საქართველოს კანონის პროექტი
„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის შესახებ

მუხლი 1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში (სსმ, 19.06.2012, სარეგისტრაციო კოდი: 140000000.05.001.016807) შეტანილ იქნეს შემდეგი ცვლილება:

1. მე-2 მუხლის:

ა) „ზ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„ზ) კრიტიკული ინფორმაციული სისტემის სუბიექტი - ამ მუხლის „ზ[1]-ზ[3] ქვეპუნქტებით გათვალისწინებული ერთერთი კატეგორიის სახელმწიფო ~~ორგანო ან~~ ან ადგილობრივი თვითმმართველობის ორგანო ან დაწესებულება, ასევე იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის;“.

ბ)„ზ“ ქვეპუნქტის შემდეგ დაემატოს შემდეგი რედაქციის „ზ[1]-ზ[3]“ ქვეპუნქტები:

~~ზ[1])~~ პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი - საქართველოს მთავრობის დადგენილებით განსაზღვრული სახელმწიფო ან ადგილობრივი თვითმმართველობის ორგანო ან დაწესებულება, საჯარო სამართლის იურიდიული პირი (გარდა ~~პოლიტიკური ან რელიგიური გაერთიანებისა),~~ საჯარო სამართლის იურიდიული პირის - მონაცემთა გაცვლის სააგენტოსი, საჯარო სამართლის იურიდიული პირის - კიბერუსაფრთხოების ბიუროსი და ამ კანონის მე-10[1] მუხლის მე-4 პუნქტის შესაბამისად განსაზღვრული თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტებისა), ასევე სახელმწიფო საწარმო რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის 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]“ გათვალისწინებული ელექტრონული კომუნიკაციის კომპანია, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის 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 თავდაცვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის.“.

~~გ) „მ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:~~

~~„მ) ქსელური სენსორი – მოწყობილობა, რომელიც გამიზნულია ქსელის სეგმენტის მონიტორინგისთვის, ისეთი ქმედებების გამოსავლენად, რომლებიც მიუთითებს ინფორმაციული სისტემის წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე.“.~~

~~დ) „ო“ ქვეპუნქტის შემდეგ დაემატოს შემდეგი შინაარსის „პ“ და „ჟ“~~

გ) „ე“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„ე) კომპიუტერული ინციდენტი-ინფორმაციული უსაფრთხოების პოლიტიკის რეალური დარღვევა, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით და იწვევს ინფორმაციის უნებართვო წვდომას, გამჟღავნებას, დაზიანებას ან შეფერხებას ან ინფორმაციული რესურსის მიტაცებას.“.

დ) „მ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„მ) ქსელური სენსორი - მოწყობილობა, რომელიც გამიზნულია ქსელის სეგმენტის მონიტორინგისთვის, ისეთი ქმედებების გამოსავლენად, რომლებიც მიუთითებს ინფორმაციული სისტემის წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე.“.

ე) „ო“ ქვეპუნქტის შემდეგ დაემატოს შემდეგი შინაარსის „პ“-„რ“ 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]“ გათვალისწინებული ელექტრონული კომუნიკაციის ~~კომპანია.“.~~ კომპანია.

რ) სახელმწიფო საწარმო - სახელმწიფოს წილობრივი მონაწილეობით შექმნილი საწარმო, სადაც სახელმწიფოს წილობრივი მონაწილეობა აღემატება 50%-ს.“.

2. მე-3 მუხლის პირველი-მე-2 პუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

„1. ~~2.~~ ამ კანონის მოქმედება ვრცელდება ყველა იურიდიულ პირსა და სახელმწიფო და ადგილობრივი თვითმმართველობის ორგანოზე, რომლებიც კრიტიკული ინფორმაციული სისტემის სუბიექტები არიან. ამ კანონის მოქმედება ასევე ვრცელდება ისეთ ორგანიზაციასა და უწყებაზე, რომლებიც კრიტიკული ინფორმაციული სისტემის სუბიექტს ექვემდებარებიან ან ამ სუბიექტთან დაკავშირებული არიან დასაქმების, სტაჟირების, სახელშეკრულებო ან სხვა ურთიერთობით და რომლებიც უზრუნველყოფენ ინფორმაციული აქტივის წვდომას ასეთი ურთიერთობის ფარგლებში.

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 მხედველობაში მიიღება 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 ფუნქციონირებისათვის; ინფორმაციული სისტემის მომხმარებელთა რაოდენობა; სუბიექტის მატერიალური მდგომარეობა და სავარაუდო ხარჯების ოდენობა, რომლებიც მისთვის ამ კანონიდან გამომდინარე ვალდებულებების დაკისრებას მოჰყვება.“.

3. მე-4 მუხლის:

ა) მე-2 და მე-3 პუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

„2. ინფორმაციული უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს ინფორმაციული უსაფრთხოების მინიმალურ ~~მოთხოვნებს (კრიტიკული ინფორმაციული სისტემის სუბიექტის კრიტიკულობის გათვალისწინებით), რომლებიც განისაზღვრება ოპერატიულ-ტექნიკურ სააგენტოს და მონაცემთა გაცვლის სააგენტოს ერთობლივი ბრძანებით~~მოთხოვნებს, რომლებიც განისაზღვრება ოპერატიულ-ტექნიკურ სააგენტოს უფროსის და მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანებებით, მათი კომპეტენციის შესაბამისად, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემების სუბიექტების მიმართ - თავდაცვის მინისტრის ბრძანებით, სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO), ამერიკის სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტის (NIST) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილი სტანდარტებისა და მოთხოვნების შესაბამისად.

~~3. პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი ამ მუხლის პირველი პუნქტის თანახმად მისაღებ ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებს განსახილველად წარუდგენს ოპერატიულ-ტექნიკურ სააგენტოს. ოპერატიულ-ტექნიკურ სააგენტოს ასევე ეცნობება ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებში შეტანილი ნებისმიერი ცვლილება. ოპერატიულ-ტექნიკური სააგენტო ახორციელებს ამგვარად მოწოდებული დოკუმენტების ზოგად ანალიზს და~~

წარადგენს სახელმძღვანელო მითითებებს ან/და რეკომენდაციებს მათში აღმოჩენილი ხარვეზების გამოსასწორებლად.“.

3. პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი ამ მუხლის პირველი პუნქტის თანახმად მისაღებ ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებს განსახილველად წარუდგენს ოპერატიულ-ტექნიკურ სააგენტოს, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი - მონაცემთა გაცვლის სააგენტოს, ხოლო თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემების სუბიექტები - კიბერუსაფრთხოების ბიუროს. ოპერატიულ-ტექნიკურ სააგენტოს, მონაცემთა გაცვლის სააგენტოს ან კიბერუსაფრთხოების ბიუროს, მათი კომპეტენციის შესაბამისად, ასევე ეცნობებათ ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებში შეტანილი ნებისმიერი ცვლილება. ოპერატიულ-ტექნიკური სააგენტო,მონაცემთა გაცვლის სააგენტო ან კიბერუსაფრთხოების ბიურო ახორციელებს ამგვარად მოწოდებული დოკუმენტების ზოგად ანალიზს და წარადგენენ შესასრულებლად სავალდებულო მითითებებს ან/და რეკომენდაციებს მათში აღმოჩენილი ხარვეზების გამოსასწორებლად. ოპერატიულ-ტექნიკური სააგენტო, მონაცემთა გაცვლის სააგენტო ან კიბერუსაფრთხოების ბიურო, მათი კომპეტენციის შესაბამისად, უფლებამოსილი არიან კრიტიკული ინფორმაციული სისტემის სუბიექტიდან გამოითხოვონ ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავებასთან, დანერგვასთან, მონიტორინგსა და გაუმჯობესებასთან დაკავშირებული ნებისმიერი სხვა ინფორმაცია.“.

ბ) მე-4 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„4. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი ამ მუხლის პირველი პუნქტის თანახმად მისაღებ ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებს განსახილველად წარუდგენს მონაცემთა გაცვლის სააგენტოს. მონაცემთა გაცვლის სააგენტოს ასევე ეცნობება ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებში შეტანილი ნებისმიერი ცვლილება. მონაცემთა გაცვლის სააგენტო ახორციელებს ამგვარად მოწოდებული დოკუმენტების ზოგად ანალიზს და წარადგენს რეკომენდაციებს მათში აღმოჩენილი ხარვეზების გამოსასწორებლად.“.

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

„5. ამ მუხლის მე-3 და მე-4 პუნქტებით გათვალისწინებული დოკუმენტების გარდა, ოპერატიულ-ტექნიკურ სააგენტოსა და მონაცემთა გაცვლის სააგენტოსამ მუხლის მე-3 პუნქტით გათვალისწინებული დოკუმენტების გარდა, ოპერატიულ-ტექნიკურ სააგენტოს, მონაცემთა გაცვლის 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“

ქვეპუნქტით და მე-10[3] მუხლის მე-3 პუნქტის „ბ“ გათვალისწინებული შემთხვევისა და იმ შემთხვევისა, როდესაც კრიტიკული ინფორმაციული სისტემის სუბიექტი ნებაყოფლობით უზრუნველყოფს ინფორმაციის და ინფორმაციული აქტივის ხელმისაწვდომობას.“.

34. მე-5 მუხლის მე-4 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„4. ინფორმაციული აქტივების მართვის წესებს, კერძოდ მათი აღწერის, კლასიფიცირების, წვდომის, გაცემის (გამოქვეყნების), შეცვლის და განადგურების წესებს, ~~ერთობლივი ბრძანებით ადგენენ ოპერატიულ ტექნიკური სააგენტო და მონაცემთა გაცვლის სააგენტო,~~შესაბამისი ბრძანებებით ადგენენ ოპერატიულ-ტექნიკური სააგენტოს უფროსი, მონაცემთა გაცვლის სააგენტო თავმჯდომარე და თავდაცვის მინისტრი, მათი კომპეტენციის შესაბამისად, გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი განსაზღვრავს საჯარო ინფორმაციის ხელმისაწვდომობას.“.

45. მე-6 მუხლი ჩამოყალიბდეს შემდეგი რედაქციით:

„მუხლის 6. ინფორმაციული უსაფრთხოების აუდიტი და ინფორმაციული სისტემების ტესტირება

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია პერიოდულად ჩაატაროს ინფორმაციული უსაფრთხოების აუდიტი - ინფორმაციული უსაფრთხოების მართვის სისტემის შესაბამისობის შეფასება ინფორმაციული უსაფრთხოების მინიმალურ სტანდარტებთან, რომელიც კრიტიკული ინფორმაციული სისტემის სუბიექტის შესაბამისი კატეგორიის მიმართ დგინდება ოპერატიულ-ტექნიკური სააგენტოს უფროსის ან მონაცემთა გაცვლის სააგენტოს თავმჯდომარის შესაბამისი ბრძანებებით, ხოლო თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემების სუბიექტების მიმართ - თავდაცვის მინისტრის ბრძანებით. ინფორმაციული უსაფრთხოების აუდიტის შემდგომ დგება დასკვნა, რომლის მოთხოვნების შესრულება სავალდებულოა.

2. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების პირველად აუდიტს უსასყიდლოდ ატარებს ოპერატიულ-ტექნიკური სააგენტო. შემდგომ, პერიოდულ აუდიტს, კრიტიკული ინფორმაციული სისტემის სუბიექტის შერჩევით, ატარებს ოპერატიულ-ტექნიკური სააგენტო ან მონაცემთა გაცვლის სააგენტოს მიერ ავტორიზებული ორგანიზაცია.

3. მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების პირველად და პერიოდულ აუდიტს, კრიტიკული ინფორმაციული სისტემის სუბიექტის შერჩევით, ატარებს ოპერატიულ-ტექნიკური სააგენტო ან მონაცემთა გაცვლის სააგენტოს მიერ ავტორიზებული ორგანიზაცია.

4. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების პირველად და პერიოდულ აუდიტს, კრიტიკული ინფორმაციული სისტემის სუბიექტის შერჩევით, ატარებს მონაცემთა გაცვლის სააგენტო ან მონაცემთა გაცვლის სააგენტოს მიერ ავტორიზებული ორგანიზაცია.
5. თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემების სუბიექტების პირველად და პერიოდულ აუდიტს ახორციელებს კიბერუსაფრთხოების ბიურო, საჭიროების შემთხვევაში თავდაცვის სამინისტროს სხვა რელევანტურ სტრუქტურულ ქვედანაყოფებთან ერთად.
6. მონაცემთა გაცვლის სააგენტოს მიერ ავტორიზებული ორგანიზაციის მიერ ჩატარებული აუდიტის ან პენეტრაციის ტესტის დასკვნის ერთი ეგზემპლარი, აუდიტის ან პენეტრაციის ტესტის დასრულებისთანავე ეგზავნება ოპერატიულ-ტექნიკურ სააგენტოს ან მონაცემთა გაცვლის სააგენტოს კრიტიკული ინფორმაციული სისტემის სუბიექტის კატეგორიის შესაბამისად.
7. ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესი კრიტიკული ინფორმაციული სისტემის სუბიექტის შესაბამისი კატეგორიის მიმართ დგინდება ოპერატიულ-ტექნიკური სააგენტოსა და მონაცემთა გაცვლის სააგენტოს ნორმატიული აქტებით, ხოლო თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტების მიმართ - თავდაცვის მინისტრის ბრძანებით.
8. ოპერატიულ-ტექნიკური სააგენტოს ან მონაცემთა გაცვლის სააგენტოს მიერ ინფორმაციული უსაფრთხოების აუდიტის საფასური განისაზღვრება კრიტიკული ინფორმაციული სისტემის სუბიექტთან გაფორმებული ხელშეკრულებით.
9. კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია უზრუნველყოს ინფორმაციული სისტემის შეღწევადობის (პენეტრაციის) ტესტის განხორციელება წინასწარ დაგეგმილი და დოკუმენტირებული ამოცანის მიხედვით. პენეტრაციის ტესტის განხორციელების წესი და პერიოდულობა განისაზღვრება ოპერატიულ-ტექნიკური სააგენტოს და მონაცემთა გაცვლის სააგენტოს ბრძანებებით, მათი კომპეტენციის შესაბამისად. თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტების ინფორმაციული სისტემების პენეტრაციის ტესტის განხორციელების წესი და პერიოდულობა განისაზღვრება თავდაცვის მინისტრის ბრძანებით. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის პენეტრაციის ტესტს ახორციელებს ოპერატიულ-ტექნიკური სააგენტო. მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის პენეტრაციის ტესტს, კრიტიკული ინფორმაციული სისტემის სუბიექტის შერჩევით, ახორციელებს ოპერატიულ-ტექნიკური სააგენტო ან მონაცემთა გაცვლის სააგენტოს მიერ ავტორიზებული ორგანიზაცია. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის პენეტრაციის ტესტს, კრიტიკული ინფორმაციული სისტემის სუბიექტის შერჩევით, ახორციელებს მონაცემთა გაცვლის სააგენტო ან მონაცემთა გაცვლის სააგენტოს მიერ

ავტორიზებული ორგანიზაცია. თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტის პენეტრაციის ტესტს ატარებს კიბერუსაფრთხოების ბიურო.

10. მონაცემთა გაცვლის სააგენტო ნორმატიული აქტით ადგენს ინფორმაციული უსაფრთხოების აუდიტის და პენეტრაციის ტესტის ჩატარების უფლებამოსილების მქონე ორგანიზაციათა მიერ ავტორიზაციის გავლის წესს, ავტორიზაციის პროცედურებს და საფასურს. ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის ჩატარების ავტორიზაცია შესაძლოა გაიაროს ორგანიზაციამ, რომლის ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის განხორციელებაზე უფლებამოსილ თანამშრომელს გავლილი აქვს უსაფრთხოებაზე შემოწმება სახელმწიფო უსაფრთხოების სამსახურის უფროსის ნორმატიული აქტით დადგენილი წესით.

11. თუ ინფორმაციული უსაფრთხოების აუდიტის შედეგად გამოვლინდა ინფორმაციული უსაფრთხოების მართვის სისტემის შეუსაბამობა ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებთან, ან შეღწევადობის (პენეტრაციის) ტესტირების შედეგად აღმოჩენილ იქნა ინფორმაციული სისტემის სისუსტეები, კრიტიკული ინფორმაციული სისტემის სუბიექტი ატარებს შეუსაბამობისა და სისუსტეების ანალიზს და განსაზღვრავს სათანადო გამოსასწორებელ ღონისძიებებს, რომელთა გრაფიკსაც აუდიტის დასკვნის შედგენიდან ან შეღწევადობის ტესტირების პროცესის დასრულებიდან ერთი თვის ვადაში, შესათანხმებლად წარუდგენს ოპერატიულ-ტექნიკურ სააგენტოს ან მონაცემთა გაცვლის სააგენტოს, კრიტიკული ინფორმაციული სისტემის სუბიექტის კატეგორიის გათვალისწინებით. თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტი გამოსასწორებელი ღონისძიებების გრაფიკს წარუდგენს კიბერუსაფრთხოების ბიუროს ამ პუნქტით გათვალისწინებული წესით. ოპერატიულ-ტექნიკური სააგენტო, მონაცემთა გაცვლის სააგენტო ან კიბერუსაფრთხოების ბიურო, მათი კომპეტენციის შესაბამისად, უზრუნველყოფენ წარმოდგენილი სამოქმედო გეგმის შეფასებას, შესაბამისი რეკომენდაციების ან/და შესასრულებლად სავალდებულო მოთხოვნების შემუშავებას და შეთანხმებული სამოქმედო გეგმის შესრულების მონიტორინგს.

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

6„1. ~~პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია ინფორმაციული უსაფრთხოების დანერგვის დასრულებისთანავე უზრუნველყოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების (ინფორმაციული უსაფრთხოების პოლიტიკის) ოპერატიულ-ტექნიკური~~

სააგენტოს და მონაცემთა გაცვლის სააგენტოს ერთობლივი ბრძანებით დადგენილ ფსაფრთხოების მინიმალურ სტანდარტებთან თავსებადობის შეფასება (ინფორმაციული ფსაფრთხოების აუდიტი). პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული ფსაფრთხოების აუდიტს ფსასყიდლოდ ატარებს ოპერატიულ ტექნიკური სააგენტო. აუდიტის ჩატარების შემდგომ დგება დასკვნა, რომელიც შესაძლოა შეიცავდეს მითითებას გასატარებელი ღონისძიებებისა და მათი განხორციელების ვადების შესახებ. აუდიტის დასკვნის მოთხოვნების შესრულება სავალდებულოა.

2. მეორე ან მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობით ოპერატიულ ტექნიკური სააგენტო, მონაცემთა გაცვლის სააგენტო ან მის მიერ ავტორიზებული პირთაგან კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ შერჩეული პირი ან ორგანიზაცია ატარებს ინფორმაციული ფსაფრთხოების აუდიტს. აუდიტის ჩატარების შემდგომ დგება დასკვნა, რომლის მოთხოვნების შესრულება სავალდებულოა. მონაცემთა გაცვლის სააგენტოს ან მის მიერ ავტორიზებული პირის მიერ ჩატარებული აუდიტის დასკვნის ერთი ეგზემპლარი ეგზავნება ოპერატიულ ტექნიკურ სააგენტოს.

3. ინფორმაციული ფსაფრთხოების აუდიტის ჩატარების წესს ერთობლივი ბრძანებით ადგენენ ოპერატიულ ტექნიკური სააგენტო და მონაცემთა გაცვლის სააგენტო.

4. ოპერატიულ ტექნიკური სააგენტოს ან მონაცემთა გაცვლის სააგენტოს მიერ ინფორმაციული ფსაფრთხოების აუდიტის საფასური განისაზღვრება კრიტიკული ინფორმაციული სისტემის სუბიექტთან გაფორმებული ხელშეკრულებით.

5. მონაცემთა გაცვლის სააგენტო ნორმატიული აქტით ადგენს ინფორმაციული ფსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესს, ავტორიზაციის პროცედურებს და ავტორიზაციის საფასურს.

6. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობით ოპერატიულ ტექნიკური სააგენტო, ხოლო მეორე ან მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობით, ოპერატიულ-ტექნიკური სააგენტო ან მონაცემთა გაცვლის სააგენტო ან ოპერატიულ ტექნიკური სააგენტოს წინასწარი ნებართვით კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ შერჩეული დამოუკიდებელი, შესაბამისი კომპეტენციის მქონე პირი ან ორგანიზაცია ატარებს ინფორმაციული სისტემის შეღწევადობის (პენეტრაციის) ტესტს და ამ სისტემის მოწყვლადობის შეფასებას წინაწარ დაგეგმილი და დოკუმენტირებული ამოცანის მიხედვით.

7. თუ ამ მუხლით გათვალისწინებული აუდიტის ან ტესტირების შედეგად გამოვლინდა ინფორმაციული ფსაფრთხოების პოლიტიკის მოთხოვნებთან შეუსაბამობა, კრიტიკული ინფორმაციული სისტემის სუბიექტი ატარებს

~~შეუსაბამობის ანალიზს და განსაზღვრავს და ახორციელებს სათანადო გამოსასწორებელ ღონისძიებებს, რომელთა გრაფიკსაც წარუდგენს შესაბამისად ოპერატიულ-ტექნიკურ სააგენტოს ან მონაცემთა გაცვლის სააგენტოს.“.~~

5. მე-7 მუხლის:

ა) მე-4 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„4. ინფორმაციული უსაფრთხოების მენეჯერი ადგენს ინფორმაციული უსაფრთხოების სამოქმედო გეგმას და ამ გეგმის შესრულების შესახებ ყოველწლიურ ანგარიშს წარუდგენს ამ მუხლის მე-3 პუნქტით განსაზღვრულ (პირს) პირებს. პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მენეჯერები ამ გეგმას და მისი შესრულების ყოველწლიურ ანგარიშს წარუდგენენ ოპერატიულ-ტექნიკურ სააგენტოს, ხოლო მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტები - მონაცემთა გაცვლის ~~სააგენტოს.“.~~სააგენტოს. თავდაცვის სფეროს კრიტიკული ინფორმაციული სისტემების სუბიექტების ინფორმაციული უსაფრთხოების მენეჯერები ინფორმაციული უსაფრთხოების სამოქმედო გეგმის და ამ გეგმის შესრულების ანგარიშს წარუდგენს კიბერუსაფრთხოების ბიუროს“.

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

„5. ინფორმაციული უსაფრთხოების მენეჯერად შესაძლოა განისაზღვროს პირი, რომელსაც აქვს სახელმწიფო საიდუმლოებაზე დაშვება.“.

67. მე-8 მუხლის:

ა) სათაური ჩამოყალიბდეს შემდეგი რედაქციით:

„მუხლი 8. კომპიუტერულ ინციდენტებზე დახმარების ჯგუფები

ბ) პირველი პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„1. ამ კანონის დებულებათა აღსრულებას, კერძოდ, საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, ასევე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ სხვა, მასთან დაკავშირებულ საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებენ ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT. OTA.GOV.GE ~~და,~~ მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.DEA.GOV.GE~~.“.~~ და კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი “.

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

„3. ოპერატიულ-ტექნიკური ~~სააგენტოსა და მონაცემთა გაცვლის სააგენტოს~~ სააგენტოსა, მონაცემთა გაცვლის სააგენტოს კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფების მოვალეობებია:

ა) კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების 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 მინიმიზაციის პროცესში დახმარების გაწევა;
ზ) კომპიუტერული ინციდენტების პრევენციისკენ მიმართული ზომების კოორდინაცია და ამგვარი ზომების დანერგვაში დახმარების ~~გაწერვა;~~გაწერა;
თ) სხვა მოვალეობები, რომლებიც დაკავშირებულია ინფორმაციული უსაფრთხოების მიზნებთან და განისაზღვრება კანონით ან სხვა ნორმატიული აქტით.
4. კომპიუტერულ ინციდენტებზე დახმარების ჯგუფების კომპეტენცია, მუშაობის პროცედურები, კომპიუტერული ინციდენტების კლასიფიცირების წესები, კომპიუტერულ ინციდენტებზე რეაგირების მექანიზმები და საქმიანობის სხვა წესები განისაზღვრება შესაბამისად ოპერატიულ-ტექნიკური სააგენტოს უფროსის ~~ბრძანებით და მონაცემთა გაცვლის სააგენტოს უფროსის ბრძანებით მათი კომპეტენციის ფარგლებში.“.~~ ბრძანებით, მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანებით და თავდაცვის მინისტრის ბრძანებით მათი კომპეტენციის ფარგლებში.“.

78. ამოღებულ იქნეს მე-8 მუხლის მე-5 პუნქტი.

9. მე-8 მუხლის შემდეგ დაემატოს შემდეგი შინაარსის მე-8[1] და მე-8[2] მუხლები:

„მუხლი 8[1]. მონაცემთა გაცვლის სააგენტოს და მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის უფლებები და მოვალეობები

1. მონაცემთა გაცვლის სააგენტო, კანონმდებლობით მინიჭებული უფლებამოსილების ფარგლებში, ინფორმაციული და კიბერუსაფრთხოების სფეროში ახორციელებს შემდეგი სახის მაკოორდინირებელ საქმიანობას, კერძოდ:
ა) კოორდინაციას უწევს კიბერუსაფრთხოების ეროვნული სტრატეგიის სამოქმედო გეგმის შემუშავების პროცესს და შესაბამის პროექტს წარუდგენს ეროვნული უსაფრთხოების საბჭოს საქართველოს მთავრობის მიერ სტრატეგიისა და სამოქმედო გეგმის დასამტკიცებლად.
ბ) ინფორმაციული და კიბერუსაფრთხოების სფეროში საჯარო პოლიტიკის, მეთოდოლოგიების, სტანდარტების, სახელმძღვანელო პრინციპების, წესებისა და პროცედურების შემუშავებისა და დანერგვის მიზნით ქმნის უწყებათშორის სამუშაო ჯგუფებს და წარმართავს მათ საქმიანობას.

