საქართველოს პარლამენტი

საქართველოს კანონის პროექტი

„ინფორმაციული უსაფრთხოების შესახებ“
საქართველოს კანონში ცვლილების შეტანის თაობაზე“

კანონპროექტის დასახელება

საქართველოს პარლამენტის წევრი ირაკლი სესიაშვილი

კანონპროექტის ინიციატორი

საქართველოს პარლამენტის წევრი ირაკლი სესიაშვილი

კანონპროექტის ავტორი

საქართველოს პარლამენტის წევრი

ირაკლი სესიაშვილი –

თანამომხსენებელი – საქართველოს პარლამენტის
იურიდიულ საკითხთა კომიტეტის თავმჯდომარე

ანრი ოხანაშვილი –

მომხსენებელი, წამყვანი კომიტეტი

საქართველოს პარლამენტის იურიდიულ საკითხთა
კომიტეტის აპარატის მთავარი სპეციალისტი

ბაჩანა სურმავა –

კანონპროექტზე კომიტეტის აპარატის პასუხისმგებელი პირი

საქართველოს პარლამენტის აპარატის იურიდიული
დეპარტამენტი

იურიდიული დეპარტამენტის უფროსი

ალექსანდრე ტაბატაძე –

პროექტი

საქართველოს კანონი

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე

მუხლი 1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში (საქართველოს საკანონმდებლო მაცნე (www.matsne.gov.ge), 19.06.2012, სარეგისტრაციო კოდი: 140000000.05.001.016807) შეტანილ იქნეს შემდეგი ცვლილება:

1. მე-2 მუხლის:

ა) „ე“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„ე) კომპიუტერული ინციდენტი – ქმედება, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით და იწვევს ან მიზნად ისახავს ინფორმაციის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის დარღვევას;“;

ბ) „ზ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„ზ) კრიტიკული ინფორმაციული სისტემის სუბიექტი – ამ მუხლის „ზ[1]“–„ზ[3]“ ქვეპუნქტებით გათვალისწინებული სახელმწიფო ან მუნიციპალიტეტის ორგანო ან დაწესებულება, თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტი, იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი

ცხოვრების შენარჩუნებისთვის;“;

გ) „ზ“ ქვეპუნქტის შემდეგ დაემატოს შემდეგი შინაარსის „ზ[1]“–„ზ[3]“ ქვეპუნქტები:

„ზ[1]) პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი – საქართველოს მთავრობის დადგენილებით განსაზღვრული სახელმწიფო ან მუნიციპალიტეტის ორგანო ან დაწესებულება, საჯარო სამართლის იურიდიული პირი (გარდა საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირისა – ციფრული მმართველობის სააგენტოსი, საქართველოს თავდაცვის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირისა – კიბერუსაფრთხოების ბიუროსი და ამ კანონის 10[1] მუხლის მე-4 პუნქტით გათვალისწინებული თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტისა), სახელმწიფო საწარმო, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის;

ზ[2]) მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი – საქართველოს მთავრობის დადგენილებით განსაზღვრული, „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის მე-2 მუხლის „ჰ[60]“ ქვეპუნქტით გათვალისწინებული ელექტრონული კომუნიკაციის კომპანია, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და

საზოგადოებრივი ცხოვრების შენარჩუნებისთვის;

ზ[3]) მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი – საქართველოს მთავრობის დადგენილებით განსაზღვრული კერძო სამართლის იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის;";

დ) „მ" ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„მ) ქსელური სენსორი – აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების ერთობლიობა, რომელიც გამიზნულია ქსელური ნაკადის მონიტორინგისთვის, ინფორმაციული სისტემის წინააღმდეგ მიმართული კომპიუტერული ინციდენტის გამოსავლენად;";

ე) „ო" ქვეპუნქტის შემდეგ დაემატოს შემდეგი შინაარსის „პ"–„ს" ქვეპუნქტები:

„პ) ოპერატიულ-ტექნიკური სააგენტო – საქართველოს სახელმწიფო უსაფრთხოების სამსახურის მმართველობის სფეროში შემავალი საჯარო სამართლის იურიდიული პირი – საქართველოს ოპერატიულ-ტექნიკური სააგენტო;

ჟ) ელექტრონული კომუნიკაციის კომპანია – „ელექტრონული კომუნიკაციების შესახებ" საქართველოს კანონის მე-2 მუხლის „ჰ[60]" ქვეპუნქტით გათვალისწინებული ელექტრონული კომუნიკაციის კომპანია;

რ) სახელმწიფო საწარმო – საწარმო, რომელიც შექმნილია სახელმწიფოს 50%-ზე მეტი წილობრივი მონაწილეობით;

ს) კომერციული ბანკი – საქართველოს ეროვნული ბანკის (შემდგომ –

ეროვნული ბანკი) მიერ ლიცენზირებული იურიდიული პირი, რომელიც იღებს დეპოზიტებს და მათი გამოყენებით თავისი სახელით ახორციელებს საქართველოს კანონმდებლობით განსაზღვრულ საბანკო საქმიანობას.“.

2. მე-3 მუხლის:

ა) პირველი და მე-2 პუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

„1. ამ კანონის მოქმედება ვრცელდება კრიტიკული ინფორმაციული სისტემის სუბიექტზე, აგრეთვე იმ ორგანიზაციაზე/უწყებაზე, რომელიც კრიტიკული ინფორმაციული სისტემის სუბიექტს ექვემდებარება ან ამ სუბიექტთანაა დაკავშირებული დასაქმების, სტაჟირების, სახელშეკრულებო ან სხვა ურთიერთობით და აღნიშნული ურთიერთობის ფარგლებში ინფორმაციული აქტივის ხელმისაწვდომობას უზრუნველყოფს.

2. კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხა მტკიცდება და შესაბამისი სუბიექტის კრიტიკულობის კლასიფიცირება დგინდება საქართველოს მთავრობის დადგენილებით, რომლის პროექტს საქართველოს მთავრობას დასამტკიცებლად წარუდგენს საქართველოს იუსტიციის სამინისტრო ეროვნული უსაფრთხოების საბჭოსთან, საქართველოს თავდაცვისა და შინაგან საქმეთა სამინისტროებთან და საქართველოს სახელმწიფო უსაფრთხოების სამსახურთან შეთანხმებით. ამ ნუსხის შედგენისას გაითვალისწინება შემდეგი კრიტერიუმები: ინფორმაციული სისტემის შეფერხების ან მწყობრიდან გამოსვლის სავარაუდო შედეგების სიმძიმე და მასშტაბი; სავარაუდო ეკონომიკური ზარალის სიმძიმე სუბიექტებისთვის ან/და სახელმწიფოსთვის; ინფორმაციული სისტემის მიერ გაწეული მომსახურების აუცილებლობა საზოგადოების ნორმალური ფუნქციონირებისთვის; ინფორმაციული

სისტემის მომხმარებელთა რაოდენობა; სუბიექტის მატერიალური მდგომარეობა და სავარაუდო ხარჯების ოდენობა, რომლებიც მისთვის ამ კანონით გათვალისწინებული ვალდებულებების დაკისრებას მოჰყვება.“;

ბ) მე-4 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„4. ნებისმიერ იურიდიულ პირს ან სახელმწიფო ხელისუფლების ორგანოს, რომელიც არ არის კრიტიკული ინფორმაციული სისტემის სუბიექტი, უფლება აქვს, ნებაყოფლობით აიღოს ამ კანონიდან გამომდინარე ვალდებულებები. კომერციული ბანკი, რომელიც არ არის კრიტიკული ინფორმაციული სისტემის სუბიექტი, ხელმძღვანელობს ეროვნული ბანკის მიერ დადგენილი წესებითა და მოთხოვნებით.“;

გ) მე-5 პუნქტი ამოღებულ იქნეს.

3. მე-4 მუხლის:

ა) მე-2–მე-4 პუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

„2. 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.

3. ამ მუხლის პირველი პუნქტის შესაბამისად მიღებულ ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებს პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტები განსახილველად წარუდგენენ ოპერატიულ-ტექნიკურ სააგენტოს, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტები – ციფრული მმართველობის სააგენტოს, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტები – კიბერუსაფრთხოების ბიუროს. ოპერატიულ-ტექნიკურ სააგენტოს, ციფრული მმართველობის სააგენტოს და კიბერუსაფრთხოების ბიუროს საკუთარი კომპეტენციის ფარგლებში ეცნობებათ აგრეთვე ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებში შეტანილი ნებისმიერი ცვლილება. ოპერატიულ-ტექნიკური სააგენტო, ციფრული მმართველობის სააგენტო და კიბერუსაფრთხოების ბიურო ახორციელებენ ამგვარად მიწოდებული დოკუმენტების ზოგად ანალიზს და მათში აღმოჩენილი ხარვეზების გამოსასწორებლად წარადგენენ შესასრულებლად სავალდებულო მითითებებს ან/და რეკომენდაციებს. ოპერატიულ-ტექნიკური სააგენტო, ციფრული მმართველობის სააგენტო და კიბერუსაფრთხოების ბიურო საკუთარი კომპეტენციის ფარგლებში უფლებამოსილი არიან კრიტიკული ინფორმაციული სისტემის სუბიექტისგან გამოითხოვონ ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავებასთან, დანერგვასთან, მონიტორინგსა და გაუმჯობესებასთან დაკავშირებული სხვა ინფორმაცია.

