საქართველოს კანონი

ინფორმაციული უსაფრთხოების შესახებ

თავი I. ზოგადი დებულებები

მუხლი 1. კანონის მიზანი

ამ კანონის მიზანია, ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, დააწესოს საჯარო და კერძო სექტორების უფლება-მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, აგრეთვე განსაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები.

მუხლი 2. ტერმინთა განმარტება

ამ კანონში გამოყენებულ ტერმინებს აქვს შემდეგი მნიშვნელობა:

ა) ინფორმაციული უსაფრთხოება – საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას;

ბ) ინფორმაციული უსაფრთხოების პოლიტიკა – ამ კანონით, საქართველოს სხვა ნორმატიული აქტებითა და საერთაშორისო შეთანხმებებით გათვალისწინებული ნორმებისა და პრინციპების, აგრეთვე პრაქტიკის ერთობლიობა, რომელიც ემსახურება ინფორმაციული უსაფრთხოების უზრუნველყოფას და შეესაბამება მისი დაცვის სფეროში დადგენილ საერთაშორისო სტანდარტებს;

გ) კიბერსივრცე – სივრცე, რომლის განმასხვავებელი ნიშანია ელექტრონული მოწყობილობებისა და ელექტრომაგნიტური სპექტრის გამოყენება ქსელით დაკავშირებული სისტემებისა და დამხმარე ფიზიკური ინფრასტრუქტურის მეშვეობით მონაცემთა შენახვისათვის, შეცვლისათვის ან გაცვლისათვის;

დ) კიბერშეტევა – ქმედება, როდესაც ელექტრონული მოწყობილობა ან/და მასთან დაკავშირებული ქსელი ან სისტემა გამოიყენება კრიტიკულ ინფორმაციულ სისტემაში შემავალი სისტემების, ქონების ან ფუნქციების მთლიანობის დარღვევის, შეფერხების ან განადგურების ან ინფორმაციის უკანონოდ მოპოვების გზით;

ე) კომპიუტერული ინციდენტი – ინფორმაციული უსაფრთხოების პოლიტიკის რეალური ან პოტენციური დარღვევა, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით და იწვევს ინფორმაციის უნებართვო წვდომას, გამჟღავნებას, დაზიანებას ან შეფერხებას ან ინფორმაციული რესურსის მიტაცებას;

ვ) კრიტიკული ინფორმაციული სისტემა – ინფორმაციული სისტემა, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის;

ზ) კრიტიკული ინფორმაციული სისტემის სუბიექტი – სახელმწიფო ორგანო ან იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის;

თ) კონფიდენციალური ინფორმაცია – ინფორმაცია, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფას, სავარაუდოდ, მოჰყვება კრიტიკული ინფორმაციული სისტემის სუბიექტის ფუნქციებისათვის მნიშვნელოვანი ზიანი და რომლის კონფიდენციალურ ინფორმაციად კლასიფიცირების მიზანია ინფორმაციული აქტივების მართვის წესების უზრუნველყოფა, გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი განსაზღვრავს საჯარო ინფორმაციის ხელმისაწვდომობას;

ი) შინასამსახურებრივი გამოყენების ინფორმაცია – ინფორმაცია, რომელიც განკუთვნილია მხოლოდ კრიტიკული ინფორმაციული სისტემის სუბიექტის თანამშრომლისათვის ან/და მასთან სახელშეკრულებო ურთიერთობის მქონე პირისათვის, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფა, სავარაუდოდ, გამოიწვევს კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ თავისი ფუნქციების შესრულების მნიშვნელოვან შეფერხებას ან ზიანს მიაყენებს სახელმწიფო ხელისუფლების ორგანოს უსაფრთხოებას, სახელმწიფო ინტერესს ან კერძო პირის საქმიან რეპუტაციას და რომლის შინასამსახურებრივი გამოყენების ინფორმაციად კლასიფიცირების მიზანია ინფორმაციული აქტივების მართვის წესების უზრუნველყოფა, გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი განსაზღვრავს საჯარო ინფორმაციის ხელმისაწვდომობას;

