი ეფექტიანობის, შესაბამისობის და ადეკვატურობის უზრუნველსაყოფად;
- ინფორმაციული უსაფრთხოების მართვის სისტემის გაუმჯობესება, რაც მოიცავს შეუსაბამობებზე რეაგირებას, შეუსაბამობის გამომწვევი მიზეზების აღმოფხვრას, საჭიროების შემთხვევაში ინფორმაციული უსაფრთხოების მართვის სისტემაში შესაბამისი ცვლილებების განხორციელებას და ინფორმაციული უსაფრთხოების მართვის სისტემის განგრძობად გაუმჯობესებას.

ხსენებული მოქმედებების განსახორციელებლად ოპერატიულ-ტექნიკური სააგენტოს უფროსის 2021 წლის 21 დეკემბრის №35 ბრძანების შესაბამისი დანართებით კი, დადგენილია დეტალური რეგულაციები.

რაც შეეხება მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მხრიდან მსგავს ვალდებულებებს, აღნიშნული დადგენილია ციფრული მმართველობის სააგენტოს თავმჯდომარის 2021 წლის 14 დეკემბრის №1 ბრძანებით და მოიცავს პირველ, მეორე და მესამე წელს შესასრულებელ მთელ რიგ მოქმედებებს.

აღსანიშნავია, რომ კრიტიკული ინფორმაციული სუბიექტებისთვის ზემოაღნიშნული ვალდებულებების განსაზღვრას არ ექნებოდა ქმედითი ეფექტი, თუ მათი შეუსრულებლობისთვის კანონმდებლობით არ დაწესდებოდა შესაბამისი პასუხისმგებლობის ზომები. სწორედ აღნიშნულიდან გამომდინარე, ადმინისტრაციული პასუხისმგებლობა კანონის მოთხოვნათა დარღვევისთვის დარეგულირებულია „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის ცალკე - III[2] თავით. განხილულ საკითხებთან მიმართებით პასუხისმგებლობებს შორის გამოსარჩევია ხსენებული კანონის 10[4] მუხლი, რომლის თანახმად:

„1. პირველი/მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-4 მუხლის მე-2 პუნქტით გათვალისწინებული ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დასანერგად ოპერატიულ-ტექნიკური სააგენტოს უფროსის/ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით განსაზღვრული ვადის დარღვევა – გამოიწვევს გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

2. იგივე ქმედება, ჩადენილი იმ პირველი/მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ, რომელსაც ამ მუხლის პირველი პუნქტით გათვალისწინებული დარღვევისთვის 1 წლის განმავლობაში შეეფარდა ადმინისტრაციული სახდელი, –

გამოიწვევს დაჯარიმებას 10 000 ლარის ოდენობით".

6. ფიზიკური და გარემო უსაფრთხოებასთან დაკავშირებული ვალდებულებები

„პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ" ოპერატიულ-ტექნიკური სააგენტოს უფროსის 2021 წლის 21 დეკემბრის №35 ბრძანებით დანართით დამტკიცებულია ინფორმაციული უსაფრთხოე-

ბის კონტროლები, რომელიც წარმოადგენს სახელმძღვანელო მითითებას ორგანიზაციებისთვის და საშუალებას აძლევს მათ, შეარჩიონ მათთვის საჭირო, საყოველთაოდ მიღებული, ინფორმაციული უსაფრთხოების კონტროლები ან ამ კონტროლების გათვალისწინებით, შექმნან ახალი კონტროლები და სახელმძღვანელო მითითებები ინფორმაციული უსაფრთხოების კონტროლების შერჩევის, დანერგვის და მართვის პროცესში.

აღნიშნული დოკუმენტით ორგანიზაციებს ევალებათ სხვადასხვა მიმართულებით პოლიტიკის შემუშავებისას და ბიზნეს პროცესის მიმდინარეობისას დაიცვან ფიზიკური და გარემო უსაფრთხოება. ამასთან, ორგანიზაციის ინფორმაციაზე და ინფორმაციის დამუშავების საშუალებებზე არაავტორიზებული ფიზიკური წვდომის, დაზიანების და ჩარევის შეზღუდვის მიზნით ხსენებული დოკუმენტით განსაზღვრულია უსაფრთხო ზონების (ფიზიკური უსაფრთხოების პერიმეტრები; ფიზიკური შესვლის კონტროლები; ოფისების, ოთახების და ობიექტების დაცვა; გარე და გარემო საფრთხეებისგან დაცვა და სხვა) და აღჭურვილობის (აღჭურვილობის განლაგება და დაცვა; კაბელების უსაფრთხოება; „სუფთა მაგიდის" და „სუფთა ეკრანის" პოლიტიკა და ა.შ.) დაცვასთან დაკავშირებით სახელმძღვანელო მითითებები.