4. ამ მუხლის მე-3 პუნქტით გათვალისწინებული დოკუმენტების გარდა, ოპერატიულ-ტექნიკურ სააგენტოს, ციფრული მმართველობის სააგენტოს და

კიბერუსაფრთხოების ბიუროს ხელი არ მიუწვდებათ კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციასა და ინფორმაციულ აქტივზე, გარდა ამ კანონის მე-10 მუხლის მე-5 პუნქტის „გ“ ქვეპუნქტითა და 10^3 მუხლის მე-3 პუნქტის „ბ“ ქვეპუნქტით გათვალისწინებული შემთხვევებისა, აგრეთვე იმ შემთხვევისა, როდესაც კრიტიკული ინფორმაციული სისტემის სუბიექტი ნებაყოფლობით უზრუნველყოფს მათთვის ინფორმაციისა და ინფორმაციული აქტივის ხელმისაწვდომობას.“;

ბ) მე-4 პუნქტის შემდეგ დაემატოს შემდეგი შინაარსის მე-5 და მე-6 პუნქტები:

„5. ეროვნული ბანკი უფლებამოსილია მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკებს მოსთხოვოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების განსახილველად წარდგენა და განახორციელოს ამ მუხლის მე-6 პუნქტის შესაბამისად დადგენილი დამატებითი სტანდარტებისა და მოთხოვნების მიმართ შესასრულებლად სავალდებულო მითითებების ან/და რეკომენდაციების გაცემა.

6. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკების მიმართ ინფორმაციული უსაფრთხოების პოლიტიკისა და ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების დამატებით სტანდარტებსა და მოთხოვნებს ადგენს ეროვნული ბანკი.“.

4. მე-5 მუხლის:

ა) მე-4 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„4. კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული

აქტივების მართვის წესები, კერძოდ, მათი აღწერის, კლასიფიცირების, ხელმისაწვდომობის, გაცემის (გამოქვეყნების), შეცვლისა და განადგურების წესები (გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი საჯარო ინფორმაციის ხელმისაწვდომობას განსაზღვრავს), 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.“;

ბ) მე-4 პუნქტის შემდეგ დაემატოს შემდეგი შინაარსის მე-5 პუნქტი:

„5. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკების მიმართ ინფორმაციული აქტივების მართვის დამატებით სტანდარტებსა და მოთხოვნებს ადგენს ეროვნული ბანკი.“.

5. მე-6 მუხლი ჩამოყალიბდეს შემდეგი რედაქციით:

„მუხლი 6. კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტი და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტი

1. 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.

2. 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. ამ პუნქტით გათვალისწინებული აუდიტის ჩატარების მოთხოვნა არ ვრცელდება საგადახდო, ფასიანი ქაღალდების ანგარიშსწორებისა და რეზერვების მართვის სისტემებზე, აგრეთვე მონეტარული და სავალუტო ოპერაციებისთვის გამოყენებულ კრიტიკულ სისტემებზე.

3. 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.

4. 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.

5. 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.

6. ინფორმაციული უსაფრთხოების აუდიტის ციფრული მმართველობის სააგენტოს მიერ ავტორიზებული ორგანიზაციის მიერ ჩატარების შემთხვევაში აღნიშნული აუდიტის დასკვნის 1 ეგზემპლარს კრიტიკული ინფორმაციული სისტემის სუბიექტი აუდიტის დასრულებისთანავე, ამ მუხლის მე-2 ან მე-3 პუნქტით გათვალისწინებულ შემთხვევაში უგზავნის ოპერატიულ-ტექნიკურ სააგენტოს, ხოლო ამ მუხლის მე-4 პუნქტით გათვალისწინებულ შემთხვევაში – ციფრული მმართველობის სააგენტოს, გარდა ამ მუხლის მე-13 პუნქტით გათვალისწინებული შემთხვევისა.

7. 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.

8. ინფორმაციული უსაფრთხოების აუდიტის საფასური განისაზღვრება კრიტიკული ინფორმაციული სისტემის სუბიექტსა და ოპერატიულ-

ტექნიკურ სააგენტოს, ციფრული მმართველობის სააგენტოს ან ციფრული მმართველობის სააგენტოს მიერ ავტორიზებულ ორგანიზაციას შორის გაფორმებული ხელშეკრულებით.

9. კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია უზრუნველყოს ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის (შემდგომ – პენეტრაციის ტესტი) 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.

10. 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 კრიტიკული 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.

11. ციფრული მმართველობის სააგენტოს მიერ ავტორიზებული ორგანიზაციის მიერ პენეტრაციის ტესტის მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტში ჩატარების შემთხვევაში პენეტრაციის ტესტის დასკვნის 1 ეგზემპლარს კრიტიკული ინფორმაციული სისტემის სუბიექტი ამ ტესტის დასრულებისთანავე უგზავნის ოპერატიულ-ტექნიკურ სააგენტოს, ხოლო ასეთი ორგანიზაციის მიერ პენეტრაციის ტესტის მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტში ჩატარების შემთხვევაში პენეტრაციის ტესტის დასკვნის 1 ეგზემპლარს კრიტიკული ინფორმაციული სისტემის სუბიექტი ამ ტესტის დასრულებისთანავე უგზავნის ციფრული მმართველობის სააგენტოს, გარდა ამ მუხლის მე-13 პუნქტით გათვალისწინებული შემთხვევისა.

12. 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.

13. ციფრული მმართველობის სააგენტოს ან ციფრული მმართველობის სააგენტოს მიერ ავტორიზებული ორგანიზაციის (მათ შორის, ამ კანონის 6^1 მუხლის მე-4 პუნქტის შესაბამისად ავტორიზებული ორგანიზაციის) მიერ ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ

ბანკში ჩატარების შემთხვევაში ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის დასკვნის 1 ეგზემპლარს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკი ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის დასრულებისთანავე უგზავნის ეროვნულ ბანკს.

14. 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.

15. ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის ჩატარებისას ოპერატიულ-ტექნიკურ სააგენტოს, ციფრული მმართველობის სააგენტოს და კიბერუსაფრთხოების ბიუროს ხელი არ მიუწვდებათ იმ ინფორმაციაზე, რომელიც სცილდება ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის ჩატარების მიზნებს.

16. სახელმწიფო აუდიტის სამსახურის მიერ ინფორმაციული ტექნოლოგიების აუდიტის (მათ შორის, ინფორმაციული უსაფრთხოების აუდიტის) ჩატარების უფლებამოსილება, მისი საქმიანობის ორგანიზება და წესი განისაზღვრება „სახელმწიფო აუდიტის სამსახურის შესახებ“ საქართველოს ორგანული კანონით.

17. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკი ამ მუხლის მე-14 პუნქტით გათვალისწინებულ სამოქმედო გეგმას და მისი შესრულების გრაფიკს ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის დასრულებიდან 1 თვის ვადაში შესათანხმებლად წარუდგენს ეროვნულ ბანკს. ეროვნული ბანკი უზრუნველყოფს მისთვის წარდგენილი სამოქმედო გეგმის შეფასებას, შესაბამისი რეკომენდაციების ან/და შესასრულებლად სავალდებულო მითითებების შემუშავებას და შეთანხმებული სამოქმედო გეგმის შესრულების მონიტორინგს.

18. ამ მუხლით გათვალისწინებული ინფორმაციული უსაფრთხოების აუდიტი ან პენეტრაციის ტესტი ტარდება კრიტიკული ინფორმაციული

სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერთან ან/და კომპიუტერული უსაფრთხოების სპეციალისტთან თანამშრომლობითა და კოორდინაციით.“.

6. კანონს დაემატოს შემდეგი შინაარსის 6^1 მუხლი:

„მუხლი 6^1. ავტორიზაცია ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის

1. ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარების უფლება აქვს ორგანიზაციას, რომელსაც ციფრული მმართველობის სააგენტოში ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით დადგენილი წესის შესაბამისად გავლილი აქვს ავტორიზაცია ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის. ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარების უფლებამოსილების მქონე ორგანიზაციათა მიერ ავტორიზაციის გავლის საფასური დგინდება „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“ საქართველოს კანონის შესაბამისად.

