რეგისტრაციის #07–3/550; 03.02.2012;
ბიურო #222; 07.02.2012.

პროექტი

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 სექტორის უფლება–მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, განსაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები.

მუხლი 2. ტერმინთა განმარტება

ამ კანონის მიზნებისათვის, მასში გამოყენებულ ტერმინებს გააჩნია შემდეგი მნიშვნელობა:

ა) **ინფორმაციული უსაფრთხოება** – საქმიანობა, რომელიც იცავს ინფორმაციას და ინფორმაციულ სისტემებს მისაწვდომობის, ერთიანობის, აუთენტიფიკაციის, კონფიდენციალურობის და განგრძობადი მუშაობის უზრუნველყოფით;

ბ) **ინფორმაციული უსაფრთხოების პოლიტიკა** – ამ კანონით, საქართველოს სხვა ნორმატიული აქტებით და საერთაშორისო შეთანხმებებით გათვალისწინებული ნორმების, პრინციპებისა და პრაქტიკის ერთობლიობა, რომელიც ემსაუხრება ინფორმაციული უსაფრთხოების უზრუნველყოფას და შეესაბამება ამ სფეროში დადგენილ საერთაშორისო სტანდარტებს;

გ) **კიბერ სივრცე** – სივრცე, რომლის განმასხვავებელ ნიშანს წარმოადგენს ელექტრონული მოწყობილობებისა და ელექტრო–მაგნიტური სპექტრის გამოყენება მონაცემთა შენახვის, შეცვლისა თუ გაცვლისათვის ქსელით დაკავშირებული სისტემებისა და დამხმარე ფიზიკური ინფრასტრუქტურის მეშვეობით;

დ) **კიბერ შეტევა** – ქმედება, რომელიც იყენებს ელექტრონულ მოწყობილობას ან/და დაკავშირებულ ქსელს ან სისტემას კრიტიკული ინფრასტრუქტურის სისტემების, ქონების ან ფუნქციების მთლიანობის დარღვევის, შეფერხების, განადგურების ან ინფორმაციის უკანონოდ მოპოვების გზით;

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

ვ) **კრიტიკული ინფრასტრუქტურა** – ამ კანონით და კანონის საფუძველზე გამოცემული სხვა ნორმატიული აქტით განსაზღვრული იურიდიული პირების, სახელმწიფო ორგანოებისა და საქმიანობის სფეროების ერთობლიობა, რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის;

ზ) **კრიტიკული ინფრასტრუქტურის სუბიექტი** – სახელმწიფო ორგანო, იურიდიული პირი, რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის, ეკონომიკური უსაფრთხოების, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის;

თ) **კონფიდენციალური ინფორმაცია** – საჯარო ინფორმაცია, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფას სავარაუდოდ მოჰყვება მნიშვნელოვანი ზიანი კრიტიკული ინფრასტრუქტურის სუბიექტის ფუნქციებისათვის;

ი) **შეზღუდული ინფორმაცია** – საჯარო ინფორმაცია, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფა სავარაუდოდ გამოიწვევს კრიტიკული ინფრასტრუქტურის სუბიექტის მიერ მისი ფუნქციების განხორციელების მნიშვნელოვან შეფერხებას, ან ზიანს მიაყენებს სახელმწიფო ინტერესს ან კერძო პირის საქმიან რეპუტაციას;

კ) **არაკლასიფიცირებული ინფორმაცია** – საჯარო ინფორმაცია, რომელიც განკუთვნილია მხოლოდ კრიტიკული ინფრასტრუქტურის სუბიექტის თანამშრომლების ან/და მასთან სახელშეკრულებო ურთიერთობაში მყოფი პირისათვის, და რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფას შესაძლებელია მოჰყვეს უმნიშვნელო ზიანი ინფრასტრუქტურის სუბიექტის ან/და სახელმწიფო ხელისუფლების ორგანოს უსაფრთხოების, სახელმწიფო ინტერესებისა ან კერძო სუბიექტის საქმიანი რეპუტაციისათვის;

ლ) **ღია ინფორმაცია** – ყველა სხვა საჯარო ინფორმაცია, გარდა კონფიდენციალური, შეზღუდული ან არაკლასიფიცირებული ინფორმაციისა;

მ) **ინფორმაციული აქტივი** - ყველა ის ინფორმაცია და ცოდნა, რომელსაც გააჩნია ღირებულება კრიტიკული ინფრასტრუქტურის სუბიექტისათვის, როგორიცაა ინფორმაციის შენახვის, დამუშავების, გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ;

ნ) **ინფორმაციული სისტემა** - ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებულ ქმედებათა ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადაწყვეტილების მიღებას;

ო) **ქსელური სენსორი** – მოწყობილობა, რომელიც სპეციალურად არის გამიზნული ქსელის სეგმენტის მონიტორინგზე ისეთი ქმედებების გამოსავლენად, რომელიც მიუთითებს ინფორმაციული სისტემის წინააღმდეგ წარმოებულ შეტევას ან მასში შეღწევას.

მუხლი 3. კანონის მოქმედების სფერო

1. ამ კანონის მოქმედება ვრცელდება ყველა იურიდიულ პირზე და სახელმწიფო ორგანოზე, რომელიც წარმოადგენს კრიტიკული ინფრასტრუქტურის სუბიექტს. კანონის მოქმედება ასევე ვრცელდება ისეთ ორგანიზაციზე ან უწყებაზე, რომელიც შედის კრიტიკული ინფრასტრუქტურის სუბიექტის დაქვემდებარებაში ან დაკავშირებულია სუბიექტთან დასაქმების, სტაჟირების, სახელშეკრულებო ან სხვა ურთიერთობით, რომელიც უზრუნველყოფს წვდომას ინფორმაციულ აქტივზე ასეთი ურთიერთობის ფარგლებში.