გ) კოორდინაციას უწევს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების საქმიანობას ფართომასშტაბიან კიბერინციდენტებზე რეაგირების პროცესში.

დ) ზედამხედველობს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემების სუბიექტების მიერ ინფორმაციული და კიბერუსაფრთხოების სამართლებრივი, სტრატეგიული და მარეგულირებელი დოკუმენტების აღსრულების პროცესს და ამზადებს შესაბამის ანგარიშებს მთავრობისთვის წარსადგენად.

ე) კოორდინაციას უწევს ეროვნულ დონეზე ინფორმაციული და კიბერუსაფრთხოების სფეროში საგანმანათლებლო და ცნობიერების ამაღლების კამპანიებისა და სფეროს სპეციალისტების შესაძლებლობების ზრდის მიზნით ერთობლივი კიბერსავარჯიშოებისა და კიბერსწავლების ღონისძიებების ჩატარების პროცესს.

ვ) ქმნის და ადმინისტრირებას უწევს კიბერინციდენტების რეპორტინგისა და მათი გაზიარების პლატფორმასა და კიბერინციდენტების რეესტრს.

ზ) საქართველოს მთავრობას წარუდგენს ანგარიშს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მიერ დადგენილი ვალდებულებების მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ შესრულების შესახებ.“.

2. ამ კანონის მე-8 მუხლის მე-3 პუნქტით გათვალისწინებული ვალდებულებების გარდა მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი ~~ოპერატიულ ტექნიკურ სააგენტოსთან კოორდინაციით~~ ახორციელებს:

ა) ინფორმაციული უსაფრთხოების საკითხებზე საზოგადოებრივ საგანმანათლებლო და ინფორმაციულ უზრუნველყოფას;

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

გ) საერთაშორისო დონეზე ინფორმაციული უსაფრთხოების საკითხებში წარმომადგენლობას;

დ) ინფორმაციული უსაფრთხოების საკითხებზე საზოგადოებრივი ცნობიერების ამაღლებას.

~~2. მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს უფლება აქვს:~~

~~ა) მოითხოვოს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივის, ინფორმაციული სისტემის ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალი საგნის წვდომა, თუ ამგვარი წვდომა აუცილებელია მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის სისტემაში მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე სათანადო რეაგირებისთვის. ინფორმაციული უსაფრთხოების მენეჯერი~~

~~მოთხოვნის გონივრულ ვადაში განხილვის შედეგად კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს დაუყოვნებლივ აცნობებს შესაბამისი წვდომის შესაძლებლობის ან შეუძლებლობის შესახებ;~~

~~ბ) მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტთან შეთანხმებით, სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტის მონაწილეობით მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელში განახორციელოს კომპიუტერული ინციდენტების იდენტიფიცირებისთვის და კვლევისთვის აუცილებელი ქსელური სენსორის (სენსორების სისტემის) კონფიგურირება და მართვა.~~

3. მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს უფლება აქვს:

ა) მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობით მიიღოს ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე წვდომა, თუ ამგვარი წვდომა აუცილებელია მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის სისტემაში მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე სათანადო რეაგირებისთვის. ინფორმაციული უსაფრთხოების მენეჯერი მოთხოვნის გონივრულ ვადაში განხილვის შედეგად კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს დაუყოვნებლივ აცნობებს წვდომაზე თანხმობის არსებობის ან არ არსებობის შესახებ.

ბ) ჰქონდეს ქსელურ სენსორზე წვდომა ამ კანონის მე-10 მუხლის მე-6 პუნქტით დადგენილი წესის შესაბამისად.

მუხლი 8[2]. ინფორმაციული უსაფრთხოების უზრუნველყოფასთან დაკავშირებული დამატებითი მოთხოვნები

1. კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ მონაცემების მიღების, დამუშავების, შენახვის და გადაცემისთვის გამოყენებული აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების ~~მწარმოებლებთან~~მწარმოებელ ქვეყნებთან დაკავშირებული მოთხოვნები დამატებით განისაზღვრება საქართველოს მთავრობის დადგენილებით.

~~2. სახელმწიფო ბიუჯეტის დაფინანსებაზე მყოფ სახელმწიფო ან ადგილობრივი თვითმმართველობის ორგანოებს ან დაწესებულებებს, კრიტიკული ინფორმაციული სისტემის სუბიექტ იურიდიულ პირებს შორის ამ კანონით გათვალისწინებული კონფიდენციალური ან შინასამსახურებრივი გამოყენების ინფორმაციის, ასევე სახელმწიფო საიდუმლოების შემცველი ინფორმაციის უსაფრთხო მიმოცვლა ხორციელდება კლასიფიცირებული ინფორმაციის მიმოცვლის სისტემის მეშვეობით, რომლის შექმნას და შემდგომ ფუნქციონირებას უზრუნველყოფს ოპერატიულ-ტექნიკური სააგენტო. ამ მიზნით სააგენტო~~

~~უფლებამოსილია შექმნას და გამოიყენოს სპეციალური ოპტიკურ ბოჭკოვანი ქსელი.“.~~

82. სახელმწიფო ბიუჯეტის დაფინანსებაზე მყოფ სახელმწიფო ან ადგილობრივი თვითმმართველობის ორგანოებს ან დაწესებულებებს, კრიტიკული ინფორმაციული სისტემის საჯარო სამართლის სუბიექტ იურიდიულ პირებს შორის ამ კანონით გათვალისწინებული კონფიდენციალური ან შინასამსახურებრივი გამოყენების ინფორმაციის, ასევე სახელმწიფო საიდუმლოების შემცველი ინფორმაციის უსაფრთხო მიმოცვლის მიზნით ოპერატიულ-ტექნიკური სააგენტო უფლებამოსილია შექმნას კლასიფიცირებული ინფორმაციის მიმოცვლის სისტემა და ამ მიზნით შექმნას და გამოიყენოს სპეციალური ოპტიკურ-ბოჭკოვანი ქსელი. სახელმწიფო ბიუჯეტის დაფინანსებაზე მყოფ სახელმწიფო ან ადგილობრივი თვითმმართველობის ორგანოები ან დაწესებულებები, კრიტიკული ინფორმაციული სისტემის საჯარო სამართლის სუბიექტი იურიდიული პირები, რომელთაც სურთ კლასიფიცირებული ინფორმაციის მიმოცვლის სისტემაში ჩართვა, წერილობით მიმართავენ ოპერატიულ-ტექნიკურ სააგენტოს ოპერატიულ-ტექნიკური სააგენტოს უფროსის ბრძანებით დადგენილი წესით.

3. ოპერატიულ-ტექნიკური სააგენტოს ხელი არ მიუწვდება ამ მუხლის მე-2 პუნქტით გათვალისწინებული კლასიფიცირებული ინფორმაციის მიმოცვლის სისტემით გადაცემული ინფორმაციის შინაარსზე.

10. მე-9 მუხლის:

ა) მეორე პუნქტის „ბ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„ბ) კომპიუტერული ინციდენტების იდენტიფიცირება, მათზე რეაგირება და პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის, ~~ხოლო მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში – მონაცემთა გაცვლის სააგენტოს~~მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში - მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის, ხოლო თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში - კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის დაუყოვნებლივი ინფორმირება;“.

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

„4. კომპიუტერული უსაფრთხოების სპეციალისტი ხელმისაწვდომი უნდა იყოს ნებისმიერ დროს, მათ შორის სამუშაო საათების შემდეგ. იგი ვალდებულია უზრუნველყოს პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფთან, ~~ხოლო მესამე კატეგორიის~~

~~კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში მონაცემთა გაცვლის სააგენტოს~~მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში - მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფთან, ხოლო თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტის შემთხვევაში - კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფთან მუდმივი კოორდინაცია კრიტიკული ინფორმაციული სისტემის სუბიექტზე მიმდინარე ან სავარაუდო კიბერშეტევის პირობებში, ასევე ამ კიბერშეტევის შედეგების აღმოფხვრის პროცესში.

~~5. თუ მიმდინარე ან სავარაუდო კიბერშეტევა განსაკუთრებულ საფრთხეს უქმნის ქვეყნის თავდაცვისუნარიანობას, ეკონომიკურ უსაფრთხოებას, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალურ ფუნქციონირებას, ოპერატიულ-ტექნიკური სააგენტო უფლებამოსილია განახორციელოს კომპიუტერული უსაფრთხოების სპეციალისტების და მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის დროებითი კოორდინაცია კიბერშეტევის თავიდან აცილების, მოგერიების ან/და მისი შედეგების აღმოფხვრის მიზნით.“.~~

5. თუ მიმდინარე კიბერშეტევა განსაკუთრებულ საფრთხეს უქმნის ქვეყნის თავდაცვისუნარიანობას, ეკონომიკურ უსაფრთხოებას, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალურ ფუნქციონირებას, ოპერატიულ-ტექნიკური სააგენტო უფლებამოსილია განახორციელოს კომპიუტერული უსაფრთხოების სპეციალისტების და მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის დროებითი კოორდინაცია კიბერშეტევის თავიდან აცილების, მოგერიების ან/და მისი შედეგების აღმოფხვრის მიზნით. საომარი მდგომარეობის დროს კიბერუსაფრთხოების უზრუნველყოფა და კიბეროპერაციების ჩატარება ხორციელდება „საომარი მდგომარეობის შესახებ“ საქართველოს კანონის შესაბამისად.“.

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

„6. კომპიუტერული უსაფრთხოების სპეციალისტად შესაძლოა განისაზღვროს პირი, რომელსაც აქვს სახელმწიფო საიდუმლოებაზე დაშვება.“.

9~~1~~1. მე-9 მუხლის შემდეგ დაემატოს შემდეგი შინაარსის 9[1] მუხლი:

„**მუხლი 9[1]**. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმება

~~1~~. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის უსაფრთხოების შემოწმების მიზნით ოპერატიულ-ტექნიკური სააგენტო უფლებამოსილია მიიღოს გადაწყვეტილება პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის ~~გეგმიური ან არაგეგმიური~~ შემოწმების შესახებ. ამ გადაწყვეტილებაში უნდა მიეთითოს

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

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

ბ) ქსელში ჩართულ პროგრამულ ან/და აპარატული უზრუნველყოფის საშუალებებს, რომლებიც გამოიყენება მონაცემების მიღების, ~~დამუშავები,~~დამუშავების, შენახვის და გადაცემისთვის;

გ) პროგრამული ან/და აპარატული საშუალებების ქსელში ჩართვის ფორმალიზებულ ან არა ფორმალიზებულ წესებს და პროცედურებს.

2. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების ჩატარების წესი და პროცედურა განისაზღვრება ოპერატიულ-ტექნიკური სააგენტოს ნორმატიული აქტით.

~~3. ამ მუხლის პირველი პუნქტის შესაბამისად საინფორმაციო-ტექნოლოგიური სისტემის 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, შეამოწმოს შესამოწმებელ საკითხთან დაკავშირებული დოკუმენტები მათი განთავსების ადგილზე, გადაიღოს ამ დოკუმენტების ასლები, მოსთხოვოს პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის წარმომადგენლებს წერილობითი ან/და ზეპირი ახსნა განმარტებები.~~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, შეამოწმოს შესამოწმებელ საკითხთან დაკავშირებული დოკუმენტები მათი განთავსების ადგილზე, გადაიღოს ამ დოკუმენტების ასლები, მოსთხოვოს პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის წარმომადგენლებს წერილობითი ან/და ზეპირი ახსნა განმარტებები. საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების დროს ოპერატიულ-ტექნიკურ სააგენტოს ხელი არ მიუწვდება ინფორმაციაზე, რომლებიც არ არის დაკავშირებული საინფორმაციო ტექნოლოგიური ინფრასტრუქტურის ფუნქციონირებასთან.

4. ამ მუხლის პირველი პუნქტის შესაბამისად შემოწმების ჩატარების უფლებამოსილების მქონე პირი დამტკიცებული ფორმის მიხედვით ადგენს შემოწმების შესახებ დასკვნას. დასკვნაში უნდა მიეთითოს: შემოწმების ჩატარების თარიღი, დრო და ადგილი; შემოწმების ჩატარების საფუძველი; შემოწმებაზე დამსწრე პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის წარმომადგენლის ვინაობა; შემოწმებული დოკუმენტების ჩამონათვალი; შემოწმებული აპარატული ან/და ქსელური ინფრასტრუქტურა და შემოწმებისთვის გამოყენებული აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებები; მიღებული ზეპირი ახსნა-განმარტებების მიმოხილვა (ახსნა-განმარტებების წერილობით მიღების შემთხვევაში დასკვნას უნდა დაერთოს შესაბამისი მასალა); დასკვნა, რომელშიც აღინიშნება რეკომენდაციები ან/და ~~სახელმძღვანელო მითითებები (მათი არსებობის შემთხვევაში); სახელმძღვანელო~~შესასრულებად სავალდებულო მითითებები (მათი არსებობის შემთხვევაში); შესასრულებლად სავალდებულო მითითებით გათვალისწინებული ღონისძიებების განხორციელების ვადა; შემოწმების ჩატარების უფლებამოსილების მქონე პირის ხელმოწერა, პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის წარმომადგენლის/წარმომადგენლების ხელმოწერა, ხოლო მის მიერ ხელმოწერაზე უარის თქმის შემთხვევაში – სულ ცოტა ორი დამსწრის ხელმოწერა.