2. ინფორმაციული უსაფრთხოების აუდიტი ან/და პენეტრაციის ტესტი შეიძლება ჩაატაროს პირმა, რომელსაც საქართველოს სახელმწიფო უსაფრთხოების სამსახურის უფროსის ნორმატიული აქტით დადგენილი წესის შესაბამისად გავლილი აქვს უსაფრთხოებაზე შემოწმება.

3. ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის ავტორიზაცია, გარდა ამ მუხლის მე-4 პუნქტით გათვალისწინებული შემთხვევისა, შეიძლება გაიაროს ორგანიზაციამ:

ა) რომელიც აკმაყოფილებს სახელმწიფო უსაფრთხოების სამსახურის

უფროსის ნორმატიული აქტით განსაზღვრულ უსაფრთხოების მოთხოვნებს;

ბ) რომლის ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარების უფლებამოსილების მქონე თანამშრომელი აკმაყოფილებს ამ მუხლის მე-2 პუნქტით განსაზღვრულ მოთხოვნას.

4. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკში ინფორმაციული უსაფრთხოების აუდიტი ან/და პენეტრაციის ტესტი კომერციული ბანკის შერჩევით შეიძლება ჩაატარონ აგრეთვე კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის ავტორიზებულმა ორგანიზაციებმა, რომელთა სიას კომერციული ბანკების მოთხოვნის საფუძველზე ციფრული მმართველობის სააგენტოს წარუდგენს ეროვნული ბანკი. ციფრული მმართველობის სააგენტო უზრუნველყოფს აღნიშნული ორგანიზაციების ავტორიზაციას კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის ავტორიზებული ორგანიზაციების დამატებით სიაში რეგისტრაციით. კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის ავტორიზებული ორგანიზაციების ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარების უფლებამოსილების მქონე თანამშრომლების ამ მუხლის მე-2 პუნქტით დადგენილი წესის შესაბამისად უსაფრთხოებაზე შემოწმების მიზნით შემოწმების პროცესის ინიციირებას მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკის ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის დაწყებამდე აღნიშნული კომერციული ბანკის შეტყობინების საფუძველზე

უზრუნველყოფს ეროვნული ბანკი. ეროვნული ბანკი უზრუნველყოფს აგრეთვე ამ კომერციული ბანკისთვის უსაფრთხოებაზე შემოწმების შედეგების შესახებ ინფორმაციის მიწოდებას.“.

7. მე-7 მუხლის:

ა) მე-4 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„4. ინფორმაციული უსაფრთხოების მენეჯერი ადგენს ინფორმაციული უსაფრთხოების სამოქმედო გეგმას და ამ სამოქმედო გეგმის შესრულების შესახებ ყოველწლიურ ანგარიშს წარუდგენს ამ მუხლის მე-3 პუნქტით გათვალისწინებულ პირს/პირებს. პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ინფორმაციული უსაფრთხოების მენეჯერები აღნიშნულ სამოქმედო გეგმას და მისი შესრულების შესახებ ყოველწლიურ ანგარიშს წარუდგენენ აგრეთვე ოპერატიულ-ტექნიკურ სააგენტოს, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების ინფორმაციული უსაფრთხოების მენეჯერები – ციფრული მმართველობის სააგენტოს, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტების ინფორმაციული უსაფრთხოების მენეჯერები – კიბერუსაფრთხოების ბიუროს.“;

ბ) მე-4 პუნქტის შემდეგ დაემატოს შემდეგი შინაარსის მე-5 პუნქტი:

„5. პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ინფორმაციული უსაფრთხოების მენეჯერებად შესაძლებელია განისაზღვროს 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.“.

8. მე-8 მუხლის:

ა) სათაური ჩამოყალიბდეს შემდეგი რედაქციით:

„ოპერატიულ-ტექნიკური სააგენტოს, ციფრული მმართველობის სააგენტოს და კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფები“;

ბ) პირველი პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„1. ამ კანონის აღსრულებას, კერძოდ, 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.“;

გ) მე-3 და მე-4 პუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

„3. ოპერატიულ-ტექნიკური სააგენტოს, ციფრული მმართველობის

სააგენტოს და კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფების მოვალეობებია:

ა) კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა ან/და ამ კანონით გათვალისწინებულ შემთხვევებში სახელმძღვანელო მითითებების გაცემა;

ბ) კომპიუტერული ინციდენტების დროული გამოვლენა;

გ) კომპიუტერულ ინციდენტებზე რეაგირება და მათზე რეაგირების კოორდინაცია;

დ) კომპიუტერული ინციდენტების აღრიცხვა და მათზე რეაგირების პრიორიტეტების დადგენა და კატეგორიზაცია;

ე) კომპიუტერული ინციდენტების ანალიზი;

ვ) კომპიუტერული ინციდენტების შედეგების გამოსწორებისა და ზიანის მინიმუმამდე შემცირების პროცესში დახმარება;

ზ) კომპიუტერული ინციდენტების პრევენციისკენ მიმართული ზომების კოორდინაცია და ამ ზომების დანერგვაში დახმარება;

თ) სხვა მოვალეობები, რომლებიც დაკავშირებულია ინფორმაციული უსაფრთხოების მიზნებთან და განისაზღვრება კანონით ან სხვა ნორმატიული აქტით.

4. ოპერატიულ-ტექნიკური სააგენტოს/ციფრული მმართველობის სააგენტოს/კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის კომპეტენცია, მუშაობის პროცედურები, კომპიუტერულ ინციდენტებზე რეაგირების მექანიზმები და მისი საქმიანობის სხვა წესები დგინდება ოპერატიულ-ტექნიკური სააგენტოს უფროსის/ციფრული მმართველობის სააგენტოს თავმჯდომარის/საქართველოს თავდაცვის

მინისტრის ბრძანებით, მისი კომპეტენციის ფარგლებში.“;

დ) მე-5 პუნქტი ამოღებულ იქნეს.

9. კანონს დაემატოს შემდეგი შინაარსის 8^1 და 8^2 მუხლები:

„მუხლი 8^1. ციფრული მმართველობის სააგენტოს და ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის უფლებები და მოვალეობები

1. ციფრული მმართველობის სააგენტო საქართველოს კანონმდებლობით განსაზღვრული უფლებამოსილებების ფარგლებში ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების სფეროებში ახორციელებს შემდეგ მაკოორდინირებელ საქმიანობებს:

ა) კოორდინაციას უწევს კიბერუსაფრთხოების ეროვნული სტრატეგიის სამოქმედო გეგმის შემუშავების პროცესს და ამ სამოქმედო გეგმის პროექტს წარუდგენს ეროვნული უსაფრთხოების საბჭოს საქართველოს მთავრობის მიერ აღნიშნული სტრატეგიისა და მისი სამოქმედო გეგმის დასამტკიცებლად;

ბ) ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების სფეროებში საჯარო პოლიტიკის, მეთოდოლოგიების, სტანდარტების, სახელმძღვანელო პრინციპების, წესებისა და პროცედურების შემუშავებისა და დანერგვის მიზნით ქმნის უწყებათაშორის სამუშაო ჯგუფებს და წარმართავს მათ საქმიანობას;

გ) ფართომასშტაბიან კიბერინციდენტებზე რეაგირების პროცესში კოორდინაციას უწევს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის საქმიანობას;

დ) ზედამხედველობას უწევს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ინფორმაციული უსაფრთხოებისა

და კიბერუსაფრთხოების სფეროებში სამართლებრივი, სტრატეგიული და მარეგულირებელი დოკუმენტების აღსრულების პროცესს და ამზადებს საქართველოს მთავრობისთვის წარსადგენ შესაბამის ანგარიშებს;

ე) კოორდინაციას უწევს ეროვნულ დონეზე ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების სფეროებში საგანმანათლებლო და ცნობიერების ამაღლების კამპანიების, აგრეთვე ამ სფეროების სპეციალისტების შესაძლებლობების გაზრდის მიზნით ერთობლივი კიბერსავარჯიშოებისა და კიბერსწავლების ღონისძიებების ჩატარების პროცესს;

ვ) ქმნის და ადმინისტრირებას უწევს კიბერინციდენტების თაობაზე ანგარიშგებისა და მათ შესახებ ინფორმაციის გაზიარების პლატფორმას და კიბერინციდენტების რეესტრს;

ზ) საქართველოს მთავრობას წარუდგენს ანგარიშს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონით გათვალისწინებული ვალდებულებების შესრულების თაობაზე.

2. ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი, ამ კანონის მე-8 მუხლის მე-3 პუნქტით გათვალისწინებული მოვალეობების შესრულების გარდა, ახორციელებს:

ა) ინფორმაციული უსაფრთხოების საკითხებზე საზოგადოების საგანმანათლებლო კამპანიას და სათანადო ინფორმაციით მის უზრუნველყოფას;

ბ) შესაძლო საფრთხეების შესახებ მოსახლეობის ფართო წრის გაფრთხილებას და მისთვის სათანადო ინფორმაციის მიწოდებას;

გ) თავისი კომპეტენციის ფარგლებში საერთაშორისო დონეზე

ინფორმაციული უსაფრთხოების საკითხებზე წარმომადგენლობას;

დ) ინფორმაციული უსაფრთხოების საკითხებზე საზოგადოების ცნობიერების ამაღლებას.

3. ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი უფლებამოსილია:

ა) მოითხოვოს და მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობის შემთხვევაში ჰქონდეს წვდომა ამ სუბიექტის ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე, თუ ასეთი წვდომა აუცილებელია მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის სისტემაში მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე რეაგირებისთვის. ინფორმაციული უსაფრთხოების მენეჯერი მოთხოვნის გონივრულ ვადაში განხილვის შემდეგ ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს დაუყოვნებლივ აცნობებს აღნიშნულ წვდომაზე თანხმობის ან უარის შესახებ;

ბ) ამ კანონის მე-10 მუხლის მე-6 პუნქტით დადგენილი წესით ჰქონდეს წვდომა მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელურ სენსორზე.

მუხლი 8^2. ინფორმაციული უსაფრთხოების უზრუნველყოფასთან დაკავშირებული დამატებითი მოთხოვნები

1. კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ მონაცემების მიღებისთვის, დამუშავებისთვის, შენახვისთვის ან/და გადაცემისთვის გამოყენებული აპარატული ან/და პროგრამული უზრუნველყოფის

საშუალებების მწარმოებელ ქვეყნებთან დაკავშირებული დამატებითი მოთხოვნები განისაზღვრება საქართველოს მთავრობის დადგენილებით.

2. საქართველოს სახელმწიფო ბიუჯეტის დაფინანსებაზე მყოფ სახელმწიფო ან მუნიციპალიტეტის ორგანოებს ან დაწესებულებებს, კრიტიკული ინფორმაციული სისტემის სუბიექტ საჯარო სამართლის იურიდიულ პირებს შორის ამ კანონით გათვალისწინებული კონფიდენციალური ან შინასამსახურებრივი გამოყენების ინფორმაციის, აგრეთვე სახელმწიფო საიდუმლოების შემცველი ინფორმაციის უსაფრთხო გაცვლისთვის ოპერატიულ-ტექნიკური სააგენტო უფლებამოსილია შექმნას კლასიფიცირებული ინფორმაციის გაცვლის სისტემა და ამ მიზნით შექმნას და გამოიყენოს სპეციალური ოპტიკურ-ბოჭკოვანი ქსელი. საქართველოს სახელმწიფო ბიუჯეტის დაფინანსებაზე მყოფმა სახელმწიფო ან მუნიციპალიტეტის ორგანოებმა ან დაწესებულებებმა, კრიტიკული ინფორმაციული სისტემის სუბიექტმა საჯარო სამართლის იურიდიულმა პირებმა, რომლებსაც კლასიფიცირებული ინფორმაციის გაცვლის სისტემაში ჩართვა სურთ, წერილობით, ოპერატიულ-ტექნიკური სააგენტოს უფროსის ბრძანებით დადგენილი წესის შესაბამისად უნდა მიმართონ ოპერატიულ-ტექნიკურ სააგენტოს.

3. ოპერატიულ-ტექნიკურ სააგენტოს ამ მუხლის მე-2 პუნქტით გათვალისწინებული კლასიფიცირებული ინფორმაციის გაცვლის სისტემით გადაცემული ინფორმაციის შინაარსზე ხელი არ მიუწვდება.“.

10. მე-9 მუხლის:

ა) მე-2 პუნქტის „ბ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„ბ) კომპიუტერული ინციდენტის იდენტიფიცირება, მასზე რეაგირება

და კომპიუტერული ინციდენტის შესახებ ინფორმაციის დაუყოვნებლივ მიწოდება: პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში – ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფისთვის, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში – ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფისთვის, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში – კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფისთვის;";

ბ) მე-4 და მე-5 პუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

„4. კომპიუტერული უსაფრთხოების სპეციალისტი ხელმისაწვდომი უნდა იყოს ნებისმიერ დროს, მათ შორის, სამუშაო საათების შემდეგ. იგი ვალდებულია კრიტიკული ინფორმაციული სისტემის სუბიექტზე მიმდინარე ან სავარაუდო კიბერშეტევის და მისი შედეგების აღმოფხვრის პროცესში უზრუნველყოს მუდმივი კოორდინაცია: პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში – ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფთან, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში – ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფთან, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში – კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფთან.

5. თუ მიმდინარე ან სავარაუდო კიბერშეტევა განსაკუთრებულ

საფრთხეს უქმნის სახელმწიფოს თავდაცვისუნარიანობას, ეკონომიკურ უსაფრთხოებას, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალურ ფუნქციონირებას, ოპერატიულ-ტექნიკური სააგენტო უფლებამოსილია კიბერშეტევის თავიდან აცილების, მოგერიების ან/და მისი შედეგების აღმოფხვრის მიზნით განახორციელოს კომპიუტერული უსაფრთხოების სპეციალისტებისა და ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის დროებითი კოორდინაცია. საომარი მდგომარეობის დროს კიბერუსაფრთხოების უზრუნველყოფა და კიბეროპერაციები ხორციელდება „საომარი მდგომარეობის შესახებ“ საქართველოს კანონის შესაბამისად.“;

გ) მე-5 პუნქტის შემდეგ დაემატოს შემდეგი შინაარსის მე-6 პუნქტი:

„6. პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების კომპიუტერული უსაფრთხოების სპეციალისტებად შესაძლებელია განისაზღვროს პირები, რომლებსაც აქვთ სახელმწიფო საიდუმლოებასთან დაშვება.“.

11. კანონს დაემატოს შემდეგი შინაარსის 9^1 მუხლი:

„მუხლი 9^1. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმება

1. 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. ამ გადაწყვეტილებაში უნდა მიეთითოს აღნიშნული შემოწმების ჩატარების

უფლებამოსილების მქონე პირის ვინაობა და შემოწმების ფარგლები. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმება შესაძლებელია მოიცავდეს:

ა) აღნიშნული სუბიექტის შიდა ქსელს, გარე ქსელზე წვდომის წერტილს, ქსელის კონფიგურირებას, ქსელის ფუნქციონირებისა და მისი უსაფრთხოებისთვის გამოყენებულ აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებებს;

ბ) ქსელში ჩართულ აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებებს, რომლებიც გამოიყენება მონაცემების მიღებისთვის, დამუშავებისთვის, შენახვისთვის ან/და გადაცემისთვის;

გ) აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების ქსელში ჩართვის ფორმალიზებულ ან არაფორმალიზებულ წესებსა და პროცედურებს.

2. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების ჩატარების წესი და პროცედურები დგინდება ოპერატიულ-ტექნიკური სააგენტოს უფროსის ბრძანებით.

3. ამ მუხლის პირველი პუნქტის შესაბამისად 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 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. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმება ტარდება პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერთან, კომპიუტერული უსაფრთხოების სპეციალისტთან ან/და სხვა უფლებამოსილ წარმომადგენლებთან თანამშრომლობითა და კოორდინაციით.

4. ამ მუხლის პირველი პუნქტის შესაბამისად საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების ჩატარების უფლებამოსილების მქონე პირი დამტკიცებული ფორმის მიხედვით ადგენს საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების შესახებ დასკვნას. ამ დასკვნაში უნდა მიეთითოს: შემოწმების ჩატარების თარიღი, დრო და ადგილი; შემოწმების ჩატარების საფუძველი; შემოწმებაზე დამსწრე პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის წარმომადგენლის/წარმომადგენლების ვინაობა; შემოწმებული დოკუმენტების ჩამონათვალი; შემოწმებული აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებები ან/და ქსელური ინფრასტრუქტურა და შემოწმებისთვის გამოყენებული აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებები; მიღებული ზეპირი ახსნა-განმარტებების

მიმოხილვა (წერილობითი ახსნა-განმარტებების მიღების შემთხვევაში აღნიშნულ დასკვნას უნდა დაერთოს შესაბამისი მასალა); დასკვნა, რომელშიც აღნიშნულია რეკომენდაციები ან/და შესასრულებლად სავალდებულო მითითებები (მათი არსებობის შემთხვევაში); შესასრულებლად სავალდებულო მითითებებით გათვალისწინებული ღონისძიებების განხორციელების ვადა; შემოწმების ჩატარების უფლებამოსილების მქონე პირის ხელმოწერა, პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის წარმომადგენლის/წარმომადგენლების ხელმოწერა/ხელმოწერები, ხოლო მის/მათ მიერ ხელის მოწერაზე უარის თქმის შემთხვევაში – შემოწმებაზე დამსწრე სულ ცოტა 2 პირის ხელმოწერები.