კ) ინფორმაციული აქტივი – ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის;

ლ) ინფორმაციული სისტემა – ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადაწყვეტილების მიღებას;

მ) ქსელური სენსორი – მოწყობილობა, რომელიც სპეციალურად გამიზნულია ქსელის სეგმენტის მონიტორინგისთვის, ისეთი ქმედებების გამოსავლენად, რომლებიც მიუთითებს ინფორმაციული სისტემის

წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე.

ნ) ციფრული მმართველობის სააგენტო – საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი;

ო) კიბერუსაფრთხოების ბიურო – საქართველოს თავდაცვის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი (შემდგომ – კიბერუსაფრთხოების ბიურო).

საქართველოს 2013 წლის 24 დეკემბრის კანონი №1829 - ვებგვერდი, 28.12.2013წ.

საქართველოს 2020 წლის 12 ივნისის კანონი №6299 – ვებგვერდი, 26.06.2020წ.

მუხლი 3. კანონის მოქმედების სფერო

1. ამ კანონის მოქმედება ვრცელდება ყველა იურიდიულ პირსა და სახელმწიფო 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 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. ამ კანონის მოქმედება არ ვრცელდება მასმედიაზე, გამომცემლობათა რედაქციებზე, სამეცნიერო, საგანმანათლებლო, რელიგიურ და საზოგადოებრივ ორგანიზაციებსა და პოლიტიკურ პარტიებზე, მიუხედავად იმისა, თუ რამდენად მნიშვნელოვანია მათი საქმიანობა ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის.

4. ნებისმიერ იურიდიულ პირსა და სახელმწიფო ხელისუფლების ორგანოს, რომელიც არ არის კრიტიკული ინფორმაციული სისტემის სუბიექტი, უფლება აქვს, ნებაყოფლობით აიღოს ამ კანონიდან გამომდინარე ვალდებულებები.

5. ამ კანონის მოქმედება არ ვრცელდება კრიტიკული ინფორმაციული სისტემის სუბიექტის წინასწარი თანხმობით ნებადართულ ქმედებაზე, რომლის მიზანია ინფორმაციული უსაფრთხოების ტესტირება.

6. ამ კანონის დებულებები გავლენას არ ახდენს საქართველოს კანონმდებლობით გათვალისწინებული იმ ნორმების მოქმედებაზე, რომლებიც არეგულირებს ინფორმაციის თავისუფლებას, პერსონალური მონაცემის დამუშავებას, სახელმწიფო, კომერციული და პირადი საიდუმლოებების დაცვას.

საქართველოს 2013 წლის 20 სექტემბრის კანონი №1250 – ვებგვერდი, 01.10.2013წ.

საქართველოს 2013 წლის 24 დეკემბრის კანონი №1829 - ვებგვერდი, 28.12.2013წ.

საქართველოს 2015 წლის 8 ივლისის კანონი №3933 - ვებგვერდი, 15.07.2015წ.

თავი II. ინფორმაციული უსაფრთხოების ორგანიზება და უზრუნველყოფა

მუხლი 4. ინფორმაციული უსაფრთხოების წესები

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია მიიღოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები, რომლებიც ემსახურება ამ კანონის დებულებათა აღსრულებას და განსაზღვრავს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკას.

2. ინფორმაციული უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს (კრიტიკული ინფორმაციული სისტემის სუბიექტის კრიტიკულობის კლასიფიცირების გათვალისწინებით). ამ მოთხოვნებს სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილი სტანდარტებისა და მოთხოვნების შესაბამისად განსაზღვრავს ციფრული მმართველობის სააგენტო.

