ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №5

2021 წლის 14 დეკემბერი

ქ. თბილისი

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის დადგენის შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-7 პუნქტის, „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტის, „ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონის 25-ე მუხლისა და „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ 2021 წლის 10 ივნისის №632-IVმს-Xმპ საქართველოს კანონის მე-2 მუხლის მე-2 პუნქტის „ე“ ქვეპუნქტის შესაბამისად, **ვბრძანებ:**

1. დამტკიცდეს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის ჩატარების თანდართული წესი.
2. ძალადაკარგულად გამოცხადდეს „ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის დამტკიცების შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2020 წლის 16 ოქტომბრის №6 ბრძანება.
3. ეს ბრძანება ამოქმედდეს 2021 წლის 30 დეკემბრიდან.

სსიპ ციფრული მმართველობის
სააგენტოს თავმჯდომარე — დავით ნადირაშვილი

ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესი

მუხლი 1. ინფორმაციული უსაფრთხოების აუდიტის მიზანი, გავრცელების სფერო

1. ინფორმაციული უსაფრთხოების აუდიტის მიზანია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით (შემდგომ – კანონი) განსაზღვრული მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის (შემდგომ – სუბიექტი) ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების – საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს (შემდგომ – სააგენტო) მიერ დადგენილ ინფორმაციული უსაფრთხოების მინიმალურ სტანდარტებთან თავსებადობის შეფასება პირველადი და პერიოდული აუდიტის (შემდგომ – აუდიტის) საშუალებით.

2. სუბიექტი ვალდებულია ჩაატაროს ინფორმაციული უსაფრთხოების აუდიტი ინფორმაციული უსაფრთხოების მართვის სისტემის (შემდგომ – იუმს) გავრცელების სფეროში შემავალ ყველა კრიტიკულ ინფორმაციულ სისტემაზე. იუმს-ის გავრცელების სფეროში შემავალი კრიტიკული ინფორმაციული სისტემები განისაზღვრება „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანების შესაბამისად.

3. ამ წესში გამოყენებულ ტერმინებს აქვს კანონით განსაზღვრული მნიშვნელობა.

მუხლი 2. აუდიტის ჩატარების უფლებამოსილების მქონე პირები

1. სუბიექტის ინფორმაციული უსაფრთხოების პირველად აუდიტსა და პერიოდულ აუდიტს ამ სუბიექტის შერჩევით ატარებს სააგენტო ან მის მიერ ავტორიზებული ორგანიზაცია.

2. სააგენტოს მიერ ამ მუხლის პირველ პუნქტში მითითებული ავტორიზაცია გაიცემა „კრიტიკული

ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების უფლებამოსილების მქონე ორგანიზაციათა მიერ ავტორიზაციის გავლის წესისა და ავტორიზაციის პროცედურების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანების შესაბამისად.

3. სააგენტოს მიერ ჩატარებული აუდიტის საფასური განისაზღვრება „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს მიერ მომსახურების გაწევის საფასურების განაკვეთების, საფასურების გადახდის, მათი გადახდისგან გათავისუფლებისა და გადახდილი საფასურების დაბრუნების წესის დამტკიცების შესახებ“ საქართველოს მთავრობის 2020 წლის 13 ივლისის №438 დადგენილებით გათვალისწინებულ ფარგლებში, სუბიექტსა და სააგენტოს ან მის მიერ ავტორიზებულ ორგანიზაციას შორის გაფორმებული ხელშეკრულებით.

4. ამ წესის მიზნებისთვის პირველადი აუდიტი გულისხმობს ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დანერგვის შემდეგ, სააგენტოს ან ავტორიზებული ორგანიზაციის მიერ ინფორმაციული უსაფრთხოების აუდიტის ჩატარებას, ხოლო პერიოდული აუდიტი – პირველადი აუდიტის ჩატარების შემდეგ, სააგენტოს ან ავტორიზებული ორგანიზაციის მიერ ყოველწლიურად ინფორმაციული უსაფრთხოების აუდიტის ჩატარებას.

მუხლი 3. აუდიტის ჩატარების პრინციპები

1. ინფორმაციული უსაფრთხოების პირველადი აუდიტი უნდა ჩატარდეს იუმს-ის დანერგვის დასრულების შემდეგ, 1 წლის ვადაში. სუბიექტი ვალდებულია, ყოველ მომდევნო წელს ჩაატაროს პერიოდული აუდიტი. პირველადი და პერიოდული აუდიტის ჩატარების გადავადება შესაძლებელია, მხოლოდ მნიშვნელოვანი არგუმენტების არსებობის შემთხვევაში, 6 თვით, სააგენტოს წერილობითი თანხმობის შემდეგ. სააგენტოს მიერ ამ პუნქტით გათვალისწინებული თანხმობა/უარი ეცნობება მესამე კატეგორიის სუბიექტს წერილობით მომართვიდან 30 დღის ვადაში. თანხმობა გაცემულად ითვლება იმ შემთხვევაშიც თუ აღნიშნულ ვადაში პასუხი არ იქნება გაცემული.

2. ინფორმაციული უსაფრთხოების აუდიტი ტარდება სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერთან თანამშრომლობითა და კოორდინაციით.