5. თუ ამ მუხლის პირველი პუნქტის შესაბამისად საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების ჩატარების შედეგად გამოვლენილი დამრღვევი პირის ქმედებაში გამოიკვეთება საქართველოს სისხლის სამართლის კანონმდებლობით განსაზღვრული დანაშაულის ნიშნები, ოპერატიულ-ტექნიკური სააგენტო ამ შემოწმების მასალებს დაუყოვნებლივ წარუდგენს საგამოძიებო ორგანოს.

6. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია:

ა) უზრუნველყოს ამ მუხლის მე-4 პუნქტით გათვალისწინებული შესასრულებლად სავალდებულო მითითებების შესრულება და ამ კანონის მე-4 მუხლის თანახმად მიღებული დოკუმენტების მათთან შესაბამისობა;

ბ) ოპერატიულ-ტექნიკურ სააგენტოს წინასწარ შეუთანხმოს საინფორმაციო-ტექნოლოგიურ ინფრასტრუქტურაში დაგეგმილი

ცვლილებები, რომლებმაც შესაძლებელია გავლენა მოახდინოს ამ მუხლის მე-4 პუნქტით გათვალისწინებული შესასრულებლად სავალდებულო მითითებების შესრულებაზე.

7. ამ მუხლით გათვალისწინებული საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმებასთან დაკავშირებული მოთხოვნები არ ვრცელდება საგადახდო, ფასიანი ქაღალდების ანგარიშსწორებისა და რეზერვების მართვის სისტემებზე, აგრეთვე მონეტარული და სავალუტო ოპერაციებისთვის გამოყენებულ კრიტიკულ სისტემებზე.“.

12. მე-10 მუხლი ჩამოყალიბდეს შემდეგი რედაქციით:

„მუხლი 10. კომპიუტერული ინციდენტის იდენტიფიცირება და მის შესახებ შეტყობინება

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი ახორციელებს კომპიუტერული ინციდენტის იდენტიფიცირებას, რაც მოიცავს ამ ინციდენტის შესწავლას, აღწერას და მასზე რეაგირებას. კრიტიკული ინფორმაციული სისტემის სუბიექტი კომპიუტერული ინციდენტის იდენტიფიცირების მიზნით იყენებს ქსელურ სენსორს. ქსელური სენსორის კონფიგურირების წესები პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის 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. ამ პუნქტით გათვალისწინებული ქსელური სენსორის კონფიგურირების წესები ოპერატიულ-ტექნიკური

სააგენტოს, ციფრული მმართველობის სააგენტოს და კიბერუსაფრთხოების ბიუროს მიერ კრიტიკული ინფორმაციული სისტემის სუბიექტის კომუნიკაციის შინაარსობრივი მონაცემის ხელმისაწვდომობის შესაძლებლობას უნდა გამორიცხავდეს.

2. კომპიუტერული ინციდენტის პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტში იდენტიფიცირების შესახებ დაუყოვნებლივ ეცნობება ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტში იდენტიფიცირების შესახებ – ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს, ხოლო თავდაცვის სფეროში შემავალ კრიტიკული ინფორმაციული სისტემის სუბიექტში იდენტიფიცირების შესახებ – კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს. კრიტიკული ინფორმაციული სისტემის სუბიექტი კომპიუტერული ინციდენტის შესახებ ინფორმაციის შენახვისა და დაცვის მიზნით აუცილებლობის შემთხვევაში ახორციელებს გადაუდებელ ღონისძიებებს.

3. კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი შეისწავლის, აღწერს კომპიუტერულ ინციდენტს და ახდენს მასზე რეაგირებას ამ კანონით გათვალისწინებული ფუნქციების შესრულებისას. კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი კომპიუტერული ინციდენტის შესწავლის შემდეგ შეიმუშავებს და კრიტიკული ინფორმაციული სისტემის სუბიექტს წარუდგენს შესასრულებლად სავალდებულო მითითებებს. შესასრულებლად სავალდებულო მითითება 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. კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია გონივრულ ვადაში მოახდინოს შესასრულებლად სავალდებულო მითითებაზე რეაგირება და განახორციელოს შესაბამისი ღონისძიებები. განხორციელებული ღონისძიებების შესახებ ინფორმაციას პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტები წარუდგენენ ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტები – ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტები – კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს.

4. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელში მიმდინარე კომპიუტერული ინციდენტის იდენტიფიცირებას ახორციელებს ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი ან/და პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტი.

5. კომპიუტერული ინციდენტის იდენტიფიცირების ან/და მასზე რეაგირების მიზნით ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ

ინციდენტებზე დახმარების ჯგუფი უფლებამოსილია:

ა) ამ მუხლის მე-4 პუნქტით გათვალისწინებული უფლებამოსილების განხორციელების მიზნით ჰქონდეს წვდომა პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელურ სენსორზე, გარდა იმ შემთხვევისა, როდესაც პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელით გადაცემული/მიღებული ტრაფიკის მაიდენტიფიცირებელი მონაცემი საბანკო გადარიცხვების შესახებ ინფორმაციას შეიცავს. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია უზრუნველყოს ამგვარი წვდომა და აღნიშნული წვდომის სტაბილური ფუნქციონირება. ქსელური სენსორის კონფიგურირებასა და მართვას ოპერატიულ-ტექნიკური სააგენტო და კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტი ერთობლივად ახორციელებენ;

ბ) მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობით ჰქონდეს წვდომა ამ სუბიექტის ქსელურ სენსორზე. ქსელური სენსორის კონფიგურირებასა და მართვას ოპერატიულ-ტექნიკური სააგენტო და კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტი ერთობლივად ახორციელებენ;

გ) პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტს მოსთხოვოს ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე წვდომა, თუ ამგვარი წვდომა აუცილებელია მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე რეაგირებისთვის. პირველი კატეგორიის კრიტიკული

ინფორმაციული სისტემის სუბიექტი ვალდებულია აღნიშნული წვდომა დაუყოვნებლივ, მოთხოვნისთანავე უზრუნველყოს. ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე წვდომა პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტის მონაწილეობით ხორციელდება;

დ) მოითხოვოს და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობის შემთხვევაში ჰქონდეს წვდომა ამ სუბიექტის ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე, თუ ასეთი წვდომა აუცილებელია მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე რეაგირებისთვის. ინფორმაციული უსაფრთხოების მენეჯერი მოთხოვნის გონივრულ ვადაში განხილვის შემდეგ ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს დაუყოვნებლივ აცნობებს აღნიშნულ წვდომაზე თანხმობის ან უარის შესახებ. თანხმობის შემთხვევაში ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე წვდომა მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტის მონაწილეობით ხორციელდება;

ე) კომპიუტერული ინციდენტის იდენტიფიცირების შემდეგ ამ ინციდენტის განმეორების საფრთხის თავიდან აცილების მიზნით მოსთხოვოს ელექტრონული კომუნიკაციის კომპანიას მის ინფრასტრუქტურაში მსგავსი კომპიუტერული ინციდენტის იდენტიფიცირებისა და ნეიტრალიზებისთვის აუცილებელი ღონისძიებების განხორციელება. აღნიშნული მოთხოვნა

ელექტრონული კომუნიკაციის კომპანიის ტექნიკურ შესაძლებლობებს უნდა ითვალისწინებდეს.

6. კომპიუტერული ინციდენტის იდენტიფიცირების ან/და მასზე რეაგირების მიზნით ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი უფლებამოსილია მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობით ჰქონდეს წვდომა ამ სუბიექტის ქსელურ სენსორზე. ქსელური სენსორის კონფიგურირებასა და მართვას ციფრული მმართველობის სააგენტო და კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტი ერთობლივად ახორციელებენ.

7. კომპიუტერული ინციდენტის იდენტიფიცირების შესახებ ინფორმაციის გაზიარებისა და შესაბამის მოქმედებათა კოორდინაციის მიზნით ოპერატიულ-ტექნიკური სააგენტოს, ციფრული მმართველობის სააგენტოს და კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფები უზრუნველყოფენ კომპიუტერული ინციდენტის შესახებ ინფორმაციის გაზიარების ერთიანი პლატფორმის შექმნას.

8. კომპიუტერული ინციდენტების კლასიფიცირების წესი განისაზღვრება საქართველოს მთავრობის დადგენილებით.