3. კრიტიკული ინფორმაციული სისტემის სუბიექტი ამ მუხლის პირველი პუნქტის შესაბამისად მიღებულ ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებს განსახილველად წარუდგენს ციფრული მმართველობის სააგენტოს. ციფრული მმართველობის სააგენტოს ეცნობება აგრეთვე ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებში შეტანილი ნებისმიერი ცვლილება. ციფრული მმართველობის სააგენტო ახორციელებს ამგვარად მიწოდებული დოკუმენტების ზოგად ანალიზს და მათში აღმოჩენილი ხარვეზების გამოსასწორებლად წარადგენს რეკომენდაციებს.

4. ამ მუხლის მე-3 პუნქტით გათვალისწინებული დოკუმენტების გარდა, ციფრული მმართველობის სააგენტოს ხელი არ მიუწვდება კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციასა და

ინფორმაციულ აქტივზე, გარდა იმ შემთხვევისა, როდესაც კრიტიკული ინფორმაციული სისტემის სუბიექტი ნებაყოფლობით უზრუნველყოფს ციფრული მმართველობის სააგენტოსთვის ინფორმაციისა და ინფორმაციული აქტივის ხელმისაწვდომობას.
საქართველოს 2013 წლის 24 დეკემბრის კანონი №1829 - ვებგვერდი, 28.12.2013წ.
საქართველოს 2020 წლის 12 ივნისის კანონი №6299 – ვებგვერდი, 26.06.2020წ.

მუხლი 5. ინფორმაციული აქტივების მართვა

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი, ამ კანონის მე-4 მუხლის პირველი პუნქტით გათვალისწინებული შინასამსახურებრივი გამოყენების წესების შესაბამისად, ატარებს ინფორმაციული სისტემების ინვენტარიზაციას ყველა ინფორმაციული აქტივის აღრიცხვის მიზნით, რის შედეგადაც ყოველ ინფორმაციულ აქტივს მიენიჭება კრიტიკულობის შესაბამისი კლასი – კონფიდენციალური ან შინასამსახურებრივი გამოყენების. ყველა სხვა ინფორმაციული აქტივი, რომელთა კლასიფიცირება საჭირო არ არის, ღია ინფორმაციად ითვლება.

2. ინფორმაციული აქტივების აღრიცხვის შედეგად აღიწერება ყოველი ინფორმაციული აქტივის მნიშვნელობა, ფასეულობა, უსაფრთხოებისა და დაცვის არსებული დონე.

3. ინფორმაციული აქტივის შექმნის დროს კრიტიკულობის შესაბამის კლასს ადგენს აქტივის ავტორი ან/და აქტივზე პასუხისმგებელი პირი.

4. ინფორმაციული აქტივების მართვის წესები, კერძოდ, მათი აღწერის, კლასიფიცირების, ხელმისაწვდომობის, გაცემის (გამოქვეყნების), შეცვლისა და განადგურების წესები (გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი საჯარო ინფორმაციის ხელმისაწვდომობას განსაზღვრავს) დგინდება ციფრული მმართველობის სააგენტოს ნორმატიული აქტით.
საქართველოს 2020 წლის 12 ივნისის კანონი №6299 – ვებგვერდი, 26.06.2020წ.

მუხლი 6. ინფორმაციული უსაფრთხოების აუდიტი და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტი

1. ციფრული მმართველობის სააგენტო ან ციფრული მმართველობის სააგენტოს მიერ ავტორიზებულ პირთაგან კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ შერჩეული პირი ან ორგანიზაცია კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობით ატარებს ინფორმაციული უსაფრთხოების აუდიტს – ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების (ინფორმაციული უსაფრთხოების პოლიტიკის) ციფრული მმართველობის სააგენტოს მიერ დადგენილ უსაფრთხოების მინიმალურ სტანდარტებთან შესაბამისობის შეფასებას. ინფორმაციული უსაფრთხოების აუდიტის ჩატარების შემდეგ დგება დასკვნა, რომლის მოთხოვნების შესრულება სავალდებულოა.