2. კრიტიკული ინფრასტრუქტურის კონკრეტული სუბიექტების ნუსხა და შესაბამისი სუბიექტის კრიტიკულობის კლასიფიცირება დგინდება საქართველოს პრეზიდენტის ბრძანებულებით, რომლის პროექტს საქართველოს პრეზიდენტს დასამატკიცებლად წარუდგენს საქართველოს ეროვნული უშიშროების საბჭო.

ვარიანტი 2: კრიტიკული ინფრასტრუქტურის კონკრეტული სუბიექტების ნუსხის შედგენის მიზნით და ნუსხაში შემავალი სუბიექტების კრიტიკულობის კლასიფიცირების დასადგენად, იქმნება ინფორმაციული უსაფრთხოების უწყებათაშორისი კომისია, რომლის შემადგენლობა და საქმიანობის წესი განისაზღვრება საქართველოს პრეზიდენტის ბრძანებულებით.

3. ნებისმიერ იურიდიულ პირს და სახელმწიფო ხელისუფლების ორგანოს, რომელიც არ წარმოადგენს კრიტიკული ინფრასტრუქტურის სუბიექტს, უფლება აქვს, ნებაყოფლობით აიღოს ამ კანონიდან გამომდინარე ვალდებულებები.

4. კანონის მოქმედება არ ვრცელდება კრიტიკული ინფრასტრუქტურის სუბიექტის წინასწარი თანხმობით ნებადართულ ქმედებაზე, რომელიც მიზნად ისახავს ინფორმაციული უსაფრთხოების ტესტირებას.

5. კანონის დებულებები გავლენას არ ახდენს საქართველოს კანონმდებლობით გათვალისწინებულ იმ ნორმათა მოქმედებაზე, რომელიც არეგულირებს ინფორმაციის თავისუფლებას, პერსონალური მონაცემის დამუშავებას, სახელმწიფო, კომერციული ან პირადი საიდუმლოს დაცვას.

თავი II. ინფორმაციული უსაფრთხოების ორგანიზაცია და შესრულების უზრუნველყოფა

მუხლი 4. ინფორმაციული უსაფრთხოების წესები

1. კრიტიკული ინფრასტრუქტურის სუბიექტი ვალდებულია მიიღოს შიდასამსახურებრივი გამოყენების წესები, რომელიც ემსახურება ამ კანონის დებულებათა აღსრულებას და განსაზღვრავს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკას.

2. ინფორმაციული უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს სუბიექტის კრიტიკულობის კლასიფიცირების გათვალისწინებით, რომელსაც განსაზღვრავს საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი – მონაცემთა გაცვლის სააგენტო (შემდგომში:

მონაცემთა გაცვლის სააგენტო) სტანდარტიზაციის საერთაშორისო ორგანიზაციისა (ISO) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილ სტანდარტებსა და მოთხოვნებთან შესაბამისობაში.

3. კრიტიკული ინფრასტრუქტურის სუბიექტი ვალდებულია წარუდგინოს მონაცემთა გაცვლის სააგენტოს მიღებული ინფორმაციული უსაფრთხოების პოლიტიკა, ისევე როგორც მასში განხორციელებული ნებისმიერი ცვლილება.

მუხლი 5. ინფორმაციული აქტივების მართვა

1. კრიტიკული ინფრასტრუქტურის სუბიექტი, ამ კანონის მე-4 მუხლის პირველი ნაწილით გათვალისწინებული შიდასამსახურებრივი გამოყენების წესების შესაბამისად, ატარებს ინფორმაციული სისტემების ინვენტარიზაციას ყველა ინფორმაციული აქტივის აღრიცხვის მიზნით, რომლის შედეგადაც ყოველ ინფორმაციულ აქტივს მიენიჭება კრიტიკულობის შესაბამისი კლასი – კონფიდენციალური, შეზღუდული, არაკლასიფიცირებული ან ღია ინფორმაციული აქტივი.

2. ინვენ ტარიაზციის 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. ინფორმაც იული აქტივების აღწერის, კლასიფიცირების, მასზე წვდომის, მისი გაცემის (გამოქვეყნების), მისი შეცვლის ან განადგურების წესს ნორმატიული აქტით ადგენს მონაცემთა გაცვლის სააგენტო.

მუხლი 6. აუდიტი და ტესტირება

1. მონაცემთა გაცვლის სააგენტო ან, მონაცემთა გაცვლის სააგენტოს მიერ ავტორიზირებულ პირთა წრიდან კრიტიკული ინფრასტრუქტურის სუბიექტის მიერ შერჩეული პირი ან ორგანიზაცია, ატარებს კრიტიკული ინფრასტრუქტურის სუბიექტის ინფორმაციული უსაფრთხოების პოლიტიკის თავსებადობის შეფასებას მონაცემთა გაცვლის სააგენტოს მიერ დადგენილ უსაფრთხოების მინიმალურ სტანდარტებთან (ინფორმაციული უსაფრთხოების აუდიტი). ინფორმაციული აუდიტის ჩატარების შედეგად დგება დასკვნა, რომელიც სავალდებულოა შესასრულებლად.