9. ამ მუხლით გათვალისწინებული კომპიუტერული ინციდენტის იდენტიფიცირებასთან დაკავშირებული მოთხოვნები არ ვრცელდება პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის საგადახდო, ფასიანი ქაღალდების ანგარიშსწორებისა და რეზერვების მართვის სისტემებზე, აგრეთვე მონეტარული და სავალუტო ოპერაციებისთვის გამოყენებულ კრიტიკულ სისტემებზე.“.

13. 10^1 მუხლის:

ა) პირველი პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„1. თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტების ინფორმაციული უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს თავდაცვის სფეროში ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს (თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტების კრიტიკულობის კლასიფიცირების გათვალისწინებით). ამ მოთხოვნებს 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 განსაზღვრავს კიბერუსაფრთხოების ბიურო და ბრძანებით ადგენს საქართველოს თავდაცვის მინისტრი.“;

ბ) მე-3–მე-5 პუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

„3. კიბერუსაფრთხოების ბიუროს მოქმედების სფერო არ ვრცელდება ოპერატიულ-ტექნიკურ სააგენტოსა და ციფრული მმართველობის სააგენტოზე, რომელთა უფლებამოსილებები, ფუნქციები და მოქმედების სფეროები განისაზღვრება ამ კანონითა და „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ და „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“ საქართველოს კანონებით.

4. თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხა მტკიცდება და შესაბამისი სუბიექტის

კრიტიკულობის კლასიფიცირება დგინდება საქართველოს მთავრობის შესაბამისი აქტით, რომლის პროექტს საქართველოს მთავრობას დასამტკიცებლად წარუდგენს საქართველოს თავდაცვის სამინისტრო ეროვნული უსაფრთხოების საბჭოსთან, საქართველოს იუსტიციისა და შინაგან საქმეთა სამინისტროებთან და საქართველოს სახელმწიფო უსაფრთხოების სამსახურთან შეთანხმებით. ამ ნუსხის შედგენისას გაითვალისწინება შემდეგი კრიტერიუმები: ინფორმაციული სისტემის შეფერხების ან მწყობრიდან გამოსვლის სავარაუდო შედეგების სიმძიმე და მასშტაბი სახელმწიფოს თავდაცვისუნარიანობის თვალსაზრისით; სავარაუდო ეკონომიკური ზარალის სიმძიმე სუბიექტებისთვის ან/და სახელმწიფოსთვის; ინფორმაციული სისტემის მიერ გაწეული მომსახურების აუცილებლობა სახელმწიფოს თავდაცვისუნარიანობის შეუფერხებელი ფუნქციონირებისათვის; ინფორმაციული სისტემის მომხმარებელთა რაოდენობა; სუბიექტის მატერიალური მდგომარეობა და სავარაუდო ხარჯების ოდენობა, რომლებიც მისთვის შესაბამისი ვალდებულებების დაკისრებას მოჰყვება.

5. კიბერუსაფრთხოების ბიუროს დებულებას ამტკიცებს საქართველოს თავდაცვის მინისტრი.“;

გ) მე-7 პუნქტი ამოღებულ იქნეს.

14. 10^2 მუხლის მე-2 პუნქტი ამოღებულ იქნეს.

15. 10^3 მუხლის:

ა) პირველი და მე-2 პუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

„1. თავდაცვის სფეროში შემავალ კრიტიკული ინფორმაციული სისტემის სუბიექტზე განხორციელებული იმ კიბერშეტევის მართვას,

რომელიც საფრთხეს უქმნის ადამიანის სიცოცხლესა და ჯანმრთელობას, სახელმწიფო ინტერესებსა და სახელმწიფოს თავდაცვისუნარიანობას, აგრეთვე ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული სხვა ინციდენტების მართვას და მასთან დაკავშირებულ საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი.

2. კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფისთვის პრიორიტეტული საფრთხეები და თავდაცვის სფეროში ამ ჯგუფის მოვალეობები განისაზღვრება ამ კანონის მე-8 მუხლით.“;

ბ) მე-2 პუნქტის შემდეგ დაემატოს შემდეგი შინაარსის მე-3–მე-5 პუნქტები:

„3. თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული ინციდენტის იდენტიფიცირებისა და მასზე რეაგირების მიზნით კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი უფლებამოსილია:

ა) ჰქონდეს წვდომა აღნიშნული კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელურ სენსორზე;

ბ) ჰქონდეს წვდომა აღნიშნული კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე, თუ ასეთი წვდომა აუცილებელია მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე რეაგირებისთვის.

4. კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე

დახმარების ჯგუფი კომპიუტერული ინციდენტის იდენტიფიცირების შემთხვევაში ინფორმაციული აქტივის უსაფრთხოების მიზნით ახორციელებს გადაუდებელ ღონისძიებებს, რომლებიც მოიცავს კომპიუტერულ ინციდენტზე რეაგირებას, მის შესწავლასა და აღწერას. კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი კომპიუტერული ინციდენტის შესწავლისა და აღწერის შემდეგ შეიმუშავებს და თავდაცვის სფეროში შემავალ კრიტიკული ინფორმაციული სისტემის სუბიექტს წარუდგენს შესასრულებლად სავალდებულო მითითებებსა და რეკომენდაციებს.

5. თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია გონივრულ ვადაში (არაუმეტეს 1 თვისა) მოახდინოს შესასრულებლად სავალდებულო მითითებაზე რეაგირება და განახორციელოს შესაბამისი ღონისძიებები. განხორციელებული ღონისძიებების შესახებ ინფორმაციას აღნიშნული კრიტიკული ინფორმაციული სისტემის სუბიექტი წარუდგენს კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს.“.

16. კანონს დაემატოს შემდეგი შინაარსის III^2 თავი:

„თავი III^2. ადმინისტრაციული პასუხისმგებლობა ამ კანონის დარღვევისთვის

მუხლი 10^4. ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დასანერგად განსაზღვრული ვადის დარღვევა

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.

მუხლი 10^5. საქართველოს მთავრობის დადგენილებით განსაზღვრული დამატებითი მოთხოვნების შეუსრულებლობა

1. პირველი/მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის 8^2 მუხლის პირველი პუნქტით გათვალისწინებული საქართველოს მთავრობის დადგენილებით განსაზღვრული დამატებითი მოთხოვნების შეუსრულებლობა –

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.

მუხლი 10^6. ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის ჩატარების ვალდებულების შეუსრულებლობა

1. პირველი/მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-6 მუხლის პირველი და მე-7 პუნქტებით გათვალისწინებული ინფორმაციული უსაფრთხოების აუდიტის ჩატარების ვალდებულების ან ამ კანონის მე-6 მუხლის მე-9 და მე-12 პუნქტებით გათვალისწინებული პენეტრაციის ტესტის ჩატარების ვალდებულების შეუსრულებლობა –

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.

მუხლი 10^7. ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების განსახილველად წარუდგენლობა ან შესასრულებლად სავალდებულო მითითების შეუსრულებლობა

1. პირველი/მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-4 მუხლის მე-3 პუნქტით გათვალისწინებული ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების განსახილველად წარუდგენლობა ან შესასრულებლად სავალდებულო მითითების შეუსრულებლობა –

გამოიწვევს გაფრთხილებას ან დაჯარიმებას 10 000 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 20 000 ლარის ოდენობით.

მუხლი 10^{8}. კომპიუტერული ინციდენტის იდენტიფიცირების შესახებ შეუტყობინებლობა, შესასრულებლად სავალდებულო მითითების შეუსრულებლობა ან განხორციელებული ღონისძიებების შესახებ ინფორმაციის წარუდგენლობა

1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-10 მუხლის მე-2 პუნქტით დადგენილი წესით კომპიუტერული ინციდენტის იდენტიფიცირების შესახებ შეუტყობინებლობა ან ამ კანონის მე-10 მუხლის მე-3 პუნქტით გათვალისწინებულ შემთხვევაში ოპერატიულ-ტექნიკური სააგენტოს მიერ გაცემული შესასრულებლად სავალდებულო მითითების შეუსრულებლობა ან განხორციელებული ღონისძიებების შესახებ ინფორმაციის წარუდგენლობა –

გამოიწვევს გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

2. ამ მუხლის პირველი პუნქტით გათვალისწინებული ქმედება, ჩადენილი იმ პირველი 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.

3. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-10 მუხლის მე-2 პუნქტით დადგენილი წესით კომპიუტერული ინციდენტის იდენტიფიცირების შესახებ შეუტყობინებლობა ან ამ კანონის მე-10 მუხლის მე-3 პუნქტით გათვალისწინებულ შემთხვევაში ციფრული მმართველობის სააგენტოს მიერ გაცემული შესასრულებლად სავალდებულო მითითების შეუსრულებლობა ან განხორციელებული ღონისძიებების შესახებ ინფორმაციის წარუდგენლობა –

გამოიწვევს გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

4. ამ მუხლის მე-3 პუნქტით გათვალისწინებული ქმედება, ჩადენილი იმ 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.