2. ამ მუხლის პირველი პუნქტით გათვალისწინებული ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესი დგინდება ციფრული მმართველობის სააგენტოს ნორმატიული აქტით.

3. ციფრული მმართველობის სააგენტოს მიერ ჩატარებული ინფორმაციული უსაფრთხოების აუდიტის საფასური განისაზღვრება კრიტიკული ინფორმაციული სისტემის სუბიექტთან საქართველოს კანონმდებლობის შესაბამისად დადებული ხელშეკრულებით.

4. ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესი და ავტორიზაციის პროცედურები დგინდება ციფრული მმართველობის სააგენტოს ნორმატიული აქტით.

5. ციფრული მმართველობის სააგენტო ან ციფრული მმართველობის სააგენტოს წინასწარი ნებართვით – კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ შერჩეული დამოუკიდებელი, შესაბამისი კომპეტენციის მქონე პირი ან ორგანიზაცია კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობით ატარებს ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტს და ამ სისტემის მოწყვლადობის შეფასებას წინასწარ დაგეგმილი და დოკუმენტირებული ამოცანის მიხედვით.

6. თუ ამ მუხლით გათვალისწინებული ინფორმაციული უსაფრთხოების აუდიტის ან ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების შედეგად გამოვლინდა ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნებთან შეუსაბამობა, კრიტიკული ინფორმაციული სისტემის სუბიექტი ატარებს შეუსაბამობის მიზეზის ანალიზს და საჭიროების შემთხვევაში განსაზღვრავს სათანადო გამოსასწორებელ ღონისძიებებს, მათ გრაფიკს წარუდგენს ციფრული მმართველობის სააგენტოს და ახორციელებს აღნიშნულ ღონისძიებებს.
საქართველოს 2020 წლის 12 ივნისის კანონი №6299 – ვებგვერდი, 26.06.2020წ.

მუხლი 7. ინფორმაციული უსაფრთხოების მენეჯერი

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი (თანამშრომლები), რომელიც (რომლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) კრიტიკული ინფორმაციის სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მოთხოვნების შესრულებისათვის (ინფორმაციული უსაფრთხოების მენეჯერი).

2. ინფორმაციული უსაფრთხოების მენეჯერის ძირითადი მოვალეობებია:

ა) ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნების შესრულების ყოველდღიური მონიტორინგი;

ბ) ინფორმაციული აქტივებისა და მათი წვდომის აღწერა;

გ) ინფორმაციული უსაფრთხოების პოლიტიკის შინაუწყებრივი დოკუმენტაციის მომზადება;

დ) ინფორმაციული უსაფრთხოების ინციდენტების შესახებ ინფორმაციის შეგროვება და მათზე რეაგირების მონიტორინგი;

ე) ინფორმაციული უსაფრთხოების საკითხებზე ანგარიშგება და სხვა სახის ადმინისტრაციული/საორგანიზაციო საქმიანობა;

ვ) ინფორმაციული უსაფრთხოების ზოგადი და დარგობრივი ტრენინგების ორგანიზება და ჩატარება;

ზ) სხვა მოვალეობები, რომლებსაც განსაზღვრავს კრიტიკული ინფორმაციული სისტემის სუბიექტი.

3. ინფორმაციული უსაფრთხოების მენეჯერი ანგარიშვალდებულია კრიტიკული ინფორმაციული სისტემის სუბიექტის ხელმძღვანელის ან მის მიერ შესაბამისად უფლებამოსილი თანამშრომლის ან ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების უფლებამოსილების მქონე პირთა ჯგუფის (კოლეგიური ორგანოს) წინაშე. ყველა მნიშვნელოვანი გადაწყვეტილება, რომლებიც შეეხება ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელებას, მიიღება ამ პუნქტით განსაზღვრული პირის (პირების) მიერ ან მასთან (მათთან) წინასწარი შეთანხმებით.