რაც შეეხება მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მხრიდან ფიზიკური და გარემოს უსაფრთხოების დაცვასთან დაკავშირებულ ვალდებულებებს, ზემოაღნიშნული პრინციპის დაცვით ხსენებული საკითხები რეგულირდება ციფრული მმართველობის სააგენტოს თავმჯდომარის 2021 წლის 14 დეკემბრის №1 ბრძანების დანართით - „კონტროლის მიზნები და მექანიზმები".

7. რისკების მართვა

აღსანიშნავია, რომ 2011 წლიდან მოქმედებს სახელმწიფო სექტორში რისკის მართვის სახელმძღვანელო, რომელიც წარმოადგენს სახელმწიფო სექტორში რისკის მართვის მეთოდოლოგიურ სახელმძღვანელოს და შექმნილია „სახელმწიფო შიდა ფინანსური კონტროლის და ინსპექტირების შესახებ" საქართველოს კანონის მოთხოვნათა შესაბამისად.

სახელმძღვანელო მოიცავს რისკის მართვის არსს და მასში შემავალ კომპონენტებს, რომელთა გათვალისწინებით ცალკეული დაწესებულება შეიმუშავებს საკუთარი რისკის მართვის სისტემას, რომელიც შესაბამისობაში მოვა კონკრეტული დაწესებულების მიზნებთან და საქმიანობის სპეციფიკასთან. რისკის მართვა ხორციელდება არა შერჩევის პრინციპით, არამედ მთელი დაწესებულების მასშტაბით, მის ყველა სტრუქტურულ, თუ ორგანიზაციულ დონეზე. ამასთან, საუკეთესო შედეგის მისაღებად რისკის მართვის პროცესის ამოქმედება სასურველია საქმიანობის განხორციელებისა, თუ დასახული ამოცანის შესრულების დაწყებისთანავე.[17]

რისკის მართვა წარმოადგენს რისკის განსაზღვრის, შეფასების, მონიტორინგის და რისკის მისაღებ დონეზე შენარჩუნების მიზნით საჭირო კონტროლის ღონისძიებების გატარების პროცესს, რომელიც გავლენას ახდენს დაწესებულების მიზნებისა და ამოცანების მიღწევაზე და გულისხმობს საჭირო ღონისძიებების განხორციელებას რისკის შემცირების მიზნით. რისკის მართვა წარმოადგენს ერთიან, უწყვეტ და განვითარებად პროცესს, რომელშიც თავისი უფლებამოსილების ფარგლებში მონაწილეობას იღებს დაწესებულების თითოეული თანამშრომელი. რისკის მართვა წარმოადგენს დაწესებულების სტრატეგიული მართვის ერთ-ერთ მნიშვნელოვან კომპონენტს.[18]

რისკის მართვის მთავარი ამოცანაა მოახდინოს რისკების იდენტიფიკაცია და საპასუხო ღონისძიებების გატარება. რისკის მართვის საშუალებით შესაძლებელია გამოვლენილ იქნეს პოტენციური დადებითი თუ უარყოფითი ფაქტორები, რაც გავლენას ახდენს დაწესებულების საქმიანობაზე.

---

[17] საქართველოს ფინანსთა მინისტრის 2011 წლის 30 დეკემბრის №644 ბრძანებით დამტკიცებული „რისკების მართვის სახელმძღვანელოს" შესავალი. <https://matsne.gov.ge/ka/document/view/1546971?publication=0> [05/12/2022].

[18] ამავე სახელმძღვანელოს მეორე თავი.