2. ამ მუხლის პირველი პუნქტით გათვალისწინებული ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესს ნორმატიული აქტით ადგენს მონაცემთა გაცვლის სააგენტო.

3. მონაცემთა გაცვლის სააგენტოს მიერ ჩატარებული ინფორმაციული უსაფრთხოების აუდიტის საფასური განისაზღვრება კრიტიკული ინფრასტრუქტურის სუბიექტთან გაფორმებული ხელშეკრულების საფუძველზე.

4. მონაცემთა გაცვლის სააგე ნტო ნორმატიული აქტით განსაზღვრავს ინფორმაციული უსაფრთხოების აუდიტის ჩატარებაზე უფლებამოსილ პირთა ან

ორგანიზაციათა ავტორიზაციის გავლის წესს, ავტორიზაციის პროცედურებსა და ავტორიზაციის საფასურს.

5. მონაცემთა გაცვლის სააგენტო ან, მისი წინასწარი ნებართვით – კრიტიკული ინფრასტრუქტურის სუბიექტის მიერ შერჩეული დამოუკიდებელი, შესაბამისი კომპეტენციის მქონე პირი ან ორგანიზაცია ატარებს ინფორმაციული სისტემის შეღწევის (პენეტრაციის) ტესტს და მოწყვლადობის შეფასებას წინასწარ დაგეგმილი და დოკუმენტირებული ამოცანის მიხედვით.

6. თუ აუდიტის ან ტესტირების შედეგად გამვლინდა ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნებთან შეუსაბამობა, კრიტიკული ინფრასტრუქტურის სუბიექტი ატარებს შეუსაბამობის მიზეზის ანალიზს და, საჭიროების შემთხვევაში, განსაზღვრავს და ახორციელებს სათანადო გამოსასწორებელ ღონისძიებებს, რომელთა გრაფიკსაც წარუდგენს მონაცემთა გაცვლის სააგენტოს.

მუხლი 7. ინფორმაციული უსაფრთხოების ოფიცერი

1. კრიტიკული ინფრასტრუქტურის სუბიექტი ვალდებულია, განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი, რომელიც პასუხისმგებელია სუბიექტის ინფორმაციული უსაფრთხოების მოთხოვნათა შესრულებაზე (შემდგომში: ინფორმაციული უსაფრთხოების ოფიცერი).

2. ინფორმაციული უსაფრთხოების ოფიცრის ძირითადი მოვალეობებია:

ა) ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნათა შესრულების ყოველდღიური მონიტორინგი;

ბ) ინფორმაციული აქტივებისა და მათზე წვდომის აღწერა;

გ) ინფორმაციული უსაფრთხოების პოლიტიკის შიდაუწყებრივი დოკუმენტაციის მომზადება;

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

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

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

ზ) სხვა მოვალეობები, რომელიც კრიტიკული ინფრასტრუქტურის სუბიექტის მიერ განისაზღვრება.

3. ინფორმაცი ული უსაფრთხოების ოფიცერი ანგარიშვალდებულია კრიტიკული ინფრასტრუქტურის სუბიექტის ხელმძღვანელი პირის ან მის მიერ შესაბამისად უფლებამოსილი თანამშრომლის ან ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელებაზე უფლებამოსილი პირთა ჯგუფის (კოლეგიური ორგანოს) წინაშე. ყველა მნიშვნელოვანი გადაწყვეტილება, რომელიც შეეხება ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელებას, მიიღება ამ პუნქტით განსაზღვრული პირის (პირების) მიერ ან მასთან (მათთან) წინაწარი შეთანხმებით.

4. ინფორმაციული უსაფრთხოების ოფიცერი ადგენს ინფორმაციული უსაფრთხოების სამოქმედო გეგმას, და გეგმის შესრულების შესახებ ყოველწლიურ ანგარიშს წარდუგენს ამ მუხლის მე–3 პუნქტით განსაზღვრულ პირს (პირებს) და მონაცემთა გაცვლის სააგენტოს.

5. ინფორმაციული უსაფრთხოების ოფიცერი უნდა აკმაყოფილებდეს ინფორმაციული პოლიტიკის აღსრულებისათვის აუცილებელ მინიმალურ სტანდარტებს, რომელთაც ნორმატიული აქტით ადგენს მონაცემთა გაცვლის სააგენტო.

თავი III. კიბერ უსაფრთხოების უზრუნველყოფა

მუხლი 8. კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფი

1. ამ კანონის დებულებათა აღსრულებას, კერძოდ, ინფ ორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას საქართველოს კიბერ–სივრცეში, ასევე ინფორმაციული უსაფრთხოების კოორდინაციაზე მიმართულ სხვა, დაკავშირებულ საქმიანობას, რომელიც ინფორმაციული უსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფი – cert.gov.ge (შემდგომში – სწრაფი რეაგირების ჯგუფი).