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

6. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია:

ა) უზრუნველყოს ამ მუხლის მე-4 პუნქტით გათვალისწინებული ~~სახელმძღვანელო~~შესასრულებლად სავალდებულო მითითებების შესრულება და აღნიშნულ მითითებთან შესაბამოსობაში მოიყვანოს ამ კანონის მე-4 მუხლის შესაბამისად მიღებული დოკუმენტები;

ბ) ოპერატიულ-ტექნიკურ სააგენტოსთან წინასწარ შეათანხმოს საინფორმაციო-ტექნოლოგიურ ინფრასტრუქტურაში დაგეგმილი ცვლილებები, რომლებმაც შესაძლოა გავლენა იქონიონ ამ მუხლის მე-4 პუნქტით გათვალისწინებული ~~სახელმძღვანელო~~ შესასრულებად სავალდებულო მითითებების შესრულებაზე.“.

1~~0~~12. მე-10 მუხლი ჩამოყალიბდეს შემდეგი რედაქციით:

„მუხლი 10. კომპიუტერული ინციდენტების იდენტიფიცირება:

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი ახორციელებს კომპიუტერული ინციდენტების იდენტიფიცირებას, რაც მოიცავს თითოეული

ინციდენტის შესწავლას და აღწერას და მასზე რეაგირებას. კომპიუტერული ინციდენტების იდენტიფიცირების მიზნით კრიტიკული ინფორმაციული სისტემის სუბიექტი იყენებს ქსელური სენსორების სისტემას, რომელთა კონფიგურირების წესები განისაზღვრება საქართველოს ოპერატიულ-ტექნიკური სააგენტოსა და მონაცემთა გაცვლის სააგენტოს ~~ერთობლივი ბრძანებით.~~ ბრძანებებით მათი კომპეტენციის შესაბამისად. თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემების სუბიექტების ქსელური სენსორების კონფიგურირების წესები განისაზღვრება თავდაცვის მინისტრის ბრძანებით. ამ პუნქტით გათვალისწინებული კონფიგურირების წესები უნდა გამორიცხავდეს კომუნიკაციის შინაარობრივ მონაცემზე წვდომის შესაძლებლობას.

~~2. კომპიუტერული ინციდენტების იდენტიფიცირების შესახებ დაუყოვნებლივ ეცნობება შესაბამის კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს და, აუცილებლობის შემთხვევაში, ხორციელდება გადაუდებელი ღონისძიებები ამ ინციდენტის შესახებ ინფორმაციის შენახვისა და დაცვის მიზნით.~~

~~3. კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი შეისწავლის და აღწერს კომპიუტერულ ინციდენტებს და ახორციელებს მათზე ადეკვატურ რეაგირებას ამ კანონით გათვალისწინებული ფუნქციების შესრულებისას.~~

2. კომპიუტერული ინციდენტების იდენტიფიცირების შესახებ დაუყოვნებლივ ეცნობება შესაბამის კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს და, აუცილებლობის შემთხვევაში, ხორციელდება გადაუდებელი ღონისძიებები ამ ინციდენტის შესახებ ინფორმაციის შენახვისა და დაცვის მიზნით.

3. კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი შეისწავლის და აღწერს კომპიუტერულ ინციდენტებს და ახორციელებს მათზე ადეკვატურ რეაგირებას ამ კანონით გათვალისწინებული ფუნქციების შესრულებისას. შესწავლის შედეგად დახმარების ჯგუფი 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. ინფორმაციული სისტემის სუბიექტი ვალდებულია შესასრულებლად სავალდებულო მითითებებზე გონივრულ ვადაში მოახდინოს რეაგირება და გაატაროს შესაბამისი ღონისძიებები. გატარებული ღონისძიებების შესახებ ინფორმაციას კრიტიკული ინფორმაციული სისტემის სუბიექტი, მისი კატეგორიის გათვალისწინებით, წარუდგენს ოპერატიულ-ტექნიკური სააგენტოს ან მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს.

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

5. კომპიუტერული ინციდენტების იდენტიფიცირების ან/და მათზე რეაგირების მიზნით ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი უფლებამოსილია:

ა) ამ მუხლის მე-4 პუნქტით გათვალისწინებული ვალდებულების შესრულების მიზნით ჰქონდეს წვდომა პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელური სენსორების ~~სისტემაზე. პირველი კატეგორიის სისტემის სუბიექტი ვალდებულია უზრუნველყოს ამგვარი წვდომა და მისი შემდგომი სტაბილური ფუნქციონირება;~~სისტემაზე, გარდა იმ შემთვევისა, თუ პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელით გადაცემული/მიღებული ტრაფიკის მაიდენტიფიცირებელი მონაცემი შეიცავს საბანკო გადარიცხვების შესახებ ინფორმაციას. პირველი კატეგორიის სისტემის სუბიექტი ვალდებულია უზრუნველყოს ამგვარი წვდომა და მისი შემდგომი სტაბილური ფუნქციონირება. ქსელური სენსორების კონფიგურირება და მართვა ხორციელდება ოპერატიულ-ტექნიკური სააგენტოს და კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტის მიერ ერთობლივად;

~~ბ) ჰქონდეს წვდომა მეორე და მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების ქსელურ სენსორებზე შესაბამისი სუბიექტის თანხმობით. ამ შემთხვევაში ქსელური სენსორების კონფიგურირება და მართვა ხორციელდება ოპერატიულ-ტექნიკური სააგენტოსა და კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტის მიერ ერთობლივად;~~

~~გ) მოსთხოვოს პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტს 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 უზრუნველყოს ამგვარი წვდომა დაუყოვნებლივ, მოთხოვნისთანავე;~~

~~დ) მოსთხოვოს მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტს ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე წვდომა, თუ ამგვარი~~

~~წვდომა აუცილებელია მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე რეაგირებისთვის. ინფორმაციული უსაფრთხოების მენეჯერი მოთხოვნის გონივრულ ვადაში განხილვის შედეგად კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს დაუყოვნებლივ აცნობებს შესაბამისი წვდომის შესაძლებლობის ან შეუძლებლობის შესახებ;~~

ბ) ჰქონდეს წვდომა მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების ქსელურ სენსორებზე შესაბამისი სუბიექტის თანხმობით. ამ შემთხვევაში ქსელური სენსორების კონფიგურირება და მართვა ხორციელდება ოპერატიულ-ტექნიკური სააგენტოსა და კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტის მიერ ერთობლივად;

გ) მოსთხოვოს პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტს 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 უზრუნველყოს ამგვარი წვდომა დაუყოვნებლივ, მოთხოვნისთანავე. ამ შემთხვევაში ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე წვდომა ხორციელდება პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტის მონაწილეობით;

დ) მოსთხოვოს მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტს ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე წვდომა, თუ ამგვარი წვდომა აუცილებელია მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე რეაგირებისთვის. ინფორმაციული უსაფრთხოების მენეჯერი მოთხოვნის გონივრულ ვადაში განხილვის შედეგად კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს დაუყოვნებლივ აცნობებს წვდომაზე თანხმობის არსებობის ან არარსებობის შესახებ.; თანხმობის შემთხვევაში ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე წვდომა ხორციელდება მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტის მონაწილეობით;

ე) კომპიუტერული ინციდენტის იდენტიფიცირების შემდეგ კომპიუტერული ინციდენტის განმეორების საფრთხის თავიდან აცილების მიზნით მოსთხოვოს ელექტრონული კომუნიკაციის კომპანიას მის ინფრასტრუქტურაში მსგავსი კომპიუტერული ინციდენტების იდენტიფიცირებისა და ნეიტრალიზებისთვის

აუცილებელი ღონისძიებების განხორციელება. აღნიშნული მოთხოვნა უნდა ითვალისწინებდეს ელექტრონული კომუნიკაციის კომპანიის ტექნიკურ შესაძლებლობებს.

6. ~~კომპიუტერული ინციდენტების იდენტიფიცირების შესახებ ინფორმაციის გაზიარებისა და ქმედებათა კოორდინაციის მიზნით ოპერატიულ ტექნიკური სააგენტოს და მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფები უზრუნველყოფენ კომპიუტერული ინციდენტების გაზიარების ერთიანი პლატფორმის ჩამოყალიბებას.“.~~კომპიუტერული ინციდენტების იდენტიფიცირების ან/და მათზე რეაგირების მიზნით მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი უფლებამოსილია ჰქონდეს წვდომა მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების ქსელურ სენსორებზე შესაბამისი სუბიექტის თანხმობით. ამ შემთხვევაში ქსელური სენსორების კონფიგურირება და მართვა ხორციელდება მონაცემთა გაცვლის სააგენტოსა და კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტის მიერ ერთობლივად.

1~~1~~7. კომპიუტერული ინციდენტების იდენტიფიცირების შესახებ ინფორმაციის გაზიარებისა და ქმედებათა კოორდინაციის მიზნით ოპერატიულ-ტექნიკური სააგენტოს, მონაცემთა გაცვლის სააგენტოს და კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფები უზრუნველყოფენ კომპიუტერული ინციდენტების გაზიარების ერთიანი პლატფორმის ჩამოყალიბებას.“.

13. მე-10[1] ~~მუხლის~~მუხლის:

ა) პირველი პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„1. თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტებისათვის ინფორმაციული უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს თავდაცვის სფეროში ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს (თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტის კრიტიკულობის კლასიფიცირების გათვალისწინებით), რომლებსაც, სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO), ამერიკის 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“.

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

„3. კიბერუსაფრთხოების ბიუროს მოქმედების სფერო არ ვრცელდება ოპერატიულ-ტექნიკურ სააგენტოზე და მონაცემთა გაცვლის სააგენტოზე, რომელთა უფლებამოსილება, ფუნქციები და მოქმედების სფერო განისაზღვრება ამ კანონით, „საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონითა და „საჯარო სამართლის იურიდიული პირის - მონაცემთა გაცვლის სააგენტოს შექმნის შესახებ“ საქართველოს კანონით.

„4. თავდაცვის სფეროში 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 საქართველოს იუსტიციისა და შინაგან საქმეთა სამინისტროებთან და საქართველოს სახელმწიფო უსაფრთხოების სამსახურთან შეთანხმებით. ამ ნუსხის შედგენისას მხედველობაში მიიღება 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.“.

12. ამოღებულ იქნეს მე-10[1] მუხლის მე-7 პუნქტი.

15.ამოღებულ იქნეს მე-10[2] მუხლის მე-2 პუნქტი.

16. მე-10[3] მუხლის პირველი და მე-2 პუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

„1. თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტებზე განხორციელებული იმ კიბერშეტევის, რომელიც საფრთხეს უქმნის ადამიანის სიცოცხლესა და ჯანმრთელობას, სახელმწიფო ინტერესებსა და ქვეყნის თავდაცვისუნარიანობას, აგრეთვე ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული სხვა ინციდენტების მართვას და მასთან დაკავშირებულ იმ საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი.

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

17. მე-10[3] მუხლს დაემატოს მე-3-5 პუნქტები შემდეგი რედაქციით:

„3. თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემების სუბიექტების კომპიუტერული ინციდენტების იდენტიფიცირებისა და მათზე რეაგირების მიზნით კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი უფლებამოსილია:

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

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

4. კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი, კომპიუტერული ინციდენტების იდენტიფიცირების შემთხვევაში, ინფორმაციული აქტივის უსაფრთხოების მიზნით ახორციელებს გადაუდებელ ღონისძიებებს, რაც მოიცავს ინციდენტზე რეაგირებას, შესწავლასა და აღწერას. შესწავლის და აღწერის შემდეგ დახმარების ჯგუფი შეიმუშავებს და თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტს წარუდგენს როგორც შესასრულებლად სავალდებულოა, ასევე სარეკომენდაციო ხასიათის მითითებებს.

5. თავდაცვის სფეროში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია შესასრულებლად სავალდებულო მითითებაზე გონივრულ ვადაში არაუმეტეს 1 თვისა მოახდინოს რეაგირება და გაატაროს შესაბამისი ღონისძიებები, რის შესახებაც ინფორმაციას წარუდგენს კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს.“.

18. კანონს დაემატოს III[2] თავი შემდეგი რედაქციით:

„თავი III[2]. ადმინისტრაციული პასუხისმგებლობა ამ კანონის დარღვევისთვის

მუხლი 10[4]. ინფორმაციული უსაფრთხოების დანერგვის ვადების დარღვევა

1. პირველი ან მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ინფორმაციული უსაფრთხოების დანერგვისთვის ოპერატიულ-ტექნიკური სააგენტოს და მონაცემთა გაცვლის სააგენტოს ~~ერთობლივი~~

~~ბრძანებით~~შესაბამისი ბრძანებებით განსაზღვრული ვადების დარღვევა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 10 ათასი ლარის ოდენობით.