საგულისხმოა, რომ ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებთან ერთად კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის მოქმედი კანონმდებლობით[19] დადგენილია ინფორმაციული რისკების მართვის მთელი რიგი წესები და პირობები, რომლებიც მოიცავენ ინფორმაციული უსაფრთხოების მართვის პროცესის ზოგადი მიმოხილვას, კონტექსტის განსაზღვრას, ინფორმაციული უსაფრთხოების რისკების შეფასებას (მათ შორის, რისკის იდენტიფიცირება, ანალიზი, ევალუაცია) რისკების მოპყრობას, მიღებას, ინფორმაციული უსაფრთხოების რისკების მონიტორინგს, გადახედვას და ა.შ.

8. ინფორმაციული უსაფრთხოების მენეჯერი და კომპიუტერული უსაფრთხოების სპეციალისტი

მოქმედი კანონმდებლობის თანახმად[20], კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი (თანამშრომლები), რომელიც (რომლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) კრიტიკული ინფორმაციის სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მოთხოვნების შესრულებისათვის (ინფორმაციული უსაფრთხოების მენეჯერი), რომელიც აღჭურვილია მთელი რიგი ვალდებულებებით (მათ შორის ინფორმაციული უსაფრთხოების სამოქმედო გეგმის შედგენის) და ანგარიშვალდებულია კრიტიკული ინფორმაციული სისტემის სუბიექტის ხელმძღვანელის ან მის მიერ შესაბამისად უფლებამოსილი თანამშრომლის წინაშე.

პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ინფორმაციული უსაფრთხოების მენეჯერებად შესაძლებელია განისაზღვრონ პირები, რომლებსაც აქვთ სახელმწიფო საიდუმლოებასთან დაშვება. ინფორმაციული უსაფრთხოების მენეჯერისთვის მინიმალური სტანდარტები პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების მიმართ დგინდება ოპერატიულ-ტექნიკური სააგენტოს უფროსის ბრძანებით, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიმართ – ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტის მიმართ – საქართველოს თავდაცვის მინისტრის ბრძანებით.

ინფორმაციული უსაფრთხოების მენეჯერთან ერთად, კრიტიკული ინფორმაციული სისტემის სუბიექტი ასევე ვალდებულია განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი (თანამშრომლები), რომელიც (რომლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული სისტემების უსაფრთხოების პრაქტიკული უზრუნველყოფისათვის (კომპიუტერული უსაფრთხოების სპეციალისტი).[21]

9. კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტი და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტი

მთავრობის დადგენილებით განსაზღვრული პირველი, მეორე და მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებს მოქმედი კანონმდებლობით აქვთ ვალდებულება ჩაატარონ ინფორმაციული უსაფრთხოების აუდიტი და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტი. პირველი კატეგორიის სუბიექტის ინფორმაციული უსაფრთხოების პირველად აუდიტს უსასყიდლოდ ატარებს ოპერატიულ-ტექნიკური სააგენტო, ხოლო პერიოდულ აუდიტს, ამ სუბიექტის შერჩევით, ატარებს ოპერატიულ-ტექნიკური სააგენტო ან

[19] ციფრული მმართველობის სააგენტოს თავმჯდომარის 2021 წლის 14 დეკემბრის №1 ბრძანება; ოპერატიულ-ტექნიკური სააგენტოს უფროსის 2021 წლის 21 დეკემბრის №35 ბრძანება; საქართველოს თავდაცვის მინისტრის 2022 წლის 8 ივლისის №46 ბრძანება.

[20] „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-7 მუხლი.

[21] „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-9 მუხლი.

ციფრული მმართველობის სააგენტოს მიერ ავტორიზებული ორგანიზაცია.

9.1. ინფორმაციული უსაფრთხოების აუდიტი

კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია ჩაატაროს ინფორმაციული უსაფრთხოების პირველადი აუდიტი და პერიოდული აუდიტი – ინფორმაციული უსაფრთხოების მართვის სისტემის ინფორმაციული უსაფრთხოების მინიმალურ სტანდარტებთან შესაბამისობის შეფასება. ინფორმაციული უსაფრთხოების აუდიტის ჩატარების შემდეგ დგება აუდიტის დასკვნა, რომლის მოთხოვნების შესრულება სავალდებულოა. ინფორმაციული უსაფრთხოების აუდიტი სრულდება ინფორმაციული უსაფრთხოების აუდიტის დასკვნის შედგენით.[22]