2. კიბერ უსაფრთხოების პრიორიტეტულ საფრთხეებს მიეკუთვნება:

ა. კიბერ–შეტევა, რომელიც საფრთხის ქვეშ აყენებს ადამიანთა სიცოცხლეს და ჯანმრთელობას, სახელმწიფო ინტერესებს ან ქვეყნის თავდაცვისუნარიანობას;

ბ. კიბერ–შეტევა კრიტიკული ინფრასტრუქტურის ინფორმაციული სისტემის წინააღმდეგ;

გ. კიბერ–შეტევა, რომელიც საფრთხეს უქმნის სახელმწიფოს, ორგანიზაციის ან კერძო პირის ფინანსურ რესურებს ან/და საკუთრების უფლებას;

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

3. სწრაფი რეაგირების ჯგუფის მოვალეებში შედის:

ა. კრიტიკული ინფრასტრუქტურის ინფორმაციული უსაფრთხოების დაცვის თაობაზე რეკომენდაციების გაცემა;

ბ. კომპიუტერული ინციდენტების დროული გამოვლენა;

გ. კომპიუტერულ ინციდენტებზე რეაგირება და მათზე რეაგირების კოორდინაცია;

დ. კომპიუტერული ინციდენტების აღრიცხვა და მათზე რეაგირების პრიორიტეტების დადგენა/კატეგორიზაცია;

ე. კომპიუტერული ინციდენტების ანალიზი;

ვ. დახმარების გაწევა კომპიუტერული ინციდენტის შედეგების გამოსწორებისა და ზიანის მინიმიზაციის პროცესში;

ზ. კომპიუტერული ინციდენტების პრევენციაზე მიმართული ზომების კოორდინაცია და დახმარების გაწევა ამგვარი ზომების დანერგვაში;

თ. ცნობიერიების ამაღლება ინფორმაციული უსაფრთხოების საკითხებში, მათ შორის ინფორმაციის მიწოდება კრიტიკული ინფრასტრუქტურის ინფორმაციულ სისტემებში არსებული საფრთხეებისა და სუსტი წერტილების შესახებ, თუ ინფორმაციის ამგვარი ხელმისაწვდომობა ზიანს არ აყენებს ინფორმაციულ უსაფრთხოებას;

ი. მომხმარებელთა ფართო წრისათვის გაფრთხილებისა და ინფორმაციის მიწოდება შესაძლო საფრთხეების შესახებ;

კ. საგანმანათლებლო და ინფორმაციული უზრუნველყოფა ინფორმაციული უსაფრთხოების საკითხებში;

ლ. ინფორმაციული უსაფრთხოების საკითხების წარმომადგენლობა და კოორდინაცია საერთაშორისო დონეზე;

მ. სხვა ფუნქციები, რომელიც დაკავშირებულია ინფორმაციული უსაფრთხოების მიზნებთან და განისაზღვრება კანონით ან სხვა ნორმატიული აქტით.

4. სწრაფი რეაგირების ჯგუფს უფლება აქვს, მოითხოვოს წვდომა კრიტიკული ინფრასტრუქტურის სუბიექტის ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე, თუ ამგვარი წვდომა აუცილებელია მიმდინარე ან მომხდარი კომპიუტერული ინციდენტზე სათანადო რეაგირებისათვის. კრიტიკული ინფრასტრუქტურის სუბიექტის ინფორმაციული უსაფრთხოების ოფიცერი, მოთხოვნის გონივრულ ვადაში განხილვის შედეგად, სწრაფი რეაგირების ჯგუფს დაუყოვნებლივ აცნობებს შესაბამისი წვდომის შესაძლებლობის თუ შეუძლებლობის შესახებ.

5. სწრაფი რეაგირების ჯგუფის კომპეტენცია, მუშაობის პროცედურები, რეაგირების მექანიზმები და საქმიანობის სხვა წესები განისაზღვრება მონაცემთა გაცვლის სააგენტოს ნორმატიული აქტით.

მუხლი 9. კომპიუტერული უსაფრთხოების სპეციალისტი

1. კრიტიკული ინფრასტრუქტურის სუბიექტი ვალდებულია, განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი, რომელიც პასუხისმგებელია კრიტიკული ინფრასტრუქტურის სუბიექტის კომპიუტერული სისტემების უსაფრთხოების პრაქტიკულ უზრუნველყოფაზე (შემდგომში: კომპიუტერული უსაფრთხოების სპეციალისტი).

2. კომპიუტერული უსაფრთხოების სპეციალისტი ძირითადი მოვალეობებია:

ა) კომპიუტერული სისტემების ყოველდღიური მონიტორინგი და შეფასება;

ბ) კომპიუტერული უსაფრთხოების ინციდენტების იდენტიფიცირება და მათზე რეაგირება;

გ) კომპიუტერული უსაფრთხოების ინციდენტებისა და ზომების ანალიზი და ანგარიშგება;

დ) კოორდინაცია მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფთან;

ე) სხვა მოვალეობები, რომელიც კრიტიკული ინფრასტრუქტურის სუბიექტის მიერ განისაზღვრება.

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

4. კომპიუტერული უსაფრთხოების სპეციალისტი ხელმისაწვდომი უნდა იყოს ნებისმიერ დროს, მათ შორის სამსახურებრივი საქმიანობის საათების შემდეგ, და ვალდებულია უზრუნველყოს მუდმივი კოორდინაცია მონაცემთა გაცვლის სააგენტოსთან კრიტიკული ინფრასტრუქტურის სუბიექტზე როგორც მიმდინარე ან სავარაუდო კიბერ–შეტევის პირობებში, ისე შეტევის შედეგების აღმოფხვრის პროცესში.

5. იმ შემთხვევაში, როდესაც მიმდინარე ან სავარაუდო კიბერშეტევა წარმოადგენს განსაკუთრებულ საფრთხეს ქვეყნის თავდაცვისუნარიანობის, ეკონომიკური უსაფრთხოების, სახელმწიფო ხელისუფლებისა და საზოგადოების ნორმალური ფუნქციონირების წინააღმდეგ, მონაცემთა გაცვლის სააგენტო უფლებამოსილია, განახორციელოს კრიტიკული ინფრასტრუქტურის სუბიექტების კომპიუტერული უსაფრთხოების სპეციალისტების დროებითი მობილიზაცია (კოორდინაცია) შეტევის პრევენციის, მოგერიების ან/და შედეგების აღმოფხვრის მიზნით.