4. ინფორმაციული უსაფრთხოების მენეჯერი ადგენს ინფორმაციული უსაფრთხოების სამოქმედო გეგმას და ამ სამოქმედო გეგმის შესრულების შესახებ ყოველწლიურ ანგარიშს წარუდგენს ამ მუხლის მე-3 პუნქტით გათვალისწინებულ პირს (პირებს) და ციფრული მმართველობის სააგენტოს.

საქართველოს 2020 წლის 12 ივნისის კანონი №6299 – ვებგვერდი, 26.06.2020წ.

თავი III. კიბერუსაფრთხოების უზრუნველყოფა

მუხლი 8. ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი

1. ამ კანონის დებულებათა აღსრულებას, კერძოდ, საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, აგრეთვე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ, მასთან დაკავშირებულ სხვა საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი (CERT.GOV.GE) (შემდგომ – დახმარების ჯგუფი).

2. კიბერუსაფრთხოების პრიორიტეტულ საფრთხეებს მიეკუთვნება:

ა) კიბერშეტევა, რომელიც საფრთხეს უქმნის ადამიანთა სიცოცხლესა და ჯანმრთელობას, სახელმწიფო ინტერესებს ან ქვეყნის თავდაცვისუნარიანობას;

ბ) კიბერშეტევა კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული სისტემების წინააღმდეგ;

გ) კიბერშეტევა, რომელიც საფრთხეს უქმნის სახელმწიფოს, ორგანიზაციის ან კერძო პირის ფინანსურ რესურსებს ან/და საკუთრების უფლებას;

დ) სხვა ნებისმიერი ქმედება, რომელიც, მისი ხასიათიდან, მიზნიდან, წყაროდან, მოცულობიდან ან რაოდენობიდან ან მისი აღკვეთისათვის საჭირო რესურსების ოდენობიდან გამომდინარე, კრიტიკული ინფორმაციული სისტემის ნორმალური ფუნქციონირებისათვის საკმარისი საფრთხის შემცველია.

3. დახმარების ჯგუფის მოვალეობებია:

ა) კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების 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 გაწევა;

თ) ინფორმაციული უსაფრთხოების საკითხებზე ცნობიერების ამაღლება, მათ შორის, კრიტიკულ ინფორმაციულ სისტემაში არსებული საფრთხეებისა და სუსტი წერტილების შესახებ ინფორმაციის მიწოდება, თუ ინფორმაციის ამგვარი ხელმისაწვდომობა ზიანს არ აყენებს ინფორმაციულ უსაფრთხოებას;

ი) შესაძლო საფრთხეების შესახებ მომხმარებელთა ფართო წრის გაფრთხილება და მისთვის სათანადო ინფორმაციის მიწოდება;

კ) ინფორმაციული უსაფრთხოების საკითხებზე საგანმანათლებლო და ინფორმაციული უზრუნველყოფა;

ლ) საერთაშორისო დონეზე ინფორმაციული უსაფრთხოების საკითხებში წარმომადგენლობა და კოორდინაცია;

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

4. დახმარების ჯგუფს უფლება აქვს, მოითხოვოს კრიტიკული ინფორმაციული სისტემის სუბიექტის

ინფორმაციული აქტივის, ინფორმაციული სისტემის ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალი საგნის წვდომა, თუ ამგვარი წვდომა აუცილებელია მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე სათანადო რეაგირებისათვის. ინფორმაციული უსაფრთხოების მენეჯერი მოთხოვნის გონივრულ ვადაში განხილვის შედეგად დახმარების ჯგუფს დაუყოვნებლივ აცნობებს შესაბამისი წვდომის შესაძლებლობის ან შეუძლებლობის შესახებ.