– **პირველი კატეგორიის** კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების პირველად აუდიტს უსასყიდლოდ ატარებს ოპერატიულ-ტექნიკური სააგენტო. შემდგომ ინფორმაციული უსაფრთხოების პერიოდულ აუდიტს ამ სუბიექტის შერჩევით ატარებს ოპერატიულ-ტექნიკური სააგენტო ან ციფრული მმართველობის სააგენტოს მიერ ავტორიზებული ორგანიზაცია;

– **მეორე კატეგორიის** კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების პირველად აუდიტსა და პერიოდულ აუდიტს ამ სუბიექტის შერჩევით ატარებს ოპერატიულ-ტექნიკური სააგენტო ან ციფრული მმართველობის სააგენტოს მიერ ავტორიზებული ორგანიზაცია;

– **მესამე კატეგორიის** კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების პირველად აუდიტსა და პერიოდულ აუდიტს ამ სუბიექტის შერჩევით ატარებს ციფრული მმართველობის სააგენტო ან ამ სააგენტოს მიერ ავტორიზებული ორგანიზაცია;

– **თავდაცვის სფეროში** შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების პირველად აუდიტსა და პერიოდულ აუდიტს ატარებს კიბერუსაფრთხოების ბიურო. საჭიროების შემთხვევაში ინფორმაციული უსაფრთხოების აუდიტი ტარდება საქართველოს თავდაცვის სამინისტროს სხვა შესაბამის სტრუქტურულ ქვედანაყოფებთან ერთად.

ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესი და პერიოდულობა პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების მიმართ დგინდება ოპერატიულ-ტექნიკური სააგენტოს უფროსის ბრძანებით, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიმართ – ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტების მიმართ – საქართველოს თავდაცვის მინისტრის ბრძანებით.[23]

9.2. ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტი

ინფორმაციული უსაფრთხოების აუდიტთან ერთად, „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის მე-6 მუხლი განსაზღვრავს ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების ვალდებულებას და წესს. კერძოდ, კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია უზრუნველყოს პენეტრაციის ტესტის ჩატარება წინასწარ დაგეგმილი და დოკუმენტირებული ამოცანის მიხედვით. პენეტრაციის ტესტის ჩატარების შემდეგ დგება პენეტრაციის ტესტის დასკვნა, რომლის მოთხოვნების შესრულება სავალდებულოა. პენეტრაციის ტესტი სრულდება პენეტრაციის ტესტის დასკვნის შედგენით.

პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის (გარდა საგადახდო, ფასიანი ქაღალდების ანგარიშსწორებისა და რეზერვების მართვის სისტემებისა, აგრეთვე მონეტარული და სავალუტო ოპერაციებისთვის გამოყენებული კრიტიკული სისტემებისა) სუბიექტის პენეტრაციის ტესტს ატარებს ოპერატიულ-ტექნიკური სააგენტო, მეორე კატეგორიის კრიტი-

[22] „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის მე-6 მუხლის პირველი პუნქტი.

[23] „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის მე-6 მუხლის მე-7 პუნქტი.

კული ინფორმაციული სისტემის სუბიექტის პენეტრაციის ტესტს – კრიტიკული ინფორმაციული სისტემის სუბიექტის შერჩევით – ოპერატიულ-ტექნიკური სააგენტო ან ციფრული მმართველობის სააგენტოს მიერ ავტორიზებული ორგანიზაცია, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის პენეტრაციის ტესტს – კრიტიკული ინფორმაციული სისტემის სუბიექტის შერჩევით – ციფრული მმართველობის სააგენტო ან ამ სააგენტოს მიერ ავტორიზებული ორგანიზაცია, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტის პენეტრაციის ტესტს – კიბერუსაფრთხოების ბიურო.[24]

პენეტრაციის ტესტის ჩატარების წესი და პერიოდულობა პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების მიმართ დგინდება ოპერატიულ-ტექნიკური სააგენტოს უფროსის ბრძანებით, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიმართ – ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტის მიმართ – საქართველოს თავდაცვის მინისტრის ბრძანებით.[25]