მუხლის 10[5]. საქართველოს მთავრობის დადგენილებით გათვალისწინებული დამატებითი მოთხოვნების შეუსრულებლობა

1. პირველი ან მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-8[2] მუხლის პირველი პუნქტით გათვალისწინებული საქართველოს მთავრობის დადგენილებით განსაზღვრული მოთხოვნების შეუსრულებლობა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 10 ათასი ლარის ოდენობით.

მუხლი 10[6]. ~~აუდიტის დასკვნით გათვალისწინებული მოთხოვნების შეუსრულებლობა~~აუდიტის ან ინფორმაციული სისტემის შეღწევადობის (პენეტრაციის) ტესტის განხორციელების ვალდებულების დარღვევა

1. პირველი ან მესამე კატეგორიის ~~კრიტიკული ინფორმაციული სისტემის~~ სუბიექტის მიერ ამ კანონის მე-6 მუხლის პირველი ~~და მეორე პუნქტებით გათვალისწინებული აუდიტის დასკვნის მოთხოვნების შეუსრულებლობა~~პუნქტით გათვალისწინებული აუდიტის ან ამ კანონის მე-6 მუხლის მე-9 პუნქტით გათვალისწინებული ინფორმაციული სისტემის შეღწევადობის (პენეტრაციის) ტესტის განხორციელების ვალდებულების დარღვევა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 10 ათასი ლარის ოდენობით.

„მუხლი 10[7]. შინასამსახურებრივი გამოყენების წესების მიუწოდებლობა ან შესასრულებლად სავალდებულო მითითებების შეუსრულებლობა

1. პირველი ან მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-4 მუხლის მე-3 პუნქტით გათვალისწინებული შინასამსახურებრივი წესების მიუწოდებლობა ან შესასრულებლად სავალდებულო მითითებების შეუსრულებლობა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 10 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 20 ათასი ლარის ოდენობით.

~~მუხლი 10[7]. საინფორმაციო ტექნოლოგიური ინფრასტრუქტურის შემოწმებისთვის ხელის შეშლა~~

~~1. პირველი კატეგორიის~~მუხლი 10[8]. სამოქმედო გეგმის წარუდგენლობა ან სამოქმედო გეგმით გათვალისწინებული შესასრულებლად სავალდებულო მითითებების შეუსრულებლობა

1. პირველი ან მესამე კატეგორიის სუბიექტის მიერ ამ კანონის მე-6 მუხლის მე-11 პუნქტით გათვალისწინებული სამოქმედო გეგმის წარუდგენლობა ან სამოქმედო გეგმით გათვალისწინებული შესასრულებლად სავალდებულო მითითებების შეუსრულებლობა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 10 ათასი ლარის ოდენობით.

მუხლი 10[9]. კომპიუტერულ ინციდენტზე რეაგირების შესახებ შესასრულებლად სავალდებულო მითითების შეუსრულებლობა

1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-10 მუხლის მე-3 პუნქტით გათვალისწინებულ შემთხვევაში

ოპერატიულ-ტექნიკური სააგენტოს მიერ გაცემული შესასრულებლად სავალდებულო მითითების შეუსრულებლობა ან გატარებული ღონისძიების შესახებ ინფორმაციის მიუწოდებლობა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 10 ათასი ლარის ოდენობით.

3. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-10 მუხლის მე-3 პუნქტით გათვალისწინებულ შემთხვევაში მონაცემთა გაცვლის სააგენტოს მიერ გაცემული შესასრულებლად სავალდებულო მითითების შეუსრულებლობა ან გატარებული ღონისძიების შესახებ ინფორმაციის მიუწოდებლობა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 10 ათასი ლარის ოდენობით.

მუხლი 10[10]. საინფორმაციო ტექნოლოგიური ინფრასტრუქტურის შემოწმებისთვის ხელის შეშლა

1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-9[1] მუხლით გათვალისწინებულ საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმებისთვის ხელის შეშლა ან/და ოპერატიულ-ტექნიკური სააგენტოს მიერ მოთხოვნილი ინფორმაციის წარმოუდგენლობა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 10 000 ლარის ოდენობით.

~~„მუხლი 10[8]. შინასამსახურებრივი გამოყენების წესების მიუწოდებლობა ან სახელმძღვანელო მითითებების შეუსრულებლობა~~

~~1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-4 ე მუხლის მე-3 ე პუნქტით გათვალისწინებული შინასამსახურებრივი წესების მიუწოდებლობა ან მე 9[1] ე მუხლით გათვალისწინებული სახელმძღვანელო მითითებების შეუსრულებლობა ან სახელმძღვანელო მითითებებით გათვალისწინებული მოთხოვნების დარღვევა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 10 000 ლარის ოდენობით.~~

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

~~გამოიწვევს დაჯარიმებას 20 ათასი ლარის ოდენობით.~~

~~„მუხლი 10[9]~~ მუხლი 10[11]. საინფორმაციო ტექნოლოგიური ინფრასტრუქტურის შემოწმების დასკვნით გათვალისწინებული შესასრულებლად სავალდებულო მითითების შეუსრულებლობა

1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-9[1] მუხლის მე-4 პუნქტით გათვალისწინებული შესასრულებლად სავალდებულო მითითების შეუსრულებლობა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 5 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 10 000 ლარის ოდენობით.

„მუხლი 10[12]. საინფორმაციო-ტექნოლოგიურ ინფრასტრუქტურაში დაგეგმილი ცვლილებების შეუთანხმებლობა

1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-9[1] მუხლის მე-6 პუნქტის „ბ“ ქვეპუნქტით გათვალისწინებული საინფორმაციო-ტექნოლოგიურ ინფრასტრუქტურაში დაგეგმილი ცვლილების წინასწარ შეთანხმების ვალდებულების დარღვევა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 10 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 20 ათასი ლარის ოდენობით.

მუხლის ~~10~~[10]10[13]. ქსელურ სენსორზე წვდომის უფლების შეზღუდვა

1. ~~პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ოპერატიულ ტექნიკური სააგენტოსთვის~~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 ან/და მისი სტაბილური ფუნქციონირების ვალდებულების შეუსრულებლობა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 10 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 20 ათასი ლარის ოდენობით.“.

მუხლის ~~10~~[11]10[14]. ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ სისტემაში შემავალ საგანზე წვდომის უფლების შეზღუდვა

1. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-10 მუხლის მე-5 პუნქტის „გ“ ქვეპუნქტით გათვალისწინებულ შემთხვევაში ოპერატიულ-ტექნიკური სააგენტოსთვის ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ სისტემაში შემავალ საგანზე წვდომის უფლების შეზღუდვა ან ამგვარი წვდომისთვის ხელის შეშლა გამოიწვევს მის გაფრთხილებას ან დაჯარიმებას 2 000 ლარის ოდენობით.

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

გამოიწვევს დაჯარიმებას 5 000 ლარის ოდენობით.

მუხლი ~~10~~[12]10[15]. მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის და ელექტრონული კომუნიკაციების კომპანიის მიერ ამ კანონით გათვალისწინებული ვალდებულებების შეუსრულებლობა

მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემების სუბიექტების მიერ ინფორმაციული უსაფრთხოების დანერგვისთვის ოპერატიულ-ტექნიკური სააგენტოს ~~და მონაცემთა გაცვლის სააგენტოს ერთობლივი ბრძანებით~~

~~განსაზღვრული ვადების დარღვევა, ამ კანონის~~ბრძანებით განსაზღვრული ვადების დარღვევა, ამ კანონის მე-4 მუხლის ~~მესამე~~მე-3 პუნქტით, მე-6 მუხლის ~~მეორე პუნქტით,~~პირველი, მე-9 ან მე-11 პუნქტებით, მე-8[2] ~~მუხლით გათვალისწინებული ვალდებულებების შეუსრულებლობა,~~მუხლით, მე-10 მუხლის მე-3 პუნქტით ასევე ელექტრონული კომუნიკაციების კომპანიის მიერ ამ კანონის მე-10-ე მუხლის მე-5 პუნქტის „ე“ ქვეპუნქტით გათვალისწინებული ვალდებულების შეუსრულებლობა გამოიწვევს ადმინისტრაციულ-სამართლებრივ პასუხისმგებლობას „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონით დადგენილი წესით.“.

„**მუხლი ~~10[13]~~10[16]**. ადმინისტრაციული სამართალდარღვევის საქმის განხილვა

1. პირველი და მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემების სუბიექტების მიერ ამ კანონის მე-10[4]-~~10[5]~~10[9] მუხლებით გათვალისწინებულ ადმინისტრაციულ სამართალდარღვევათა საქმეების განხილვისა და ადმინისტრაციული სახდელის დადების უფლება აქვთ:

ა) პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების შემთხვევაში - ოპერატიულ-ტექნიკურ სააგენტოს;

ბ) მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების შემთხვევაში - მონაცემთა გაცვლის სააგენტოს.

2. ~~მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ამ კანონის მე-10[6] მუხლით გათვალისწინებულ ადმინისტრაციულ სამართალდარღვევათა საქმეების განხილვისა და ადმინისტრაციული სახდელის დადების უფლება აქვთ:~~პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ ამ კანონის 10[4]-10[14] მუხლებით გათვალისწინებულ ადმინისტრაციულ სამართალდარღვევათა საქმეების განხილვის და ადმინისტრაციული სახდელის დადების უფლება აქვს ოპერატიულ-ტექნიკური სააგენტოს უფლებამოსილ პირებს.

~~ა) ოპერატიულ-ტექნიკურ სააგენტოს უფლებამოსილ პირებს, თუ ინფორმაციული უსაფრთხოების აუდიტი ჩატარებულია ოპერატიულ-ტექნიკური სააგენტოს მიერ;~~

~~ბ) მონაცემთა გაცვლის სააგენტოს უფლებამოსილ პირებს, თუ ინფორმაციული უსაფრთხოების აუდიტი ჩატარებულია მონაცემთა გაცვლის სააგენტოს ან ამ კანონის მე-6 მუხლის მე-5 პუნქტის შესაბამისად ავტორიზებული პირის მიერ.~~

~~3. პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ ამ კანონის 10[6]-10[11] მუხლებით გათვალისწინებულ ადმინისტრაციულ სამართალდარღვევათა საქმეების განხილვის და ადმინისტრაციული სახდელის დადების უფლება აქვს ოპერატიულ-ტექნიკური სააგენტოს უფლებამოსილ პირებს.~~

~~4. ამ მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით, მეორე პუნქტის „ა“ ქვეპუნქტით და მესამე პუნქტით გათვალისწინებულ შემთხვევებში სამართალდარღვევის ოქმს ადგენს ოპერატიულ ტექნიკური სააგენტოს უფლებამოსილი პირი, ხოლო ამ მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტით და მეორე პუნქტის „ბ“ ქვეპუნქტით გათვალისწინებულ შემთხვევაში მონაცემთა გაცვლის სააგენტოს უფლებამოსილი პირი. სამართალდარღვევის ოქმი დგება და საქმე განიხილება საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსით, ასევე მათი კომპეტენციის ფარგლებში ოპერატიულ ტექნიკური სააგენტოს და მონაცემთა გაცვლის სააგენტოს ნორმატიული აქტებით დადგენილი წესით.~~

3. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემების სუბიექტების მიერ ამ კანონის 10^{4}-10^{9} მუხლებით გათვალისწინებულ ადმინისტრაციულ სამართალდარღვევათა საქმეების განხილვის და ადმინისტრაციული სახდელის დადების უფლება აქვს მონაცემთა გაცვლის სააგენტოს უფლებამოსილ პირებს.

4. ამ მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით, გათვალისწინებულ შემთხვევებში სამართალდარღვევის ოქმს ადგენს ოპერატიულ-ტექნიკური სააგენტოს უფლებამოსილი პირი, ხოლო ამ მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტით გათვალისწინებულ შემთხვევაში - მონაცემთა გაცვლის სააგენტოს უფლებამოსილი პირი. სამართალდარღვევის ოქმი დგება და საქმე განიხილება საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსით, ასევე ოპერატიულ-ტექნიკური სააგენტოს და მონაცემთა გაცვლის სააგენტოს მიერ მათი კომპეტენციის შესაბამისად გამოცემული ნორმატიული აქტებით დადგენილი წესით.

5. მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის, ასევე ამ კანონის მე-10 მუხლის მე-5 პუნქტის „ე“ ქვეპუნქტით გათვალისწინებულ შემთხვევაში ელექტრონული კომუნიკაციების კომპანიის მიმართ ადმინისტრაციული სამართალდარღვევის საქმეების განხილვის და ადმინისტრაციული სახდელის დადების უფლება აქვს საქართველოს კომუნიკაციების ეროვნულ კომისიას „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონით დადგენილი წესით, ოპერატიულ-ტექნიკური სააგენტოს მიმართვის საფუძველზე.“.

მუხლი 2.

1. ამ კანონის ამოქმედებიდან ~~1~~6 თვის ვადაში საქართველოს მთავრობამ უზრუნველყოს:

ა) „პირველი, მეორე და მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ“ დადგენილების მიღება;

ბ) „კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ მონაცემების მიღების, დამუშავების, შენახვის ან/და გადაცემისთვის გამოყენებული აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების მწარმოებლებთან დაკავშირებული მოთხოვნების განსაზღვრის შესახებ“ დადგენილების მიღება.