5. დახმარების ჯგუფის კომპეტენცია, მუშაობის პროცედურები, კომპიუტერულ ინციდენტებზე რეაგირების მექანიზმები და საქმიანობის სხვა წესები დგინდება ციფრული მმართველობის სააგენტოს ნორმატიული აქტით.

საქართველოს 2020 წლის 12 ივნისის კანონი №6299 – ვებგვერდი, 26.06.2020წ.

მუხლი 9. კომპიუტერული უსაფრთხოების სპეციალისტი

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

2. კომპიუტერული უსაფრთხოების სპეციალისტის ძირითადი მოვალეობებია:

ა) კომპიუტერული სისტემების ყოველდღიური მონიტორინგი და შეფასება;

ბ) კომპიუტერული ინციდენტების იდენტიფიცირება და მათზე რეაგირება;

გ) კომპიუტერული ინციდენტებისა და უსაფრთხოების ზომების ანალიზი და ანგარიშგება;

დ) დახმარების ჯგუფთან კოორდინაცია;

ე) სხვა მოვალეობები, რომლებსაც განსაზღვრავს კრიტიკული ინფორმაციული სისტემის სუბიექტი.

3. კომპიუტერული უსაფრთხოების სპეციალისტი ანგარიშვალდებულია კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული ტექნოლოგიების სამსახურის ხელმძღვანელის ან მის მიერ შესაბამისად უფლებამოსილი თანამშრომლის წინაშე.

4. კომპიუტერული უსაფრთხოების სპეციალისტი ხელმისაწვდომი უნდა იყოს ნებისმიერ დროს, მათ შორის, სამუშაო საათების შემდეგ. იგი ვალდებულია კრიტიკული ინფორმაციული სისტემის სუბიექტზე მიმდინარე ან სავარაუდო კიბერშეტევის და ამ კიბერშეტევის შედეგების აღმოფხვრის პროცესში უზრუნველყოს ციფრული მმართველობის სააგენტოსთან მუდმივი კოორდინაცია.

5. თუ მიმდინარე ან სავარაუდო კიბერშეტევა განსაკუთრებულ საფრთხეს უქმნის სახელმწიფოს თავდაცვისუნარიანობას, ეკონომიკურ უსაფრთხოებას, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალურ ფუნქციონირებას, ციფრული მმართველობის სააგენტო უფლებამოსილია კიბერშეტევის თავიდან აცილების, მოგერიების ან/და მისი შედეგების აღმოფხვრის მიზნით განახორციელოს კომპიუტერული უსაფრთხოების სპეციალისტების დროებითი კოორდინაცია.

საქართველოს 2020 წლის 12 ივნისის კანონი №6299 – ვებგვერდი, 26.06.2020წ.

მუხლი 10. კომპიუტერული ინციდენტის იდენტიფიცირება

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი ახორციელებს კომპიუტერული ინციდენტების იდენტიფიცირებას, რაც მოიცავს თითოეული ინციდენტის შესწავლასა და აღწერას და მასზე რეაგირებას.

2. ციფრული მმართველობის სააგენტო და კომპიუტერული უსაფრთხოების სპეციალისტი კრიტიკული ინფორმაციული სისტემის სუბიექტთან შეთანხმებით ამ სუბიექტის ქსელში ახორციელებენ კომპიუტერული ინციდენტების იდენტიფიცირებისა და კვლევისთვის აუცილებელი ქსელური სენსორის (სენსორების სისტემის) კონფიგურაციასა და მართვას. ქსელური სენსორის კონფიგურაციის წესები დგინდება ციფრული მმართველობის სააგენტოს ნორმატიული აქტით.

3. კომპიუტერული ინციდენტის იდენტიფიცირების შესახებ დაუყოვნებლივ ეცნობება დახმარების ჯგუფს და, აუცილებლობის შემთხვევაში, ხორციელდება გადაუდებელი ღონისძიებები ამ ინციდენტის შესახებ ინფორმაციის შენახვისა და დაცვის მიზნით.