მუხლი 10. კომპიუტერული უსაფრთხოების ინციდენტის იდენტიფიცირება

1. კრიტიკული ინფრასტრუქტურის სუბიექტი ახორციელებს კომპიუტერული ინციდენტების იდენტიფიცირებას, რაც მოიცავს თითოეული ინციდენტის შესწავლას, აღწერასა და მასზე რეაგირებას.

2. კრიტიკული ინფრასტრუქტურის სუბ იექტთან შეთანხმებით, მონაცემთა გაცვლის სააგენტო და კრიტიკული ინფრასტრუქტურის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტი კრიტიკული ინფრასტრუქტურის სუბიექტის ქსელში ახდენენ კომპიუტერული ინციდენტების იდენტიფიცირებისა და კვლევისათვის აუცილებელი ქსელური სენსორის (სენსორების სისტემის) კონფიგურირებას და მართვას. ქსელური სენსორის კონფიგურაციის წესები დგინდება მონაცემთა გაცვლის სააგენტოს ნორმატიული აქტით.

3. კომპიუტერული ინციდენტის იდენტიფიცირების შესახებ დაუყოვნებლივ ეცნობება სწრაფი რეაგირების ჯგუფს და, თუ ეს აუცილებელია, ტარდება გადაუდებელი ღონისძიებები ინციდენტის შესახებ ინფორმაციის შენახვისა და დაცვის მიზნით.

4. სწრაფი რეაგირების ჯგუფი ახდენს კომპიუტერული ინციდენტების შესწავლას, აღწერასა და მათზე ადეკვატურ რეაგირებას ამ კანონით გათვალისწინებული ფუნქციების შესრულებისას.

თავი IV. გარდამავალი და დასკვნითი დებულებები

მუხლი 11. გარდამავალი დებულებები

1. ამ კანონის ძალაში შესვლიდან 6 თვის ვადაში, საქართველოს პრეზიდენტმა გამოსცეს ბრძნებულება „კრიტიკული ინფრასტრუქტურის სუბიექტების ნუსხის დამტკიცების შესახებ“.

2. ა მ კანონის ძალაში შესვლიდან 3 თვის ვადაში, მონაცემთა გაცვლის სააგენტოს დაევალოს შემდეგი ნორმატიული აქტების გამოცემა:

ა. ბრძანება „მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფის შესახებ“;

ბ. ბრძანება „კრიტიკული ინფრასტრუქტურის სუბიექტის ინფორმაციული უსაფრთხოების ოფიცერისათვის მინიმალური სტანდარტების დამტკიცების შესახებ“;

გ. ბრძანება „კრიტიკული ინფრასტუქტურის სუბიექტის ქსელში ქსელური სენსორის კონფიგურაციის წესების შესახებ“;

დ. ბრძანება ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესახებ“;

ე. ბრძანება ,,ინფორმაციული უსაფრთხოების აუდიტის ჩატარებაზე უფლებამოსილ პირთა ან ორგანიზაციათა ავტორიზაციის გავლის წესის, ავტორიზაციის პროცედურებისა და ავტორიზაციის საფასურის შესახებ“;

ვ. ბრძანება ,,აუდიტის ჩატარების წესის შესახებ“;

ზ. ბრძანება „ინფორმაციული აქტივების აღწერის, კლასიფიცირების, მასზე წვდომის, მისი გაცემის (გამოქვეყნების), მისი შეცვლის ან განადგურების წესის დამტკიცების შესახებ“.

3. ამ კანონის ძალაში შესვლიდან 6 თვის ვადაში, კრიტიკული ინფრასტრუქტურის თითოეულ სუბიექტს დაევალოს ინფორმაციული უსაფრთხოების შიდასამსახურებრივი გამოყენების წესების დამტკიცება.

მუხლი 12. დასკვნითი დებულება

ეს კანონი ამოქმედდეს 2012 წლის 1 ივნისიდან.

საქართველოს პრეზიდენტი მიხეილ სააკაშვილი

განმარტებითი ბარათი

საქართველოს კანონის პროექტზე „ინფორმაციული უსაფრთხოების შესახებ“

ა) ზოგადი ინფორმაცია კანონპროექტის შესახებ

ა. ა) კანონპროექტის მიღების მიზეზი:

2009 წელს 17 ივლისს მიღებული „საჯარო სამართლის იურიდიული პირის – მონაცემთა გაცვლის სააგენტოს შექმნის შესახებ“ საქართველოს კანონის (საქართველოს საკანონმდებლო მაცნე, სარეგისტრაციო კოდი 040.030.000.05.001.003.579) მე –5 მუხლის მე –2 პუქნტის შესაბამისად, „ სააგენტოს საქმიანობის საგანია [...] ინფორმაციული ტექნოლოგიების (სისტემების) და ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა“, ხოლო ამავე კანონის მე –6 მუხლის „ბ“ ქვეპუნქტის თანახმად, სააგენტოს ევალება „უზრუნველყოს ინფორმაციული უსაფრთხოება, მათ შორის, განახორციელოს საგანმანათლებლო საქმიანობა როგორც საჯარო, ისე სამოქალაქო სექტორში“, რა მიზნითაც მას შეუძლია „შეიმუშაოს ინფორმაციული ტექნოლოგიების (სისტემების) სფეროს მარეგულირებელი სამართლებრივი აქტების პროექტები“ (იმავე მუხლის „მ“ ქვეპუნქტი). შემოთავაზებული კანონპროექტი სწორედ ამ უფლებამოსილებათა განხორციელებას ემსახურება.