აღსანიშნავია, რომ თუ ინფორმაციული უსაფრთხოების აუდიტის ჩატარების შედეგად გამოვლინდა ინფორმაციული უსაფრთხოების მართვის სისტემის ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებთან შეუსაბამობა ან პენეტრაციის ტესტის ჩატარების შედეგად აღმოჩენილ იქნა ინფორმაციული სისტემის სისუსტეები, კრიტიკული ინფორმაციული სისტემის სუბიექტი ატარებს ამ შეუსაბამობის/სისუსტეების ანალიზს და აღნიშნული შეუსაბამობის/სისუსტეების აღმოსაფხვრელად განსაზღვრავს სამოქმედო გეგმას. ეს სამოქმედო გეგმა უნდა შეიცავდეს მისი შესრულების გრაფიკს. აღნიშნულ სამოქმედო გეგმას ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის დასრულებიდან 1 თვის ვადაში პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტები შესათანხმებლად წარუდგენენ ოპერატიულ-ტექნიკურ სააგენტოს, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტები, გარდა ამ მუხლის მე-17 პუნქტით გათვალისწინებული შემთხვევისა, – ციფრული მმართველობის სააგენტოს, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტები – კიბერუსაფრთხოების ბიუროს. ოპერატიულ-ტექნიკური სააგენტო, ციფრული მმართველობის სააგენტო და კიბერუსაფრთხოების ბიურო საკუთარი კომპეტენციის ფარგლებში უზრუნველყოფენ წარდგენილი სამოქმედო გეგმის შეფასებას, შესაბამისი რეკომენდაციების ან/და შესასრულებლად სავალდებულო მითითებების შემუშავებას და შეთანხმებული სამოქმედო გეგმის შესრულების მონიტორინგს.[26]

10. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმება

პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის უსაფრთხოების შემოწმების მიზნით, ოპერატიულ-ტექნიკური სააგენტო უფლებამოსილია მიიღოს გადაწყვეტილება ამ სუბიექტის საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების ჩატარების შესახებ, ხოლო საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების ჩატარების წესი და პროცედურები დგინდება ოპერატიულ-ტექნიკური სააგენტოს უფროსის ბრძანებით.[27]

საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების ჩატარების უფლებამოსილების მქონე პირს უფლება აქვს, სპეციალური ტექნიკური და პროგრამული უზრუნველყოფის საშუალებების გამოყენებით შეამოწმოს პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის აპარატული ან/და

[24] „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-10 პუნქტი.
[25] ამავე მუხლის მე-12 პუნქტი.
[26] „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-14 პუნქტი.
[27] ამავე კანონის 9^1 მუხლი.

პროგრამული უზრუნველყოფის საშუალებები ან/და ქსელური ინფრასტრუქტურა, ასევე შეამოწმოს შესამოწმებელ საკითხთან დაკავშირებული დოკუმენტები მათი განთავსების ადგილზე და გადაიღოს ამ დოკუმენტების ასლები, მოსთხოვოს პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის წარმომადგენელს/წარმომადგენლებს წერილობითი ან/და ზეპირი ახსნა-განმარტებები. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების დროს ოპერატიულ-ტექნიკურ სააგენტოს ხელი არ მიუწვდება ისეთ ინფორმაციაზე, რომელიც საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის ფუნქციონირებასთან დაკავშირებული არ არის.[28]

შემოწმების ჩატარების უფლებამოსილების მქონე პირი დამტკიცებული ფორმის მიხედვით ადგენს საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების შესახებ დასკვნას[29], რომელში ასახული მითითებული შესასრულებლად სავალდებულო ხასიათისაა. ამასთან, გასათვალისწინებელია, რომ „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონით ადმინისტრაციული პასუხისმგებლობის სახით დადგენილია ფულადი ჯარიმები შემდეგი სამართალდარღვევებისთვის:

- ტექნოლოგიური ინფრასტრუქტურის შემოწმებისთვის ხელის შეშლისთვის;
- საინფორმაციო ტექნოლოგიური ინფრასტრუქტურის შემოწმების დასკვნით გათვალისწინებული შესასრულებლად სავალდებულო მითითების შეუსრულებლობისთვის;
- საინფორმაციო-ტექნოლოგიურ ინფრასტრუქტურაში დაგეგმილი ცვლილებების შეუთანხმებლობისთვის.