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

საქართველოს 2020 წლის 12 ივნისის კანონი №6299 – ვებგვერდი, 26.06.2020წ.

თავი III[1]. კიბერუსაფრთხოების ბიურო

საქართველოს 2013 წლის 24 დეკემბრის კანონი №1829 - ვებგვერდი, 28.12.2013წ.

მუხლი 10[1]. კიბერუსაფრთხოების ბიუროს სტატუსი და ფუნქციები

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 განსაზღვრავს კიბერუსაფრთხოების ბიურო სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილი სტანდარტებისა და მოთხოვნების შესაბამისად.

2. კიბერუსაფრთხოების ბიურო იქმნება ამ კანონისა და „საჯარო სამართლის იურიდიული პირის შესახებ“

საქართველოს კანონის შესაბამისად.

3. კიბერუსაფრთხოების ბიუროს მოქმედების სფერო არ ვრცელდება ციფრული მმართველობის სააგენტოზე, რომლის უფლებამოსილებები, ფუნქციები და მოქმედების სფერო განისაზღვრება ამ კანონითა და „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს 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 იუსტიციის სამინისტრო 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 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 დებულებასა და სტრუქტურას ამტკიცებს საქართველოს თავდაცვის მინისტრი.

6. კიბერუსაფრთხოების ბიუროს ძირითადი ფუნქციაა საქართველოს კანონმდებლობით, მათ შორის, ამ კანონით, მისთვის მინიჭებულ უფლებამოსილებათა ფარგლებში საქმიანობის განხორციელება.

7. ამ კანონის მე-6 და მე-7 მუხლების, მე-9 მუხლის მე-4 პუნქტისა და მე-10 მუხლის მე-2 პუნქტის მოქმედება არ ვრცელდება კიბერუსაფრთხოების ბიუროს საქმიანობაზე.

საქართველოს 2013 წლის 24 დეკემბრის კანონი №1829 - ვებგვერდი, 28.12.2013წ.
საქართველოს 2015 წლის 8 ივლისის კანონი №3933 - ვებგვერდი, 15.07.2015წ.
საქართველოს 2020 წლის 12 ივნისის კანონი №6299 – ვებგვერდი, 26.06.2020წ.

მუხლი 10^2. კიბერუსაფრთხოების ბიუროს დირექტორი

1. კიბერუსაფრთხოების ბიუროს დირექტორს თანამდებობაზე ნიშნავს და თანამდებობიდან ათავისუფლებს საქართველოს თავდაცვის მინისტრი.

2. კიბერუსაფრთხოების ბიუროს დირექტორს ჰყავს ორი მოადგილე, მათ შორის, ერთი პირველი მოადგილე, რომელიც ასრულებს დირექტორის მოვალეობას მისი არყოფნის შემთხვევაში. დირექტორის მოადგილეებს თანამდებობაზე ნიშნავს და თანამდებობიდან ათავისუფლებს კიბერუსაფრთხოების ბიუროს დირექტორი საქართველოს თავდაცვის მინისტრთან შეთანხმებით.

3. კიბერუსაფრთხოების ბიუროს დირექტორი მოქმედებს ამ კანონითა და კიბერუსაფრთხოების ბიუროს დებულებით მისთვის მინიჭებულ უფლებამოსილებათა ფარგლებში.

4. კიბერუსაფრთხოების ბიუროს დირექტორი უფლებამოსილია საქართველოს კანონმდებლობით დადგენილი წესით თანამდებობაზე დანიშნოს და თანამდებობიდან გაათავისუფლოს კიბერუსაფრთხოების ბიუროს თანამშრომლები.

5. კიბერუსაფრთხოების ბიუროს დირექტორი გამოსცემს ნორმატიულ აქტს – ბრძანებას ამ კანონითა და საქართველოს სხვა საკანონმდებლო აქტებით განსაზღვრულ შემთხვევებსა და ფარგლებში. კიბერუსაფრთხოების სფეროში თავდაცვის პოლიტიკის მარეგულირებელ ნორმატიულ აქტებს გამოსცემს საქართველოს თავდაცვის მინისტრი.