ა. ბ) კანონპროექტის მიზანი:

– ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, რა მიზნითაც კანონპროექტი ადგენს ინფორმაციული უსაფრთოების ძირითად სტანდარტებს და კიბერ–უსაფრთხოების განხორციელების სამართლებრივ და ინსტიტუციურ საფუძვლებს;

– დააწესოს საჯარო და კერძო სექტორის უფლება–მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, როგორიცაა ინფორმაციული უსაფრთოების შიდაუწყებრივი (ორგანიზაციის) სტანდარტებს მიღება და დანერგვა, ინფრომაციულ უსაფრთხოებაზე პასუხისმგებელი პირების დანიშვნა, კიბერ – უსაფრთხოების უზრუველყოფა შიდა და თანამშმობაზე დამყარებული მეაქნიზმების გამოყენებით და სხვ.

– განსაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები, როგორიცაა კრიტიკული ინფრასტრუქტურის სუბიექტთა წრის დადგენა, ასევე აუდიტის, აქტივების ინვენტარიზაციის, ინფორმაციის კლასიფიცირების და სხვა ვალდებულებათა მონიტორინგის სისტემის შექმნა, და კიბერ–უსაფრთხოების სფეროში ყოველდღიური თანამშრომლობის დამყარება უწყებებსა და კომპიუტერულ ინციდენტებზე რეაგირების ეროვნულ მექანიზმებს შორის.

ა. გ) კანონპროექტის ძირითადი არსი:

21-ე საუკუნეში ინფო-საკომუნიკაციო ტექნოლოგიების განვითარებამ სახელმწიფოს და მისი მოქალაქეების მოღვაწეობის ყველა სფეროში მნიშვნელოვანი ადგილი დაიკავა, საფუძველი ჩაეყარა ინფორმაცია–ტევადი ეკონიმიკებისა და ინფორმაციული საზოგადოების შექმნას. ახალმა ტექნოლოგიურმა რეალობამ უპირობოდ დადებითი ეფექტი იქონია ქვეყნის საზოგადოებრივ კეთილდღეობაზე. ინფო-საკომუნიკაციო ტექნოლოგიები ინოვაციებისა და წარმატების განუყოფელი ნაწილი გახდა და დღეს სწორედ მათი საშუალებით ხდება ყველა მნიშვნელოვანი თუ უმნიშვნელო ურთიერთობა მოქალაქეებს, ბიზნესსა თუ სახელმწიფოს ყველა წვერს შორის.

საქართველო, მიუხედავად მის წინაშე არსებული სირთულეებისა, ბოლო წლების განმავლობაში ცდილობდა დაენერგა და თავის საკეთილდღეოდ გამოეყენებინა ის სიკეთეები, რაც ინფო-საკომუნიკაციო ტექნოლოგიების განვითარებამ მოიტანა მსოფლიოში. ამ მიმართულებით, კერძო სექტორიდან განსაკუთრებით აღსანიშნავია საფინანსო-საბანკო სექტორის წარმატებები, რაც საბანკო ელექტრონული სერვისებისა და ინფო-საკომუნიკაციო გადაწყვეტილებების სიმრავლეში ვლინდება. საჯარო სექტორში ადგილი ჰქონდა ინფორმაციული ტექნოლოგოების აქტიური დანერგვას ბიზნეს პროცესების ოპტიმიზებისა და არსებული პროცესების გამჭვირვალობის უზრუნველყოფისათვის. საქართველოს მთავრობის ინიცირებით განხორციელებულმა საქართველოს სამთავრობო ქსელის პროექტმა (GGN) შეძლო მთელი ქვეყნის ინტერნეტით დაფარვა. ასევე ამჟამად უკვე დღის წესრიგშია ელ-მმართველობის ისეთი ფუძემდებლური კომპონენტების განვითარება, როგორცია მონაცემთა გაცვლის ერთიანი ინფრასტრუქტურა, მოქალაქის პორტალი, ელექტრონული პირადობის მოწმობა და ელექტრონული ხელმოწერა.

ინფო-საკომუნიკაციო ტექნოლოგიებს მნიშვნელოვანი ადგილი უკავია საქართველოს მოქალაქეების ყოველდღიურ ცხოვრებასა და სახელმწიფოს მიერ მისი მოვალეობის განხორციელების პროცესში. თანამედროვე ტექნოლოგიებზე დამოკიდებულება დღითიდღე იზრდება. აქედან გამომდინარე, არსებული სისტემების შეფერხებამ ან მათმა კომპრომეტირებამ შესაძლებელია მნიშვნელოვანი, ზოგიერთ შემთხვევაში კი გამოუსწორებელი, პოლიტიკურ-ეკონომიკური ზიანი მიაყენოს ქვეყანას, რისი ყველაზე ნათელი მაგალითი გახლდათ საქართველოს წინააღმდეგ 2008 წლის აგვისტოში განხორციელებული მასშტაბური კიბერ–შეტევა.

