საქართველოს კანონი

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე

მუხლი 1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში (საქართველოს საკანონმდებლო მაცნე (www.matsne.gov.ge), 19.06.2012, სარეგისტრაციო კოდი: 140000000.05.001.016807) შეტანილ იქნეს შემდეგი ცვლილება:
1. მე-2 მუხლის „ნ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

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

2. მე-4 მუხლის მე-2–მე-4 პუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

„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.“.

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

„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.“.

4. მე-6 მუხლი ჩამოყალიბდეს შემდეგი რედაქციით:

„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.“.

5. მე-7 მუხლის მე-4 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

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

6. მე-8 მუხლის:

ა) სათაური ჩამოყალიბდეს შემდეგი რედაქციით:

„ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი“;

ბ) პირველი პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„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).“;

გ) მე-5 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

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

7. მე-9 მუხლის მე-4 და მე-5 პუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

„4. კომპიუტერული უსაფრთხოების სპეციალისტი ხელმისაწვდომი უნდა იყოს ნებისმიერ დროს, მათ შორის, სამუშაო საათების შემდეგ. იგი ვალდებულია კრიტიკული ინფორმაციული სისტემის სუბიექტზე მიმდინარე ან სავარაუდო კიბერშეტევის და 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.“.

8. მე-10 მუხლის მე-2 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„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.“.

9. 10^1 მუხლის მე-3 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„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.“.

მუხლი 2. ეს კანონი ამოქმედდეს გამოქვეყნებიდან მე-15 დღეს.

საქართველოს პრეზიდენტი **სალომე ზურაბიშვილი**

თბილისი,

12 ივნისი 2020 წ.

N6299-IIს