11. მონაცემთა უსაფრთხოების დაცვა

მონაცემთა უსაფრთხოების დაცვასთან დაკავშირებულ სამართლებრივ აქტებს შორის გამოსარჩევია „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი[30], რომლის მე-17 მუხლით დადგენილია მონაცემთა უსაფრთხოების დაცვის წესები, რაც სავალდებულოდ შესასრულებელია როგორც საჯარო, ასევე კერძო სექტორისთვის. აღნიშნული მუხლის პირველი პუნქტის თანახმად, მონაცემთა დამმუშავებელი ვალდებულია მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო განადგურებისაგან, შეცვლისაგან, გამჟღავნებისაგან, მოპოვებისაგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან. ამავე მუხლის თანახმად, მონაცემთა დამმუშავებელი ვალდებულია უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა, ხოლო მონაცემთა უსაფრთხოებისათვის მიღებული ზომები მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური უნდა იყოს.

ელექტრონული ფორმით არსებული მონაცემების მიმართ განხორციელებულ ქმედებებს (მაგალითად, მონაცემების დათვალიერების, გადმოწერის, წაშლისა და რედაქტირების ფაქტებს) მონაცემთა დამმუშავებლები რიგ შემთხვევებში არ აღრიცხავენ, ზოგჯერ კი - არასრულად. ხშირ შემთხვევაში დაწესებულების მიერ არ აღირიცხება მონაცემთა ბაზაზე პირდაპირი წვდომის გზით მონაცემთა მიმართ შესრულებული მოქმედებები. აღსანიშნავია, რომ მათი სრულყოფილად აღრიცხვის გარეშე, მონაცემებზე წვდომის უფლებამოსილების მქონე პირის მიერ მონაცემთა უკანონო დამუშავების, მათ შორის, გამჟღავნების შემთხვევაში, შესაძლოა, ვერ მოხდეს შესაბამისი ფაქტის დაფიქსირება და პასუხისმგებელი პირის იდენტიფიცირება. ამდენად, აღრიცხვა და პერიოდული მონიტორინგი წარმოადგენს მონაცემთა უკანონო დამუშავების პრევენციის ეფექტიან საშუალებას. აქვე, აღსანიშნავია, რომ მნიშვნელოვანია ელექტრონულ მონაცემთა მიმართ განხორციელებული ქმედებები აღირიცხოს ავტომატურად, რადგან

[28] ამავე მუხლის მე-3 პუნქტი.
[29] ამავე მუხლის მე-4 პუნქტი.
[30] „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი <https://matsne.gov.ge/ka/document/view/1561437?publication=23> [05/12/2022].

ადამიანური რესურსის გამოყენებით, მექანიკურად (მაგალითად, "MS Excel"-ის ფორმატის დოკუმენტში შეყვანის გზით) მოქმედებების აღრიცხვის შემთხვევაში, მაღალია ინფორმაციის არასრულად/არასწორად მითითების ალბათობა.[31]

„პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-17 მუხლით, მონაცემთა უსაფრთხოების დაცვის მოთხოვნის შეუსრულებლობისთვის დადგენილია ადმინისტრაციული პასუხისმგებლობა, კერძოდ, გაფრთხილება ან დაჯარიმება 500 ლარის ოდენობით, ხოლო იგივე ქმედება, ჩადენილი იმ პირის მიერ, რომელსაც ერთი წლის განმავლობაში შეეფარდა ადმინისტრაციული სახდელი ამ მუხლის პირველი პუნქტით გათვალისწინებული დარღვევისათვის, გამოიწვევს დაჯარიმებას 2000 ლარის ოდენობით.