ინფო-საკომუნიკაციო ტექნოლოგიები, ისევე როგორც ნებისმიერი სხვა საშუალება, მიუხედავად მათი დანიშნულებისა, შეიძლება ასევე სხვადასხვა საფრთხეებისა და გამოწვევების მომტანი იყოს. მათ შეიძლება არასასურველი

გავლენა მოახდინონ მოქალაქის პირადი ცხოვრების დაცულობაზე, ბიზნესის კონფიდენციალურობასა და მდგრადობაზე და სახელმწიფოს შეუქმნან სირთულეები მისი ფუნქციების შესრულებაში. თავისი ხასიათის სპეციფიკიდან გამომდინარე, საფრთხეები, რომლებიც ინფორმაციულ ტექნოლოგიებს უკავშირდება, ხშირად რთულად იდენტიფიცირებადია. უმეტეს შემთხვევებში ისინი ასიმეტრიულ ხასიათს ატარებს და მხოლოდ გამონაკლის შემთხვევებში არსებობს საშუალება ცალსახად მოხდეს უსაფრთხოების ინციდენტის ინიციატორის იდენტიფიცირება, ისევე როგორც მსგვასი შემთხვევების პრევენცია. შეტევა სხვადასხვა ფორმით ვლინდება და მავნე ზემოქმედებას ახდენს მთალიანად ქვეყნის განვითარებაზე.

ინფორმაციული უსაფრთხოების სამართლებრივი ასპექტები საკმაოდ დაურეგულირებელია როგორც საერთაშორისო არენაზე, ასევე შიდა ეროვნული კანონმდებლობებით. არ არსებობს ინფორმაციული უსაფრთხოების საკითხებზე სპეციალური საერთაშორისო კონვენცია თუ სხვა სავალდებულოდ შესასრულებელი საერთაშორისო სამართლებრივი აქტი, რომლის პრინციპებზე დაყრდნობით ცალკეული ქვეყნები განსაზღვრავდნენ შიდა სამართლებრივ ბაზას. ისეთი მნიშვნელოვანი ცნებები, როგორიცაა კრიტიკული ინფრასტრუქტურა, კიბერ საფრთხე, კიბერ შეტევა და ა.შ., არ არის განსაზღვრული საერთაშორისო დონეზე, რაც ხშირ შემთხვევაში მრავალ გაუგებრობასა და ამა თუ იმ ქმედების კვალიფიკაციის პრობლემას ქმნის.

საქართველოს არც ერთი სამართლებრივი აქტით არ არის განსაზღვრული, თუ რომელი სექტორები წარმოადგენს საქართველოსთვის კრიტიკული ინფრასტრუქტურას. როგორც სართაშორისო პრაქტიკა გვიჩვენებს, მსგავსი ცნების არსებობა აუცილებელია, რათა მკაფიოდ იყოს იდენტიფიცირებული იმ ინფრასტრუქტურათა ერთობლიობა, რომელთა შეფერხებულმა მუშაობამ შეიძლება გამოუსწორებელი ზიანი მიაყენოს ქვეყნის მდგრადობასა თუ მის სოციალურ-ეკონომიკურ კეთილდღეობას. საქართველოში არსებული ინფორმაციული საიდუმლოების დონეები არ შეესაბამება მსოფლიოში (EU და NATO ქვეყნებში) მოქმედ სტანდარტებს, აგრეთვე არ არსებოს ინფორმაციის და აქტივების კრიტიკულობის დონის განსაზღვრება.

დღეს არსებული მდგომარეობით თითოეული სამინისტრო და სახელმწიფო უწყება თავისი არსებული რესურესების გამოყენებით ზრუნავს კიბერ უსაფრთოების დაცვაზე. რესურსებიდან გამომდნინარე დაცვის დონე განსხვავებულია უწყებს შორის. ხშირად ეს დონე არ შეესაბამება დაცვის მინიმალურ დონესაც. რაც შეეხება სამოქალაქო სექტორს ან მოქალაქეებს ამ მიართულებით თითქმის არავითარი ნაბიჯები არ არის გადადგმული.

ამასთან, საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – მონაცემთა გაცვლის სააგენტოს

საქმიანობის საგანია სახელმწიფო ხელისუფლების განხორციელებისას ელექტრონული მმართველობის პრინციპებზე დაფუძნებული ერთიანი სისტემის შექმნა, ინფორმაციული ტექნოლოგიების (სისტემების) და, რაც მთავარია, ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა. მონაცემთა გაცვლის სააგენტოში მიმდინარეოს ინფორმაციული უსაფთხოების პოლიტიკის შექმნის და დანერგვის პროექტი, პირველად იუსტიციის სამინისტროში, შემდეგ იგი მოდიფიცირდება და გავრცელედება სხვა სახელმწიფო სტრუქტურებზეც ქვეყნის მასშტაბით. მონაცემთა გაცვლის სააგენტოს ინიციატივით, ჩამოყალიბდა კომპიუტერულ ინდიდენტებზე სწრაფი რეაგირების ჯგუფი (საქართველოს ნაციონალური CERT.GOV). აქვე აღსანიშნავია რომ, სააგენტოს უფლემამოსლება ინფორმაციული უსაფთხოების საკითხებში ვრცელედება მხოლოდ საჯარო სექტორზე და კრიტიულ ინფრასტრუტურაზე.

ინფო-საკომუნიკაციო ტექნოლოგიებით მიღებული დადებითი შედეგების სრულფასოვნად გამოყენებისა და ამავდროულად მათგან მომდინარე საფრთხეების მინიმიზაციისა და თავიდან ასაცილებლად, სახელმწიფო ვალდებულია იზრუნოს მისი მოქალაქეების დაცულობაზე, შექმნას შესაბამისი რეგულირების წესები და კონტროლის მექანიზმები, რათა საზოგადოებამ სრულფასოვნად და საფრთხეების მინიმალური ოდენობით მიიღოს ის სიკეთე, რომელიც ახალ ტექნოლოგიების გამოყენებას მოაქვს.