მუხლი 10^9. კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ინფორმაციული უსაფრთხოების აუდიტის დასკვნის ეგზემპლარის ან პენეტრაციის ტესტის დასკვნის ეგზემპლარის წარუდგენლობა

1. პირველი/მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-6 მუხლის მე-6 პუნქტით გათვალისწინებული ინფორმაციული უსაფრთხოების აუდიტის დასკვნის ეგზემპლარის ან ამ კანონის მე-6 მუხლის მე-11 პუნქტით გათვალისწინებული პენეტრაციის ტესტის დასკვნის ეგზემპლარის წარუდგენლობა –

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.

3. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკის მიერ ამ კანონის მე-6 მუხლის მე-13 პუნქტით გათვალისწინებული ინფორმაციული უსაფრთხოების აუდიტის დასკვნის ეგზემპლარის ან პენეტრაციის ტესტის დასკვნის ეგზემპლარის წარუდგენლობა –

გამოიწვევს დაჯარიმებას დარღვევის გამოვლენის მომენტისთვის ბოლო ანგარიშგების მდგომარეობით არსებული საზედამხედველო კაპიტალის 0.01%-ის, 0.05%-ის ან 0.1%-ის, მაგრამ არანაკლებ 20 000 (ოცი ათასი) ლარის ოდენობით, დარღვევის სერიოზულობიდან ან/და კომერციული ბანკის აქტივებისთვის მიყენებული ზარალიდან ან/და შესაძლო საფრთხიდან გამომდინარე.

მუხლი 10^{10}. სამოქმედო გეგმის შესათანხმებლად წარუდგენლობა ან შეთანხმებული სამოქმედო გეგმით გათვალისწინებული შესასრულებლად სავალდებულო მითითების შეუსრულებლობა

1. პირველი/მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-6 მუხლის მე-14 პუნქტით გათვალისწინებული სამოქმედო გეგმის შესათანხმებლად წარუდგენლობა ან შეთანხმებული სამოქმედო გეგმით გათვალისწინებული შესასრულებლად სავალდებულო

მითითების შეუსრულებლობა –

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.

3. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკის მიერ ამ კანონის მე-6 მუხლის მე-17 პუნქტით გათვალისწინებული სამოქმედო გეგმის შესათანხმებლად წარუდგენლობა ან შეთანხმებული სამოქმედო გეგმით გათვალისწინებული შესასრულებლად სავალდებულო მითითების შეუსრულებლობა –

გამოიწვევს დაჯარიმებას დარღვევის გამოვლენის მომენტისთვის ბოლო ანგარიშგების მდგომარეობით არსებული საზედამხედველო კაპიტალის 0.01%-ის, 0.05%-ის ან 0.1%-ის, მაგრამ არანაკლებ 20 000 (ოცი ათასი) ლარის ოდენობით, დარღვევის სერიოზულობიდან ან/და კომერციული ბანკის აქტივებისთვის მიყენებული ზარალიდან ან/და შესაძლო საფრთხიდან გამომდინარე.

მუხლი 10^{11}. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმებისთვის ხელის შეშლა ან/და მოთხოვნილი ინფორმაციის წარუდგენლობა

1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის 9^{1} მუხლით გათვალისწინებული საინფორმაციო-

ტექნოლოგიური ინფრასტრუქტურის შემოწმებისთვის ხელის შეშლა ან/და ოპერატიულ-ტექნიკური სააგენტოს მიერ მოთხოვნილი ინფორმაციის წარუდგენლობა –

გამოიწვევს გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

2. იგივე ქმედება, ჩადენილი იმ პირველი 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.

მუხლი 10^{12}. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების შესახებ დასკვნით გათვალისწინებული შესასრულებლად სავალდებულო მითითების შეუსრულებლობა

1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის 9^{1} მუხლის მე-4 პუნქტით განსაზღვრული საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების შესახებ დასკვნით გათვალისწინებული შესასრულებლად სავალდებულო მითითების შეუსრულებლობა –

გამოიწვევს გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

2. იგივე ქმედება, ჩადენილი იმ პირველი 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.

მუხლი 10^{13}. საინფორმაციო-ტექნოლოგიურ ინფრასტრუქტურაში დაგეგმილი ცვლილებების წინასწარ შეთანხმების ვალდებულების შეუსრულებლობა

1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის 9^{1} მუხლის მე-6 პუნქტის „ბ“ ქვეპუნქტით გათვალისწინებული საინფორმაციო-ტექნოლოგიურ ინფრასტრუქტურაში დაგეგმილი ცვლილებების წინასწარ შეთანხმების ვალდებულების შეუსრულებლობა –

გამოიწვევს გაფრთხილებას ან დაჯარიმებას 10 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 20 000 ლარის ოდენობით.

მუხლი 10^{14}. ქსელურ სენსორზე წვდომის უზრუნველყოფის ვალდებულების ან/და ასეთი წვდომის სტაბილური ფუნქციონირების ვალდებულების შეუსრულებლობა

1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფისთვის ამ კანონის მე-10 მუხლის მე-5 პუნქტის „ა“ ქვეპუნქტით გათვალისწინებულ ქსელურ სენსორზე წვდომის უზრუნველყოფის ვალდებულების ან/და ასეთი წვდომის სტაბილური ფუნქციონირების ვალდებულების შეუსრულებლობა –

გამოიწვევს გაფრთხილებას ან დაჯარიმებას 10 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 20 000 ლარის ოდენობით.

მუხლი 10^{15}. ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ სისტემაში შემავალ საგანზე წვდომის უფლების შეზღუდვა ან ასეთი წვდომისთვის ხელის შეშლა

1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ოპერატიულ-ტექნიკური სააგენტოსთვის ამ კანონის მე-10 მუხლის მე-5 პუნქტის „გ“ ქვეპუნქტით გათვალისწინებულ ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ სისტემაში შემავალ საგანზე წვდომის უფლების შეზღუდვა ან ასეთი წვდომისთვის ხელის შეშლა –

გამოიწვევს გაფრთხილებას ან დაჯარიმებას 2 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 5 000 ლარის ოდენობით.

მუხლი 10^{16}. მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ან ელექტრონული კომუნიკაციის კომპანიის მიერ ამ კანონით გათვალისწინებული ვალდებულების შეუსრულებლობა

მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დასანერგად ოპერატიულ-ტექნიკური სააგენტოს უფროსის ბრძანებით განსაზღვრული ვადის დარღვევა ან ამ კანონის მე-4 მუხლის მე-3 პუნქტით, მე-6 მუხლის პირველი, მე-9 ან მე-14 პუნქტით, 8^{2} მუხლით ან მე-10 მუხლის მე-2 ან მე-3 პუნქტით გათვალისწინებული ვალდებულების შეუსრულებლობა ანდა ელექტრონული კომუნიკაციის კომპანიის მიერ ამ კანონის მე-10 მუხლის მე-5 პუნქტის „ე“ ქვეპუნქტით გათვალისწინებული ვალდებულების შეუსრულებლობა –

გამოიწვევს „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონით დადგენილი წესით ადმინისტრაციულ-სამართლებრივი პასუხისმგებლობის დაკისრებას.

მუხლი 10^{17}. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკის მიერ ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების განსახილველად წარუდგენლობა ან დამატებითი სტანდარტებისა და მოთხოვნების დარღვევა

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკის მიერ ეროვნული ბანკისთვის ამ კანონის მე-4 მუხლის მე-5 პუნქტის შესაბამისად ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების განსახილველად წარუდგენლობა

ან იმავე მუხლის მე-6 პუნქტის ან მე-5 მუხლის მე-5 პუნქტის შესაბამისად დადგენილი დამატებითი სტანდარტებისა და მოთხოვნების ფარგლებში ვალდებულების შეუსრულებლობა –

გამოიწვევს დაჯარიმებას დარღვევის გამოვლენის მომენტისთვის ბოლო ანგარიშგების მდგომარეობით არსებული საზედამხედველო კაპიტალის 0.01%-ის, 0.05%-ის ან 0.1%-ის, მაგრამ არანაკლებ 20 000 (ოცი ათასი) ლარის ოდენობით, დარღვევის სერიოზულობიდან ან/და კომერციული ბანკის აქტივებისთვის მიყენებული ზარალიდან ან/და შესაძლო საფრთხიდან გამომდინარე.