2. ამ კანონის ამოქმედებიდან ~~1 თვის ვადაში ოპერატიულ-ტექნიკურმა სააგენტომ და მონაცემთა გაცვლის სააგენტომ გამოსცენ შემდეგი ერთობლივი~~6 თვის ვადაში მონაცემთა გაცვლის სააგენტომ გამოსცეს შემდეგი ნორმატიული აქტები:

~~ა) ერთობლივი ბრძანება „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესახებ“;~~

~~ბ) ერთობლივი ბრძანება „ინფორმაციული აქტივების მართვის წესის შესახებ“;~~

~~გ) ერთობლივი ბრძანება „კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისთვის მინიმალური სტანდარტების დამტკიცების შესახებ“;~~

~~დ) ერთობლივი ბრძანება „ქსელური სენსორის კონფიგურირების წესების შესახებ“;~~

~~ე) ერთობლივი ბრძანება „ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის შესახებ“.~~

~~3. ამ კანონის ამოქმედებიდან 1 თვის ვადაში ოპერატიულ-ტექნიკურმა სააგენტომ გამოსცეს შემდეგი ნორმატიული აქტები:~~

~~ა) ბრძანება „საქართველოს ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ“;~~

~~ბ) ბრძანება „საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების ჩატარების წესის განსაზღვრის შესახებ”.~~

~~4. ამ კანონის ამოქმედებიდან 5 თვის ვადაში ოპერატიულ-ტექნიკურმა სააგენტომ უზრუნველყოს კლასიფიცირებული ინფორმაციის მიმოცვლის სისტემის შექმნა.~~

~~5. ამ კანონის ამოქმედებიდან 1 თვის ვადაში მონაცემთა გაცვლის სააგენტომ გამოსცეს ბრძანება „მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ“.~~

ა) ბრძანება „ მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესახებ“;

ბ) ბრძანება „ მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივების მართვის წესის შესახებ“;

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

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

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

ვ) ბრძანება „მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ“;

ზ) ბრძანება „საჯარო სამართლის იურიდიული პირის - მონაცემთა გაცვლის სააგენტოს მიერ ადმინისტრაციულ სამართალდარღვევათა განხილვის წესის შესახებ“;

თ) ბრძანება „ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარების უფლებამოსილების მქონე ორგანიზაციათა მიერ ავტორიზაციის გავლის წესის, ავტორიზაციის პროცედურის და ავტორიზაციის საფასურის დამტკიცების შესახებ“.

3. ამ კანონის ამოქმედებიდან 6 თვის ვადაში ოპერატიულ-ტექნიკურმა სააგენტომ გამოსცეს შემდეგი ნორმატიული აქტები:

ა) ბრძანება „პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესახებ“;

ბ) ბრძანება „პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივების მართვის წესის შესახებ“;

გ) ბრძანება „პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისთვის მინიმალური სტანდარტების დამტკიცების შესახებ“;

დ) ბრძანება „პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტში ქსელური სენსორის კონფიგურირების წესების შესახებ“;

ე) ბრძანება „პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის შესახებ“;

ვ) ბრძანება „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს მიერ ადმინისტრაციულ სამართალდარღვევათა განხილვის წესის შესახებ“.

ზ) ბრძანება „საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების წესის შესახებ“;

თ) ბრძანება „ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ“;

ი) ბრძანება „კლასიფიცირებული ინფორმაციის მიმოცვლის სისტემაში ჩართვის წესის შესახებ.“.

4. ამ კანონის ამოქმედებიდან 6 თვის ვადაში ოპერატიულ-ტექნიკურმა სააგენტომ უზრუნველყოს კლასიფიცირებული ინფორმაციის მიმოცვლის სისტემის შექმნა.

მუხლი 3.

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

საქართველოს პრეზიდენტი **სალომე ზურაბიშვილი**

განმარტებითი ბარათი
საქართველოს კანონის პროექტზე
„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“

ა) ზოგადი ინფორმაცია კანონპროექტის შესახებ:

ა.ა) კანონპროექტის მიღების მიზეზი:

ა. ა. ა.) პრობლემა რომლის გადაჭრასაც მიზნად ისახავს კანონპროექტი:

სახელმწიფო მმართველობის, ასევე საზოგადოებრივი ცხოვრების ფაქტობრივად ყველა სფეროში ინფორმაციული ტექნოლოგიების დანერგვის და მასზე დამოკიდებულების ზრდის მუდმივი ტენდენციის გათვალისწინებით, განსაზღვრელ მნიშვნელობას იძენს ქვეყანაში არსებული საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის და იმ ინფორმაციული სისტემების დაცვა კომპიუტერული ინციდენტებისგან, რომელთა უსაფრთხო ფუნქციონირებას კრიტიკული მნიშვნელობა აქვს ქვეყნის თავდაცვისთვის, ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის.

აღნიშნული განსაკუთრებით მნიშვნელოვანია იმის გათვალისწინებით, რომ სწორედ მოცემული კრიტიკული ინფორმაციული სისტემები და მათში დაცული ინფორმაციული აქტივები წარმოდგენენ სხვადასხვა ქვეყნების სპეციალური სამსახურების მომეტებული ინტერესის ობიექტს. ამ ფონზე, სახელმწიფო უსაფრთხოების სამსახურს, რომელიც წარმოადგენს წამყვან უწყებას ქვეყანის უსაფრთხოების უზრუნველყოფის პროცესში, მოქმედი საკანონმდებლო რეგულაციის ფარგლებში, არ გააჩნია უფლებამოსილებები ინფორმაციული უსაფრთხოებისა და ქვეყნის კიბერ-სივრცის უსაფრთხოების უზრუნველყოფის სფეროში. ამასთან, სამსახურის მმართველობის სფეროში შედის საჯარო სამართლის იურიდიული პირი - საქართველოს ოპერატიულ-ტექნიკური სააგენტო (შემდგომში ოპერატიულ-ტექნიკური სააგენტო), რომელიც ფლობს შესაბამის მატერიალურ და ტექნიკურ ბაზას, ისევე როგორც სათანადო კვალიფიკაციის საკადრო რესურსს აღნიშნული ფუნქციის წარმატებით შესასრულებლად.

ზემოაღნიშნულის გათვალისწინებით, არსებული საკანონმდებლო რეგულაცია წარმოშობს ინფორმაციული უსაფრთხოებისა და კიბერ-უსაფრთხოების სფეროში სახელმწიფო უსაფრთხოების სამსახურის და კონკრეტულად მისი მმართველობის სფეროში შემავალი ოპერატიულ-ტექნიკური სააგენტოს კომპეტენციის შემდგომი სამართლებრივი რეგლამენტირების აუცილებლობას.

ასევე, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი არ ითვალისწინებს ადმინისტრაციულ-სამართლებრივ სანქციებს, როგორც კანონით გათვალისწინებული დებულებების აღსრულების უზრუნველყოფის საშუალებას, რაც ასევე წარმოადგენს მნიშვნელოვან ხელშემშლელ ფაქტორს ინფორმაციული

უსაფრთხოების დანერგვისა და კიბერ-უსაფრთხოების უზრუნველყოფის პროცესში.

ა. ა. ბ) არსებული პრობლემის გადასაჭრელად კანონის მიღების აუცილებლობა:
კანონპროექტის მიღება აუცილებელია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის პრაქტიკაში განხორციელების შედეგად გამოვლენილი ხარვეზების აღმოფხვრის, კერძოდ ინფორმაციული უსაფრთხოების შესახებ დებულებების აღსრულების ხარისხის ამაღლების, ადმინისტრაციულ-სამართლებრივი სანქციების შემოღების, კომპიუტერული ინციდენტების გამოვლენის, აღმოფხვრის და მათი შედეგების მინიმიზების მექანიზმების გაუმჯობესების, ასევე ინფორმაციული უსაფრთხოების და კიბერუსაფრთხოების სფეროში ოპერატიულ-ტექნიკური სააგენტოს კომპეტენციის განსაზღვრის მიზნით.

ა. ბ) კანონპროექტის მოსალოდნელი შედეგები:
კანონპროექტის მიღების შედეგად გაიზრდება ინფორმაციული უსაფრთხოების დაცვის ხარისხი კანონმდებლობით გათვალისწინებული მოთხოვნების შესრულებაზე კონტროლის გამკაცრების, ასევე აღნიშნული მოთხოვნების შეუსრულებლობისთვის ადმინისტრაციულ-სამართლებრივი სანქციების შემოღების გზით. ასევე, ოპერატიულ-ტექნიკური სააგენტოს შესაბამისი უფლებამოსილებებით აღჭურვის შედეგად გაიზრდება კომპიუტერული ინციდენტების გამოვლენის და შესაბამისად მასზე რეაგირების, მისი აღმოფხვრის და უარყოფითი შედეგების სწრაფი მინიმიზების შესაძლებლობა.

ა.გ) კანონპროექტის ძირითადი არსი:
კანონპროექტი ითვალისწინებს მოქმედი საკანონმდებლო რეგულაციების ცვლილებას რამდენიმე ძირითადი მიმართულებით.

1. კრიტიკული ინფორმაციული სისტემების სუბიექტების კატეგორიზაცია

საკანონმდებლო ცვლილებების პირველ მიმართულებას წარმოადგენს კრიტიკული ინფორმაციული სისტემების სუბიექტების კატეგორიზაცია და მათ მიმართ კონტროლის და ადმინისტრაციულ-სამართლებრივი პასუხისმგებლობის დიფერენცირებული მიდგომების გამოყენება.

ამჟამად იმ კრიტიკული ინფორმაციული სისტემის სუბიექტთა წრე, ანუ სუბიექტთა წრე, რომელზეც ვრცელდება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის დებულებები, განისაზღვრება საქართველოს მთავრობის დადგენილებით „კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხის დამტკიცების შესახებ“.

კანონპროექტით გათვალისწინებული ცვლილების შესაბამისად, კრიტიკული ინფორმაციული სისტემის სუბიექტები დაიყოფიან 3 კატეგორიად. კერძოდ:

ა) პირველი კატეგორიის სუბიექტებში მოხვდებიან ის სახელმწიფო ორგანოები, დაწესებულებები, საჯარო სამართლის იურიდიული პირები (გარდა რელიგიური და პოლიტიკური გაერთიანებებისა) და სახელმწიფო საწარმოები, რომელთა ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის;

ბ) მეორე კატეგორიის სუბიექტებში მოხვდებიან ის ელექტრონული კომუნიკაციების კომპანიები, რომელთა ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის;

გ) მესამე კატეგორიის სუბიექტებში მოხვდებიან ის კერძო სამართლის იურიდიული პირები, რომლებიც არ წარმოადგენენ ელექტრონული კომუნიკაციის კომპანიებს, თუმცა რომელთა ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის. შესაბამისად, აღნიშნული კატეგორია მოიცავს ისეთ კერძო სამართლის იურიდიულ პირებს, როგორებიც არიან მაგალითად ბანკები.

კანონით განისაზღვრება ის ზოგადი ვალდებულებები, რომლებიც საერთოა ყველა კატეგორიის კრიტიკული ინფორმაციული სისტემისთვის მუხედავად მისი კატეგორიისა. კერძოდ, ყველა კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებული იქნება:

ა) დანიშნოს ინფორმაციული უსაფრთხოების მენეჯერი და კომპიუტერული უსაფრთხოების სპეციალისტი;

ბ) უზრუნველყოს ინფორმაციული უსაფრთხოების დანერგვა კანონმდებლობით განსაზღვრულ ვადებში;

გ) ინფორმაციული უსაფრთხოების დანერგვის შემდეგ უზრუნველყოს ინფორმაციული უსაფრთხოების აუდიტის ჩატარება და ა.შ.

თუმცა, განსაზღვრავს რა აღნიშულ და სხვა საერთო, ზოგად ვალდებულებებს, კანონპროექტს, როგორც აღინიშნა, შემოაქვს ასევე დიფერენცირებული მიდგომები სხვადასხვა კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიმართ. აღნიშნული კატეგორიზაცია იძლევა კონტროლის და ადმინისტრაციულ-სამართლებრივი პასუხისმგებლობის თვალსაზრისით დიფერენცირებული მიდგომების და რეჟიმების გამოყენების საშუალებას სხვადასხვა კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებისადმი.

ყველაზე მკაცრი რეგულაციები დაუწესდებათ პირველი კატეგორიის სუბიექტებს. ამ კატეგორიის სუბიექტები ვალდებული იქნებიან:

ა) ჰქონდეს ქსელური სენსორები (მოწყობილობები, რომლებიც გამოიყენება კომპიუტერული ინციდენტების აღმოჩენისთვის) და მისცენ წვდომა ოპერატიულ-ტექნიკურ სააგენტოს აღნიშნულ ქსელურ სენსორებზე;

ბ) მოთხოვნისთანავე მისცენ წვდომა ოპერატიული ტექნიკურ სააგენტოს ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე, თუ ამგვარი წვდომა აუცილებელია მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე რეაგირებისთვის.