გასათვალისწინებელია, რომ კანონის მე-17 და 46-ე მუხლების შესაბამისად, მონაცემთა უსაფრთხოების დაცვასთან დაკავშირებული მოთხოვნების შეუსრულებლობის დადგენისათვის აუცილებელი არ არის სამართლებრივი შედეგის (მონაცემთა უკანონო გამჟღავნება ან სხვა ფორმით დამუშავება) დადგომა, საკმარისია მონაცემთა დამმუშავებელმა არ გაითვალისწინოს მონაცემთა უსაფრთხოების დასაცავად მოქმედი კანონმდებლობით განსაზღვრული წესები, მონაცემთა დამუშავებასთან დაკავშირებული რისკები და თავისი ქმედებით ან უმოქმედობით შექმნას მონაცემთა უკანონო დამუშავების საფრთხე.[32]

11.1. მონაცემთა უსაფრთხოების დარღვევის შესახებ შეტყობინება

2018 წლის 25 მაისს ძალაში შევიდა ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია („General Data Protection Regulation") (შემდგომში - „GDPR"). რეგულაციას პერსონალურ მონაცემთა დაცვა სრულიად ახალ საფეხურზე გადაჰყავს და მიზნად ისახავს ტექნოლოგიური პროგრესისა და თანამედროვე გამოწვევების პირობებში ინდივიდების უფლებების სათანადო დაცვას.

„GDPR-ით" განისაზღვრა პერსონალურ მონაცემთა უსაფრთხოების დარღვევის ცნება, რომელიც გულისხმობს უსაფრთხოების დარღვევას, რომელიც იწვევს გადაცემული, შენახული ან სხვაგვარად დამუშავებული პერსონალური მონაცემების შემთხვევით ან უკანონო განადგურებას, დაკარგვას, შეცვლას, მათ უკანონო გამჟღავნებას ან მათზე არასანქცირებულ წვდომას.

თუ დაირღვა მონაცემთა უსაფრთხოება, ორგანიზაციამ დარღვევის აღმოჩენიდან არაუგვიანეს 72 საათისა უნდა შეატყობინოს პერსონალურ მონაცემთა საზედამხედველო ორგანოს და დარღვევის შესახებ უნდა აცნობოს იმ პირებს, რომელთა მონაცემებსაც შეეხო ინციდენტი, თუ ეს დიდი ალბათობით გამოიწვევს ამ პირთა უფლების შელახვას .

„GDPR-ის" 33-ე და 34-ე მუხლებით დადგენილია იმ ინფორმაციის ჩამონათვალი, რომლებიც ინციდენტის დადგომის შემთხვევაში უნდა მიეწოდოს მონაცემთა დაცვის საზედამხედველო ორგანოს და მონაცემთა სუბიექტს.

საზედამხედველო ორგანოსთვის განკუთვნილი შეტყობინება უნდა შეიცავდეს, სულ მცირე, შემდეგ ინფორმაციას:

ა) მონაცემთა უსაფრთხოების დარღვევის ხასიათის აღწერილობა, მათ შორის, თუ შესაძლებელია, მონაცემთა სუბიექტების კატეგორიები და რაოდენობა, ასევე მონაცემთა კატეგორიები და რაოდენობას, რომელსაც შეეხო უსაფრთხოების დარღვევა;

ბ) მონაცემთა დაცვის ოფიცრის ან სხვა საკონტაქტო პირის ვინაობა და საკონტაქტო მონაცემები, რომელთაგანაც უფრო მეტი ინფორმაციის მოპოვება იქნება შესაძლებელი;

გ) დარღვევის მოსალოდნელი შედეგების აღწერა;

[31] პერსონალურ მონაცემთა დაცვის სამსახურის 2022 წლის საქმიანობის ანგარიში, 108 <https://personaldata.ge/cdn/2023/04/პერსონალურ-მონაცემთა-დაცვის-სამსახურის-2022-წლის-საქმიანობის-ანგარიში.pdf> [28/07/2023].

[32] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის 2022 წლის 13 ივლისის №გ-1/061/2022 გადაწყვეტილება.

დ) დარღვევის აღმოსაფხვრელად დამმუშავებლის მიერ მიღებული ან შეთავაზებული ზომები, მათ შორის, შესაბამის შემთხვევებში, დარღვევის შესაძლო უარყოფითი შედეგის შემამსუბუქებელი ზომების აღწერა.

მონაცემთა სუბიექტთან მონაცემთა უსაფრთხოების დარღვევის შესახებ კომუნიკაცია უნდა განხორციელდეს გასაგები და მარტივი ენით, უნდა აღწერდეს დარღვევის ხასიათს და მინიმუმ უნდა შეიცავდეს ზემოაღნიშნული 33-ე მუხლის, მე-3 პუნქტის, „ბ“, „გ“ და „დ“ ქვეპუნქტებით დადგენილ ინფორმაციას და ზომებს.