3. აუდიტის ჩატარებისას დაცული უნდა იქნეს შემდეგი პრინციპები:

ა) საქმის კეთილსინდისიერად და პასუხისმგებლობით შესრულება;

ბ) მიუკერძოებლობა;

გ) აუდიტის პროცესში მოსალოდნელი გავლენებისადმი სიმტკიცის გამოჩენა;

დ) სამართლიანობა (ზუსტი და ჭეშმარიტი ანგარიშგების ვალდებულება);

ე) აუდიტის ჩატარებისას სათანადო ყურადღება;

ვ) კონფიდენციალურობა (ინფორმაციის გაუმჟღავნებლობა);

ზ) დამოუკიდებლობა (აუდიტის მიუკერძოებლობისა და აუდიტის დასკვნების ობიექტურობის საფუძველი);

თ) მტკიცებულებებზე ორიენტირებული მიდგომა: აუდიტის სანდო და განმეორებადი დასკვნების მიღების გონივრული მეთოდი;

ი) რისკზე ორიენტირებული მიდგომა: აუდიტის მიდგომა, რომელიც ითვალისწინებს რისკებსა და შესაძლებლობებს.

მუხლი 4. აუდიტის ანგარიში

1. ინფორმაციული უსაფრთხოების აუდიტის სააგენტოს მიერ ავტორიზებული ორგანიზაციის მიერ

ჩატარების შემთხვევაში აღნიშნული აუდიტის ანგარიშის (დასკვნის) 1 ეგზემპლარს სუბიექტი აუდიტის დასრულებისთანავე უგზავნის სააგენტოს, გარდა ამ მუხლის მე-2 პუნქტით გათვალისწინებული შემთხვევისა.

2. სააგენტოს ან მის მიერ ავტორიზებული ორგანიზაციის (მათ შორის, კანონის 6^1 მუხლის მე-4 პუნქტის შესაბამისად ავტორიზებული ორგანიზაციის) მიერ ინფორმაციული უსაფრთხოების აუდიტის მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკში ჩატარების შემთხვევაში ინფორმაციული უსაფრთხოების აუდიტის დასკვნის 1 ეგზემპლარს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკი ინფორმაციული უსაფრთხოების აუდიტის დასრულებისთანავე უგზავნის საქართველოს ეროვნულ ბანკს.

3. ანგარიში უნდა მოიცავდეს შემდეგ საკითხებს:

ა) აუდიტის მიზნებს;

ბ) აუდიტის გავრცელების სფეროს;

გ) აუდიტორთა გუნდის და აუდიტს დაქვემდებარებული ორგანიზაციის მონაწილეებს;

დ) აუდიტის აქტივობების ჩატარების ადგილმდებარეობას, თარიღსა და დროს;

ე) აუდიტის კრიტერიუმებს;

ვ) აუდიტის აღმოჩენებსა და მათთან დაკავშირებულ მტკიცებულებებს;

ზ) აუდიტის დასკვნებს;

თ) აუდიტის კრიტერიუმებით შესრულების შეფასება.

4. აუდიტის ანგარიში უნდა იყოს დათარიღებული, განხილული და დამტკიცებული.

მუხლი 5. აუდიტის შემდგომი ქმედებები

1. აუდიტის მიზნებიდან გამომდინარე, აუდიტის დასკვნები შესაძლოა მიუთითებდეს ინფორმაციული უსაფრთხოების მართვის სისტემაში გარკვეული შესწორებების, მაკორექტირებელი, პრევენციული ან გაუმჯობესებისკენ მიმართული აქტივობების საჭიროებაზე.

2. თუ ინფორმაციული უსაფრთხოების აუდიტის ჩატარების შედეგად გამოვლინდა იუმს-ის ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებთან შეუსაბამობა, სუბიექტი ატარებს ამ შეუსაბამობის ანალიზს და მათ აღმოსაფხვრელად განსაზღვრავს სამოქმედო გეგმას. სამოქმედო გეგმა უნდა შეიცავდეს მისი შესრულების გრაფიკს. სუბიექტი აღნიშნულ სამოქმედო გეგმას ინფორმაციული უსაფრთხოების აუდიტის დასრულებიდან 1 თვის ვადაში შესათანხმებლად წარუდგენს სააგენტოს. ხოლო, კანონის მე-6 მუხლის მე-17 პუნქტით გათვალისწინებულ შემთხვევაში, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკი სამოქმედო გეგმას და მისი შესრულების გრაფიკს ინფორმაციული უსაფრთხოების აუდიტის დასრულებიდან 1 თვის ვადაში შესათანხმებლად წარუდგენს ეროვნულ ბანკს.

3. სააგენტო საკუთარი კომპეტენციის ფარგლებში უზრუნველყოფს წარდგენილი სამოქმედო გეგმის შეფასებას, შესაბამისი რეკომენდაციების ან/და შესასრულებლად სავალდებულო მითითებების შემუშავებასა და შეთანხმებული სამოქმედო გეგმის შესრულების მონიტორინგს.

4. ინფორმაციული უსაფრთხოების აუდიტის ჩატარებისას სააგენტოს ხელი არ მიუწვდება იმ ინფორმაციაზე, რომელიც სცილდება ინფორმაციული უსაფრთხოების აუდიტის ჩატარების მიზნებს.