ასევე, მათ მიმართ სავალდებულო წესით გავრცელდება საინფორმაციო ტექნოლოგიური ინფრასტრუქტურის შემოწმების პროცედურა. საინფორმაციო ტექნოლოგიური შემოწმება შესაძლებელია ოპერატიულ-ტექნიკური სააგენტოს მიერ ჩატარდეს ნებისმიერ დროს, გეგმიური ან არაგეგმიური სახით და მისი ჩატარება არ არის დაკავშირებული პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ინფორმაციული უსაფრთხოების დანერგვასთან. შემოწმების შედეგად შემუშავებული დასკვნა შესასრულებლად სავალდებულოა აღნიშნული სუბიექტისთვის და მისი შეუსრულებლობა ან დასკვნით გათვალისწინებული მოთხოვნების დარღვევა გამოიწვევს ადმინისტრაციულ სამართლებრივ პასუხისმგებლობას. ასევე, აღნიშნული კატეგორიის სუბიექტი ვალდებული იქნება შემოწმების შედეგად შემუშავებულ სახელმძღვანელო მითითებებთან შესაბამისობაში მოიყვანოს მის მიერ დამტკიცებული ინფორმაციული უსაფრთხოების პოლიტიკები და დოკუმენტები.

მეორე კატეგორიაში, როგორც აღინიშნა, თავს მოიყრიან ელექტრონული კომუნიკაციების კომპანიები (მაგ: შპს „მაგთიკომი“, სს „სილქნეტი“ და .შ.), ხოლო მესამე კატეგორიაში ის კერძო სამართლის იურიდიული პირები, რომლებიც არ წარმოადგენენ ელექტრონული კომუნიკაციების კომპანიებს, თუმცა რომელთა ინფორმაციული სისტემების უსაფრთხოება კრიტიკულია ქვეყნის ნორმალური ფუნქციონირებისთვის. აღნიშნულ ორი კატეგორიის სუბიექტებთან მიმართებაში კანონმდებლობით გათვალისწინებული მავალდებულებელი დებულებები და ასევე მათ მიმართ ადმინისტრაციულ-სამართლებრივი სახდელების გამოყენების სამართლებრივი საფუძვლები იქნება მინიმიზებული. კერძოდ, მეორე და მესამე კატეგორიების კრიტიკული ინფორმაციული სისტემის სუბიექტების ვალდებულებები შესაძლოა წარმოდგენილ იქნეს შემდეგი სახით:

ა) აღნიშნული კატეგორიის სუბიექტები ვალდებული იქნებიან დანერგონ ინფორმაციული უსაფრთხოება ინფორმაციული უსაფრთხოების დანერგვისთვის დადგენილ ვადებში. აღნიშული ვადები განისაზღვრება საქართველოს ოპერატიულ-ტექნიკური სააგენტოს და მონაცემთა გაცვლის სააგენტოს ერთობლივი ნორმატიული აქტით. ინფორმაციული უსაფრთხოების დანერგვის შემდეგ ისინი უფლებამოსილი არიან თავად შეარჩიონ აუდიტორი ინფორმაციული უსაფრთხოების აუდიტის ჩატარების მიზნით.

ბ) ინციდენტის შემთხვევაში ისინი იღებენ გადაწყვეტილებას მისცენ თუ არა დაშვება დახმარების ჯგუფს ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე;

გ) დახმარების ჯგუფს არ აქვს პირდაპირი და სავალდებულო წვდომა აღნიშნული კატეგორიის სუბიექტების ქსელური სენსორების სისტემაზე და აღნიშნული წვდომა დასაშვებია განხორციელდეს მხოლოდ მათი თანხმობით და ნებართვით.

2. ოპერატიულ-ტექნიკური სააგენტოს უფლებამოსილებათა განსაზღვრა

კანონპროექტის მეორე ძირითად მიმართულებას წარმოადგენს ოპერატიულ-ტექნიკური სააგენტოს უფლებამოსილებების განსაზღვრა ინფორმაციული უსაფრთხოების დანერგვისა და კიბერუსაფრთხოების უზრუნველყოფის პროცესში, ამ სფეროებში ოპერატიულ-ტექნიკური სააგენტოსა და მონაცემთა გაცვლის სააგენტოს უფლებამოსილებების მკაფიო გამიჯვნა, ასევე საერთო კომპეტენციას მიკუთვნებულ საკითხთა ზუსტი წრის განსაზღვრა.

კანონპროექტის მიხედვით ერთობლივი კომპეტენციის სფეროს განეკუთვნება მაგალითად ინფორმაციული უსაფრთხოების მარეგულირებელი კანონქვემდებარე ნორმატიული აქტების დამტკიცება. კერძოდ, ოპერატიულ-ტექნიკური სააგენტოსა და მონაცემთა გაცვლის სააგენტოს ერთობლივი ბრძანებებით დამტკიცდება ინფორმაციული უსაფრთხოების მარეგულირებელი მთელი რიგი ნორმატიული აქტები, მაგალითად ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები, ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესი და ა.შ.

ინფორმაციული უსაფრთხოების სფეროში მონაცემთა გაცვლის სააგენტო უფლებამოსილი იქნება განახორციელოს:

- ინფორმაციული უსაფრთხოების საკითხებზე საგანმანათლებლო და ინფორმაციული საქმიანობა;

- შესაძლო საფრთხეების შესახებ მოსახლეობის ფართო წრის გაფრთხილება და მისთვის სათანადო ინფორმაციის მიწოდება;

- საერთაშორისო დონეზე ინფორმაციული უსაფრთხოების საკითხებში წარმომადგენლობა;

- ინფორმაციული უსაფრთხოების საკითხებზე ცნობიერების ამაღლება.

ასევე, მონაცემთა გაცვლის სააგენტო უფლებამოსილი იქნება:

- მეორე და მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემების სუბიექტების თანხმობით ჩაატაროს მათი ინფორმაციული უსაფრთხოების აუდიტი;

- გამოიყენოს ადმინისტრაციულ-სამართლებრივი სანქციები მესამე კატეგორიის სუბიექტების მიმართ მათ მიერ ინფორმაციული უსაფრთხოების დანერგვისთვის

დადგენილი ვადების დარღვევის ან აუდიტის დასკვნის შეუსრულებლობის შემთხვევაში;

- განახორციელოს კანონით გათვალისწინებული სხვა უფლებამოსილებები.

ქვეყნის კიბერუსაფრთხოების დაცვის გაძლიერების მიზნით ოპერატიულ-ტექნიკურ სააგენტოში შეიქმნება კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფი - CERT.OTA.GOV.GE. ამგვარად, კომპიუტერული უსაფრთხოების უზრუნველყოფაზე პასუხისმგებლობა განაწილდება ერთის მხრივ ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის -CERT.OTA.GOV.GE-ს და მეორეს მხრივ, მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს - CERT.DEA.GOV.GE-ს შორის. კომპეტენციათა გამიჯვნა დაეფუძნება კრიტიკული ინფორმაციული სისტემების სუბიექტების კატეგორიზაციას. კერძოდ, ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი კანონით განსაზღვრული უფლებამოსილების ფარგლებში, უზრუნველყოფს და წარმართავს კომპიუტერულ ინციდენტების აღმოჩენის, მათზე რეაგირების და შედეგების მინიმიზაციის პროცესს პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებში, ხოლო მონაცემთა გაცვლის სააგენტოს დახმარების ჯგუფი - მესამე კატეგორიის სუბიექტებში.

მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.DEA.GOV.GE უფლებამოსილი იქნება:

- მოითხოვოს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივის, ინფორმაციული სისტემის ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალი საგნის წვდომა, თუ ამგვარი წვდომა აუცილებელია მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის სისტემაში მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე სათანადო რეაგირებისთვის;

- მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტთან შეთანხმებით, სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტის მონაწილეობით მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელში განახორციელოს კომპიუტერული ინციდენტების იდენტიფიცირებისთვის და კვლევისთვის აუცილებელი ქსელური სენსორის (სენსორების სისტემის) კონფიგურირება და მართვა.

ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი CERT.OTA.GOV.GE თავის მხრივ უფლებამოსილი იქნება:

ა) განახორციელოს პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელში კომპიუტერული ინციდენტების იდენტიფიცირება და ამ მიზნით ჰქონდეს წვდომა პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელური სენსორების სისტემაზე. პირველი კატეგორიის

სისტემის სუბიექტი ვალდებულია უზრუნველყოს ამგვარი წვდომა და მისი შემდგომი სტაბილური ფუნქციონირება;

ბ) ჰქონდეს წვდომა მეორე და მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების ქსელურ სენსორებზე შესაბამისი სუბიექტის თანხმობით. ამ შემთხვევაში ქსელური სენსორების კონფიგურირება და მართვა ხორციელდება ოპერატიულ-ტექნიკური სააგენტოსა და კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტის მიერ ერთობლივად;

გ) მოსთხოვოს პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტს 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 უზრუნველყოს ამგვარი წვდომა დაუყოვნებლივ, მოთხოვნისთანავე;

დ) კომპიუტერული ინციდენტის იდენტიფიცირების შემდეგ კომპიუტერული ინციდენტის განმეორების საფრთხის თავიდან აცილების მიზნით მოსთხოვოს ელექტრონული კომუნიკაციის კომპანიას მის ინფრასტრუქტურაში მსგავსი კომპიუტერული ინციდენტების იდენტიფიცირებისა და ნეიტრალიზებისთვის აუცილებელი ღონისძიებების განხორციელება. აღნიშნული მოთხოვნა უნდა ითვალისწინებდეს ელექტრონული კომუნიკაციის კომპანიის ტექნიკურ შესაძლებლობებს.

ე) განახორციელოს კანონით გათვალისწინებული სხვა უფლებამოსილებები.

3. ადმინისტრაციულ-სამართლებრივი სანქციების შემოღება

როგორც აღინიშნა, ინფორმაციული უსაფრთხოებისა და კიბერ-უსაფრთხოების დანერგვის ერთ-ერთ მთავარ დამაბრკოლებელ გარემოებას წარმოადგენს შესაბამისი ადმინისტრაციულ-სამართლებრივი უზრუნველყოფის მექანიზმების არ არსებობა მოქმედ კანონმდებლობაში. აღნიშნულის გათვალისწინებით, კანონპროექტის ერთ-ერთ ძირითად მიმართულებას წარმოადგენს შესაბამისი ადმინისტრაციული სანქციების შემოღება ინფორმაციული უსაფრთხოების კანონმდებლობით გათვალისწინებული მოთხოვნების დარღვევისთვის.

კანონპროექტი ითვალისწინებს ადმინისტრაციულ სამართლებრივი სანქციების გამოყენების განსხვავებული რეჟიმებს კრიტიკული ინფორმაციული სისტემის სუბიექტის კატეგორიის მიხედვით. კერძოდ, ყველაზე მკაცრად კონტროლისა და აღსრულების მექანიზმები გამოყენებული იქნება პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიმართ. აღნიშნული სუბიექტები შესაძლოა დაექვემდებარონ ადმინისტრაციულ სანქციებს ინფორმაციული უსაფრთხოების დანერგვის ვადების დარღვევისთვის (მუხლის 10^4), საქართველოს მთავრობის დადგენილებით გათვალისწინებული დამატებითი

მოთხოვნების შეუსრულებლობისთვის (მუხლი 10^5), ინფორმაციული უსაფრთხოებს აუდიტის დასკვნის შეუსრულებლობისთვის (მუხლის 10^6), საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების ხელის შეშლისთვის (მუხლის 10^7), საინფორმაციო-ტექნოლოგიური შემოწმების დასკვნით გათვალისწინებული სახელმძღვანელო მითითებების შეუსრულებლობისთვის (მუხლის 10^8) და ა.შ. აღნიშნული კატეგორიის სუბიექტების მიმართ ადმინისტრაციულ-სამართლებრივი სანქციების გამოყენების შესახებ გადაწყვეტილება მიიღება ოპერატიულ-ტექნიკური სააგენტოს მიერ, ადმინისტრაციულ სამართალდარღვევათა კოდექსით დადგენილი წესით.

ადმინისტრაციულ-სამართლებრივი პასუხისმგებლობის შედარებით მსუბუქი რეჟიმი იქნება გამოყენებული მეორე და მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიმართ. კერძოდ, მათ მიმართ ადმინისტრაციულ-სამართლებრივი სახდელების გამოყენება განხორციელდება ინფორმაციული უსაფრთხოების დანერგვისთვის დადგენილი ვადების დარღვევის (მუხლი 10^4), ინფორმაციული უსაფრთხოების აუდიტის მოთხოვნების შეუსრულებლობის (მუხლი 10^6) ან საქართველოს მთავრობის დადგენილებით გათვალისწინებული დამატებითი მოთხოვნების (მუხლი 10^5) შეუსრულებლობისთვის. მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტს შესაძლოა ასევე დაეკისრება პასუხისმგებლობა შინასამსახურებრივი გამოყენების წესების ოპერატიულ-ტექნიკური სააგენტოსთვის მიუწოდებლობისთვის. აღნიშნულ შემთხვევებში მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიმართ ადმინისტრაციული სახდელის გამოყენების შესახებ გადაწყვეტილებას მიიღებს მონაცემთა გაცვლის სააგენტო (გარდა იმ შემთხვევისა, თუ მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის მოთხოვნით ინფორმაციული უსაფრთხოების აუდიტს ჩაატარებს ოპერატიულ-ტექნიკური სააგენტო), ხოლო მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემების, ანუ ელექტრონული კომუნიკაციის კომპანიების მიმართ - კომუნიკაციების მარეგულირებელი ეროვნული კომისია, „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონით დადგენილი წესით.