6. კიბერუსაფრთხოების ბიუროს საშტატო განრიგსა და თანამდებობრივ სარგოებს ამტკიცებს საქართველოს თავდაცვის მინისტრი საქართველოს კანონმდებლობით დადგენილი წესით.

საქართველოს 2013 წლის 24 დეკემბრის კანონი №1829 - ვებგვერდი, 28.12.2013წ.

მუხლი 10^3. კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი

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 – CERT.MOD.GOV.GE (შემდგომ – კიბერუსაფრთხოების ბიუროს დახმარების ჯგუფი).

2. კიბერუსაფრთხოების ბიუროს დახმარების ჯგუფისათვის პრიორიტეტული საფრთხეები და ამ ჯგუფის მოვალეობები თავდაცვის სფეროში განისაზღვრება ამ კანონის მე-8 მუხლის მე-2 და მე-3 პუნქტებით.

საქართველოს 2013 წლის 24 დეკემბრის კანონი №1829 - ვებგვერდი, 28.12.2013წ.

თავი IV. გარდამავალი და დასკვნითი დებულებები

მუხლი 11. გარდამავალი დებულებები

1. ამ კანონის ამოქმედებიდან 6 თვის ვადაში საქართველოს პრეზიდენტმა გამოსცეს ბრძანებულება „კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ“.

2. ამ კანონის ამოქმედებიდან 6 თვის ვადაში მონაცემთა გაცვლის სააგენტომ გამოსცეს შემდეგი ნორმატიული აქტები:

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

ბ) ბრძანება „კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისათვის მინიმალური სტანდარტების დამტკიცების შესახებ“;

გ) ბრძანება „ქსელური სენსორის კონფიგურაციის წესების შესახებ“;

დ) ბრძანება „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესახებ“;

ე) ბრძანება „ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესის, ავტორიზაციის პროცედურებისა და ავტორიზაციის საფასურის შესახებ“;

ვ) ბრძანება „ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის შესახებ“;

ზ) ბრძანება „ინფორმაციული აქტივების მართვის წესების შესახებ“.

3. საქართველოს მთავრობამ 2014 წლის 1 აპრილამდე უზრუნველყოს „კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ“ დადგენილების მიღება.

4. ამ მუხლის მე-3 პუნქტით გათვალისწინებული დადგენილების მიღებამდე იურიდიულ ძალას ინარჩუნებს საქართველოს პრეზიდენტის 2013 წლის 11 მარტის №157 ბრძანებულება „კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ“.

5. საქართველოს თავდაცვის სამინისტრომ 2014 წლის 1 აპრილამდე უზრუნველყოს კიბერუსაფრთხოების ბიუროს შექმნის მიზნით საქართველოს კანონმდებლობით განსაზღვრული შესაბამისი ღონისძიებების განხორციელება.

6. საქართველოს თავდაცვის მინისტრმა 2014 წლის 1 აპრილამდე გამოსცეს შემდეგი ნორმატიული აქტები:

ა) ბრძანება „საჯარო სამართლის იურიდიული პირის – კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ“;

ბ) ბრძანება „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესახებ“;

გ) ბრძანება „ინფორმაციული აქტივების მართვის წესების შესახებ“.

საქართველოს 2013 წლის 20 სექტემბრის კანონი №1250 – ვებგვერდი, 01.10.2013წ.
საქართველოს 2013 წლის 24 დეკემბრის კანონი №1829 - ვებგვერდი, 28.12.2013წ.

მუხლი 12. დასკვნითი დებულება

ეს კანონი ამოქმედდეს 2012 წლის 1 ივლისიდან.

საქართველოს პრეზიდენტი მ . სააკაშვილი
თბილისი,
2012 წლის 5 ივნისი.
№6391- Iს