შესაბამისად, აუცილებელია მონაცემთა დამმუშავებლების მიერ გატარდეს ყველა სათანადო ორგანიზაციული და ტექნიკური ზომა მონაცემების დასაცავად, ხოლო მათი უსაფრთხოების დარღვევის შემთხვევაში, აღნიშნულის დაუყოვნებლივ დასადგენად. ამასთან, მნიშვნელოვანია კანონმდებლობით დადგინდეს, ინციდენტის დადგომისას საზედამხედველო ორგანოსა და მონაცემთა სუბიექტისთვის დაუყოვნებლივ შეტყობინების ვალდებულება, ხოლო ორგანიზაციების მიერ შემუშავებულ იქნას მონაცემთა უსაფრთხოების დარღვევის შეტყობინების პოლიტიკა, ინციდენტების გამოვლენისა და მათზე რეაგირების პროცედურა.

12. დასკვნა

საერთაშორისო გამოცდილება ცხადყოფს, რომ კარგად ორგანიზებული კიბერ-სივრცის არქიტექტურა, სწორად გადანაწილებული უფლებამოსილებები და ანგარიშვალდებულებისა და კოორდინაციის დახვეწილი მექანიზმები წარმოადგენს კიბერ-სივრცის გამართული და უსაფრთხო ფუნქციონირების მთავარ წინაპირობას.[33]

ევროკავშირის ქსელური და საინფორმაციო უსაფრთხოების სააგენტოს (ENISA) მიერ მომზადებულ ანგარიშში, ჩატარებული კვლევის საფუძველზე, შემოთავაზებულია ძირითადი რეკომენდაციები კიბერუსაფრთხოებასთან დაკავშირებული საზოგადოებრივი ცნობიერების ეფექტიანობის გაზრდის მიზნით[34]. აღნიშნული ანგარიშის მიხედვით, აუცილებელია:

1. კიბერუსაფრთხოების შესახებ ცნობიერების ამაღლების შესაძლებლობების შექმნა;

2. კიბერუსაფრთხოების ტენდენციებისა და გამოწვევების რეგულარული შეფასება;

3. კიბერუსაფრთხოებასთან დაკავშირებული ქცევის გაზომვა;

4. კიბერუსაფრთხოების თაობაზე ცნობიერების ამაღლების კამპანიების დაგეგმვა.

მიუხედავად იმისა, რომ საქართველოში ინფორმაციული უსაფრთხოების საკითხების სათანადოდ ორგანიზების მიზნით არსებობს შესაბამისი საკანონმდებლო ბაზა და სამართლებრივი საფუძვლები - „ინფორმაციული უსაფრთხოების შესახებ” საქართველოს კანონი, პერსონალურ მონაცემთა უსაფრთხოების დაცვის ნაწილში „პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონი თუ სხვადასხვა კანონქვემდებარე აქტი -, აუცილებელია აღნიშნული დარგების მუდმივი განვითარება და მათი ევროპულ კანონმდებლობასთან ჰარმონიზაცია. ასევე, მნიშვნელოვანია დაწესებულებების მხრიდან მიღებულ იქნას სათანადო ზომები და სრულყოფილად შესრულდეს მათზე კანონმდებლობით დაკისრებული მოვალეობები.

ამასთან, როგორც ნაშრომის შესავალში აღინიშნა, ინფორმაციული ტექნოლოგიების მზარდ განვითარებასთან ერთად, იზრდება უსაფრთხოების დარღვევის რისკები და, შესაბამისად, აუცილებელია უსაფრთხოების დაცვის სტანდარტების ასამაღლებლად ნორმატიული აქტების მუდმივი განახლება. ასევე, მონაცემთა დაცვისათვის მიღებული ეფექტიანი ორგანიზაციულ-ტექნიკური ზომების პრაქტიკაში გატარება, რათა საჯარო და კერძო ორგანიზაციებმა სათანადოდ უპასუხონ თანამედროვე გამოწვევებს.

[33] „კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და გამოწვევები“. ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 2020, 7.

[34] Raising Awareness Of Cybersecurity, A Key Element of National Cybersecurity Strategies, 2021, 29. https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity [05/12/2022].