ა. დ) კანონპროექტის კავშირი სამთავრობო პროგრამასთან და შესაბამის სფეროში არსებულ სამოქმედო გეგმასთან, ასეთის არსებობის შემთხვევაში (საქართველოს მთავრობის მიერ ინიციირებული კანონპროექტის შემთხვევაში):

აღნიშნული ქვეპუნქტი არ გამოიყენება წარმოდგენილ კანონპროექტთან მიმართებით (კანონპროექტი არ არის ინიცირებული საქართველოს მთავრობის მიერ)

ა. ე) კანონპროექტის ძალაში შესვლის თარიღის შერჩევის პრინციპი, ხოლო კანონისთვის უკუძალის მინიჭების შემთხვევაში - აღნიშნულის თაობაზე შესაბამისი დასაბუთება;

კანონპროექტის მიღება არ ითვალისწინებს მისთვის უკუძალის მინიჭებას. კანონპროექტით წარმოდგენილი რეგულაციების გათვალისწინებით მიზანშეწონილია კანონპროექტით გათვალისწინებული მე-2 და მე-3 მუხლები, რომლებიც განსაზღვრავენ მისაღები კანონქვემდებარე აქტების ჩამონათვალს, მათი მიღების ვადას და კანონის ამოქმედებასთან დაკავშირებულ ნორმებს ძალაში შევიდეს 2020 წლის 1 იანვრიდან, გარდა კანონპროექტის პირველი მუხლისა, რომელიც მისი ნორმატიული შინაარსის გათვალისწინებით ძალაში შევა კანონის ამოქმედებიდან ერთი თვის ვადაში. (გამონაკლისია პირველი მუხლის მე-7 პუნქტით გათვალისწინებული მე-8[2] მუხლის მე-2 პუნქტი, რომლის ამოქმედებაც მიზანშეწონილია განხორციელდეს კანონის ამოქმედებიდან 5 თვის ვადაში.)

ა. ვ) კანონპროექტის დაჩქარებული წესით განხილვის მიზეზები და შესაბამისი დასაბუთება (თუ ინიციატორი ითხოვს კანონპროექტის დაჩქარებული წესით განხილვას):

დაჩქარებული წესით განხილვა არ არის მოთხოვნილი.

ბ)კანონპროექტის ფინანსური გავლენის შეფასება საშუალოვადიან პერიოდში (კანონპროექტის ამოქმედების წელი და შემდგომი 3 წელი). მასში აღინიშნება:

ბ.ა) კანონპროექტის მიღებასთან დაკავშირებით აუცილებელი ხარჯების დაფინანსების წყარო:

კანონპროექტის მიღებასთან დაკავშირებული ხარჯების დაფინანსების წყაროა სახელმწიფო ბიუჯეტი.

ბ.ბ) კანონპროექტის გავლენა სახელმწიფო ან/და მუნიციპალიტეტის ბიუჯეტის საშემოსავლო ნაწილზე:

წარმოდგენილი კანონპროექტი ითვალისწინებს საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს და საჯარო სამართლის იურიდიული პირის - მონაცემთა გაცვლის სააგენტოს უფლებამოსილებას გამოყენონ ამ კანონით გათვალისწინებული ადმინისტრაციული სახდელები იმ კრიტიკული ინფორმაციული სისტემის სუბიექტის მიმართ, რომელიც დაარღვევს ამ კანონით გათვალისწინებულ მოთხოვნებს. საშემოსავლო ნაწილზე გავლენის სიდიდე დამოკიდებული იქნება ჩადენილი ადმინისტრაციული სამართალდარღვევების რაოდენობაზე.

კანონპროექტის მიღება იქონიებს გავლენას სახელმწიფო ბიუჯეტის საშემოსავლო ნაწილზე. კერძოდ, საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოში შეიქმნება ახალი სპეციალიზებული სტრუქტურული ერთეული. (წლიურად 450 000 ლარი - 8 საშტატო ერთეულის

ხელფასი). საშემოსავლო ნაწილზე ზეგავლენა განისაზღვრება ახალდასაქმებული ადამიანური რესურსის საშემოსავლო გადასახადის სახით.

ამასთანავე, საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტო და საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო მიიღებენ შემოსავალს მათ მიერ გაწეული აუდიტორიული მომსახურებით მისაღები შემოსავლების სახით. სააგენტოების ბიუჯეტის საშემოსავლო ნაწილზე გავლენის სიდიდე დამოკიდებული იქნება მათ მიერ ჩატარებული აუდიტის რაოდენობაზე. გარდა ამისა, აღნიშნულს გავლენა ექნება სახელმწიფო ბიუჯეტის საშემოსავლო ნაწილზე ხსენებული სააგენტოების მიერ გადახდილი დღგ-ს სახით.

ბ.გ) კანონპროექტის გავლენა სახელმწიფო ან/და მუნიციპალიტეტის ბიუჯეტის ხარჯვით ნაწილზე;

2020-2023 წლების ბიუჯეტის ხარჯვითი ნაწილის ზრდას გამოიწვევს სააგენტოში ახალი სპეციალიზებული სტრუქტურული ერთეულის შექნა 8 საშტატო ერთეულით (წლიურად 450 000 ლარი - 8 საშტატო ერთეულის ხელფასი). რაც შეეხება აღნიშნული სტრუქტურული ერთეულის ტექნიკურ აღჭურვილობას (პერსონალური კომპიუტერი და ა.შ.) უზრუნველყოფილი იქნება საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს ინფრასტრუქტურაში არსებული ტექნიკური აღჭურვილობით.

ამასთანავე, პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებული იქნება ინფორმაციული უსაფრთხოების დანერგვის დასრულებისთანავე უზრუნველყოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების (ინფორმაციული უსაფრთხოების პოლიტიკის) ოპერატიულ-ტექნიკური სააგენტოს და მონაცემთა გაცვლის სააგენტოს ერთობლივი ბრძანებით დადგენილ უსაფრთხოების მინიმალურ სტანდარტებთან თავსებადობის შეფასება (ინფორმაციული უსაფრთხოების აუდიტი). პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტს უსასყიდლოდ ატარებს ოპერატიულ-ტექნიკური სააგენტო. ოპერატიულ-ტექნიკური საგენტოს ხარჯები გამოიხატება და იფარება 8 საშტატო ერთეულის დამატებით, რომელიც იქნება გამოყენებული აუდიტის მიზნებისთვის.

რაც შეეხება საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს და საჯარო სამართლის იურიდიული პირის - მონაცემთა გაცვლის სააგენტოს მიერ კანონპროექტით წარმოდგენილი ფუნქციების განხორციელებისას პროგრამულ უზრუნველყოფას, მათ მიერ აღნიშნული ფუნქციების განხორციელება დამატებით ხარჯებს არ წარმოშობს. ამგვარ ხარჯებს არ წარმოშობს ასევე, კომპიუტერული ინციდენტების იდენტიფიცირების შესახებ ინფორმაციის გაზიარებისა და ქმედებათა კოორდინაციის მიზნით ოპერატიულ-

ტექნიკური სააგენტოს და მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფების მიერ კომპიუტერული ინციდენტების გაზიარების ერთიანი პლატფორმის ჩამოყალიბება, ვინაიდან ამგვარი პლატფორმის შექმნა მოხდება არსებული ტექნიკური ინფრასტრუქტურის ბაზაზე და დამატებით ხარჯს არ გამოიწვევს.

ბ.დ) სახელმწიფოს ახალი ფინანსური ვალდებულებები, კანონპროექტის გავლენით სახელმწიფოს ან მის სისტემაში არსებული უწყების მიერ მისაღები პირდაპირი ფინანსური ვალდებულებების (საშინაო ან საგარეო ვალდებულებები) მითითებით;

კანონპროექტის მიღება სახელმწიფოს მხრიდან ახალი ფინანსური ვალდებულებების აღებას არ ითვალისწინებს.

ბ.ე) კანონპროექტის მოსალოდნელი ფინანსური შედეგები იმ პირთათვის, რომელთა მიმართაც ვრცელდება კანონპროექტის მოქმედება, იმ ფიზიკურ და იურიდიულ პირებზე გავლენის ბუნებისა და მიმართულების მითითებით, რომლებზედაც მოსალოდნელია კანონპროექტით განსაზღვრულ ქმედებებს ჰქონდეს პირდაპირი გავლენა;

კანონპროექტის მიღებას ფინანსური შედეგი ექნება იმ პირებისთვის, რომლებიც არ შეასრულებენ ინფორმაციული უსაფრთხოების შესახებ კანონმდებლობით გათვალისწინებულ მოთხოვნებს.

კანონპროექტის მიღებას ფინანსური შედეგი ექნება იმ პირებზე, რომლებიც ისარგებლებენ ოპერატიულ-ტექნიკური ან მონაცემთა გაცვლის სააგენტოების მომსახურებით ინფორმაციული უსაფრთხოების აუდიტის სფეროში და მოუწევთ შესაბამისი საფასურის გადახდა სახელშეკრულებო საწყისზე.

ბ.ვ) კანონპროექტით დადგენილი გადასახადის, მოსაკრებლის ან სხვა სახის გადასახდელის (ფულადი შენატანის) ოდენობა შესაბამის ბიუჯეტში და ოდენობის განსაზღვრის პრინციპი:

კანონპროექტი ითვალისწინებს ჯარიმების დაწესებას, რომლებიც დიფერენცირებულია დარღვევის სიმძიმის მიხედვით.

გ) კანონპროექტის მიმართება საერთაშორისო სამართლებრივ სტანდარტებთან:
გ.ა) კანონპროექტის მიმართება ევროკავშირის სამართალთან:
კანონპროექტი არ ეწინააღმდეგება ევროკავშირის სამართალს.

გ.ბ) კანონპროექტის მიმართება საერთაშორისო ორგანიზაციებში საქართველოს წევრობასთან დაკავშირებულ ვალდებულებებთან:

კანონპროექტი არ ეწინააღმდეგება საერთაშორისო ორგანიზაციებში საქართველოს წევრობასთან დაკავშირებულ ვალდებულებს.

გ.გ) კანონპროექტის მიმართება საქართველოს ორმხრივ და მრავალმხრივ ხელშეკრულებებთან და შეთანხმებებთან, აგრეთვე, ისეთი ხელშეკრულების/შეთანხმების არსებობის შემთხვევაში, რომელსაც უკავშირდება კანონპროექტის მომზადება, – მისი შესაბამისი მუხლი ან/და ნაწილი:
კანონპროექტი არ ეწინააღმდეგება საქართველოს ორმხრივ და მრავალმხრივ ხელშეკრულებებს და შეთანხმებებს. აგრეთვე, კანონპროექტის მიღება არ უკავშირდება რომელიმე ხელშეკრულებას/შეთანხმებას.

გ.დ) არსებობის შემთხვევაში, ევროკავშირის ის სამართლებრივი აქტი, რომელთან დაახლოების ვალდებულებაც გამომდინარეობს „ერთი მხრივ, საქართველოსა და, მეორე მხრივ, ევროკავშირსა და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებს შორის ასოცირების შესახებ შეთანხმებიდან“ ან ევროკავშირთან დადებული საქართველოს სხვა ორმხრივი და მრავალმხრივი ხელშეკრულებებიდან:
ასეთი არ არსებობს.

დ) კანონპროექტის მომზადების პროცესში მიღებული კონსულტაციები:
დ.ა) სახელმწიფო, არასახელმწიფო ან/და საერთაშორისო ორგანიზაცია/დაწესებულება, ექსპერტი, სამუშაო ჯგუფი, რომელმაც მონაწილეობა მიიღო კანონპროექტის შემუშავებაში, ასეთის არსებობის შემთხვევაში:
ასეთი არ არსებობს.

დ.ბ) კანონპროექტის შემუშავებაში მონაწილე ორგანიზაციის/დაწესებულების, სამუშაო ჯგუფის, ექსპერტის შეფასება კანონპროექტის მიმართ, ასეთის არსებობის შემთხვევაში:
ასეთი არ არსებობს.

დ.გ) სხვა ქვეყნების გამოცდილება კანონპროექტის მსგავსი კანონების იმპლემენტაციის სფეროში, იმ გამოცდილების მიმოხილვა, რომელიც მაგალითად იქნა გამოყენებული კანონპროექტის მომზადებისას, ასეთი მიმოხილვის მომზადების შემთხვევაში:
ასეთი არ არსებობს.

ე) კანონპროექტის ავტორი:
კანონპროექტის ავტორია საქართველოს პარლამენტის წევრი ირაკლი სესიაშვილი

ვ)კანონპროექტის ინიციატორი:

კანონპროექტის ინიციატორია საქართველოს პარლამენტის წევრი ირაკლი სესიაშვილი