მუხლი 10^{18}. ადმინისტრაციული სამართალდარღვევის საქმის განხილვა

1. პირველი/მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის 10^4–10^8 მუხლებით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის საქმის განხილვისა და ადმინისტრაციული სახდელის დადების უფლება აქვს:

ა) პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიმართ – ოპერატიულ-ტექნიკურ სააგენტოს;

ბ) მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიმართ – ციფრული მმართველობის სააგენტოს.

2. პირველი/მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის 10^9 ან 10^{10} მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის საქმის განხილვისა და ადმინისტრაციული სახდელის დადების უფლება აქვს:

ა) პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის

სუბიექტის მიმართ – ოპერატიულ-ტექნიკურ სააგენტოს;

ბ) მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის (გარდა კომერციული ბანკისა) მიმართ – ციფრული მმართველობის სააგენტოს;

გ) მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკის მიმართ – ეროვნულ ბანკს.

3. ამ კანონის 10^{11}–10^{15} მუხლებით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის საქმის განხილვისა და ადმინისტრაციული სახდელის დადების უფლება აქვს ოპერატიულ-ტექნიკურ სააგენტოს.

4. ამ კანონის 10^{16} მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის საქმის განხილვისა და ადმინისტრაციულ-სამართლებრივი პასუხისმგებლობის დაკისრების უფლება აქვს საქართველოს კომუნიკაციების ეროვნულ კომისიას „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონით დადგენილი წესით, ოპერატიულ-ტექნიკური სააგენტოს მიმართვის საფუძველზე.

5. ამ კანონის 10^{17} მუხლით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის საქმის განხილვისა და ადმინისტრაციულ-სამართლებრივი პასუხისმგებლობის დაკისრების უფლება აქვს ეროვნულ ბანკს.

6. ადმინისტრაციული სამართალდარღვევის ოქმს ამ მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით, მე-2 პუნქტის „ა“ ქვეპუნქტით ან მე-3 ან მე-4 პუნქტით გათვალისწინებულ შემთხვევაში ადგენს ოპერატიულ-ტექნიკური სააგენტოს უფლებამოსილი პირი, ამ მუხლის პირველი პუნქტის „ბ“

ქვეპუნქტით ან მე-2 პუნქტის „ბ“ ქვეპუნქტით გათვალისწინებულ შემთხვევაში – ციფრული მმართველობის სააგენტოს უფლებამოსილი პირი. ადმინისტრაციული სამართალდარღვევის ოქმი დგება და ადმინისტრაციული სამართალდარღვევის საქმე განიხილება საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსით დადგენილი წესით, აგრეთვე ოპერატიულ-ტექნიკური სააგენტოს/ციფრული მმართველობის სააგენტოს მიერ საკუთარი კომპეტენციის ფარგლებში გამოცემული ნორმატიული აქტით დადგენილი წესით. ამ მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტით ან მე-5 პუნქტით გათვალისწინებულ შემთხვევაში ეროვნული ბანკი ადმინისტრაციული სამართალდარღვევის საქმეს განიხილავს „საქართველოს ეროვნული ბანკის შესახებ“ საქართველოს ორგანული კანონისა და „კომერციული ბანკების საქმიანობის შესახებ“ საქართველოს კანონის შესაბამისად, ეროვნული ბანკის მიერ დადგენილი წესით.“.

მუხლი 2

1. ამ კანონის ამოქმედებიდან 6 თვის ვადაში საქართველოს მთავრობამ უზრუნველყოს შემდეგი დადგენილებების მიღება:

ა) „პირველი, მეორე და მესამე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხის დამტკიცების შესახებ“;

ბ) „კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ მონაცემების მიღებისთვის, დამუშავებისთვის, შენახვისთვის ან/და გადაცემისთვის გამოყენებული აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების მწარმოებელ ქვეყნებთან დაკავშირებული დამატებითი მოთხოვნების განსაზღვრის შესახებ“;

გ) „კომპიუტერული ინციდენტების კლასიფიცირების წესის განსაზღვრის შესახებ“.

2. ამ კანონის ამოქმედებიდან 6 თვის ვადაში საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს თავმჯდომარემ გამოსცეს შემდეგი ბრძანებები:

ა) „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“;

ბ) „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივების მართვის წესების დადგენის შესახებ“;

გ) „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისთვის მინიმალური სტანდარტების დადგენის შესახებ“;

დ) „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელური სენსორის კონფიგურირების წესების დადგენის შესახებ“;

ე) „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის დადგენის შესახებ“;

ვ) „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ“;

ზ) „საჯარო სამართლის იურიდიული პირის – ციფრული

მმართველობის სააგენტოს მიერ ადმინისტრაციული სამართალდარღვევის საქმის განხილვის წესის შესახებ“;

თ) „კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის ან/და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების უფლებამოსილების მქონე ორგანიზაციათა მიერ ავტორიზაციის გავლის წესისა და ავტორიზაციის პროცედურების დადგენის შესახებ“;

ი) „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების წესისა და პერიოდულობის დადგენის შესახებ“.

3. ამ კანონის ამოქმედებიდან 6 თვის ვადაში საქართველოს სახელმწიფო უსაფრთხოების სამსახურის მმართველობის სფეროში შემავალი საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს უფროსმა გამოსცეს შემდეგი ბრძანებები:

ა) „პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“;

ბ) „პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ინფორმაციული აქტივების მართვის წესების დადგენის შესახებ“;

გ) „პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ინფორმაციული უსაფრთხოების მენეჯერებისთვის მინიმალური სტანდარტების დადგენის შესახებ“;

დ) „პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული

სისტემის სუბიექტის ქსელური სენსორის კონფიგურირების წესების დადგენის შესახებ“;

ე) „პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის დადგენის შესახებ“;

ვ) „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს მიერ ადმინისტრაციული სამართალდარღვევის საქმის განხილვის წესის შესახებ“;

ზ) „საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების ჩატარების წესისა და პროცედურების დადგენის შესახებ“;

თ) „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ“;

ი) „კლასიფიცირებული ინფორმაციის გაცვლის სისტემაში ჩართვის წესის დადგენის შესახებ“;

კ) „პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების წესისა და პერიოდულობის დადგენის შესახებ“.

4. ამ კანონის ამოქმედებიდან 6 თვის ვადაში საქართველოს თავდაცვის მინისტრმა გამოსცეს ბრძანება „თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისთვის მინიმალური სტანდარტების დადგენის შესახებ“.

5. ამ კანონის ამოქმედებიდან 6 თვის ვადაში საქართველოს სახელმწიფო

უსაფრთხოების სამსახურის უფროსმა გამოსცეს ბრძანება „ინფორმაციული უსაფრთხოების აუდიტის ან/და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარებისთვის ავტორიზაციის მსურველი ორგანიზაციის ან/და შესაბამისი თანამშრომლის უსაფრთხოებაზე შემოწმების წესის დადგენის შესახებ“.

6. ამ კანონის ამოქმედებიდან 6 თვის ვადაში საჯარო სამართლის იურიდიულმა პირმა – საქართველოს ოპერატიულ-ტექნიკურმა სააგენტომ უზრუნველყოს კლასიფიცირებული ინფორმაციის გაცვლის სისტემის შექმნა.

7. ამ კანონის პირველი მუხლის მე-9 პუნქტით გათვალისწინებული „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის 8^2 მუხლის პირველი პუნქტით განსაზღვრული საქართველოს მთავრობის დადგენილების დარღვევად არ ჩაითვლება შემდეგი შემთხვევა:

ა) კრიტიკული ინფორმაციული სისტემის სუბიექტმა მონაცემების მიღებისთვის, დამუშავებისთვის, შენახვისთვის ან/და გადაცემისთვის გამოყენებული აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებები საქართველოს მთავრობის დადგენილების მიღებამდე მოიპოვა;

ბ) მონაცემების მიღებისთვის, დამუშავებისთვის, შენახვისთვის ან/და გადაცემისთვის გამოყენებული აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებები არის საქართველოს მთავრობის დადგენილების მიღებამდე მოპოვებული, საინფორმაციო-ტექნოლოგიური ან სატელეკომუნიკაციო სისტემის ნაწილი, ამ საშუალებების მოპოვება აუცილებელია აღნიშნული სისტემის ფუნქციონირების უზრუნველსაყოფად და მათი სხვა მწარმოებელი ქვეყნის მიერ წარმოებული ანალოგიური აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებებით

ჩანაცვლება შეუძლებელია.

მუხლი 3

1. ეს კანონი, გარდა ამ კანონის პირველი მუხლისა, ამოქმედდეს გამოქვეყნებისთანავე.

2. ამ კანონის პირველი მუხლი ამოქმედდეს 2020 წლის 30 დეკემბრიდან.

საქართველოს პრეზიდენტი სალომე ზურაბიშვილი

თბილისი,

2020 წლის ... სექტემბერი.