შეთავაზებული კანონპროექტის მიღების მიზანია, ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, დააწესოს საჯარო თუ კერძო სექტორის (კრიტიკული ინფრასტრუქტურის) კანონისმიერი ვალდებულებანი და მისი განხორციელების სახელმწიფო და საზოგადოებრივი კონტროლის მოქნილი მექანიზმები. ამგვარი კანონმდებლობის მიღება ასევე გაზრდის არამარტო სახელმწიფოს მონაწილეობას, არამედ კერძო სექტორისა და სამოქალაქო საზოგადოების ჩართულობას ინფორმაციული უსაფრთხოების დაცვისა და განვითარების პროცესში. ინფორმაციული უსაფრთხოების მარეგულირებელი ახალი სამართლებრივი ბაზა უნდა გახდეს ქვეყანაში ინფორმაციული უსაფრთხეობის დაცვის ყველაზე მნიშვნელოვანი და მოქნილი მექანიზმი, რომლის საშუალებითაც სახელმწიფო ადექვატურ ზომებს მიიღებს მოსახლეობის დასაცავად ინფორმაციული ტექნოლოგიებიდან გამომიდნარე საფრთხეებისაგან.

ბ) კანონპროექტის ფინანსური დასაბუთება

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

კანონპროექტის მიღება არ გამოიწვევს სახელმწიფო ბიუჯეტიდან ხარჯების გამოყოფის აუცილებლობას.

ბ. ბ) კანონპროექტის გავლენა ბიუჯეტის საშემოსავლო ნაწილზე:

კანონპროექტის მიღება გავლენას არ მოახდენს ბიუჯეტის საშემოსავლო ნაწილზე.

ბ. გ) კანონპროექტის გავლენა ბიუჯეტის ხარჯვით ნაწილზე:

კანონპროექტი გავლენას არ ახდენს სახელმწიფო ბიუჯეტის ხარჯვით ნაწილზე.

ბ. დ) სახელმწიფოს ახალი ფინანსური ვალდებულებები:

კანონპროექტის თანახმად სახელმწიფოს ახალი ფინანსური ვალდებულებები არ ეკისრება.

ბ. ე) კანონპროექტის მოსალოდნელი ფინანსური შედეგები იმ პირთათვის, რომელთა მიმართაც ვრცელდება კანონპროექტის მოქმედება:

ფინანსურ შედეგებს არ გამოიწვევს.

ბ. ვ) კანონპროექტით დადგენილი გადასახადის, მოსაკრებლის ან სხვა სახის გადასახდელის ოდენობის განსაზღვრის წესი (პრინციპი):

საქართველოს საგადასახადო კოდექსით დადგენილი საერთო წესი.

გ) კანონპროექტის მიმართება საერთაშორისო სამართლებრივ სტანდარტებთან

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

კანონპროექტით არ იცვლება საერთაშორისო ორგანიზაციებში საქართველოს წევრობასთან დაკავშირებული ვალდებულებები.

გ. ბ) კანონპროექტის მიმართება საქართველოს ორმხრივ და მრავალმხრივ ხელშეკრულებებთან:

კანონპროექტი შეესაბამება საქართველოს ორმხრივ და მრავალმხრივ ხელშეკრულებებს.

დ. ა) კანონპროექტის მომზადების პროცესში მიღებული კონსულტაციები:

კანონპროექტის შემუშავების სტადიაზე, მიღებული იქნა საექსპერტო დახმარება ევროკავშირის TAIEX პროგრამის ფარგლებში; საქართველოში მოვლენილმა ექსპერტმა, ზეპირი კონსულტაციების საფუძველზე, შეიმუშავა საკანონმდებლო სახის რეკომენდაციები, რომელიც კანონპროექტში

გათვალისწინებულ იქნა. კანონპროექტის ძირითადი პრინციპების შესახებ ზეპირი კონსულტაციები ასევე მიმიდნარეობა საქართველოს უშიშროების საბჭოს სამუშაო ჯგუფის შეხვედრებზე, რომელიც კიბერ–უსაფრთოების ეროვნულ სტრატეგიასა და სამოქმედო გეგმას ეხებოდა.

დ. ბ) კანონპროექტის შემუშავებაში მონაწილე ორგანიზაციის (დაწესებულების) ან/და ექსპერტის შეფასება კანონპროექტის მიმართ, ასეთის არსებობის შემთხვევაში:

კანონპროექტზე შენიშვნები და წინადადებები წარმოადგინა ბ-ნმა მიროსლავ მაიმ, პოლონეთის კიბერ-უსაფრთხოების ერთ-ერთმა წამყვანმა ექსპერტმა, რომელიც მონაცემთა გაცვლის სააგენტოს დახმარებას უწევდა გაეროს განვითარების პროგრამის (UNDP) შესაბამისი პროექტის ფარგლებში. ბ-ნი მიროსლავის შენიშვნები და წინადადებები ძირითადად CERT.GOV.GE-ს ფუქნციებს და სერვისებს ეხებოდა და მათი უმეტესობა კანონპროექტში გათვალისწინებულ იქნა.

დ. გ) კანონპროექტის ავტორი:

საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში შემავალი საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო.

დ. დ) კანონპროექტის ინიციატორი: საქართველოს პარლამენტის წევრები: კახაბერ ანჯაფარიძე და ზვიად კუკავა.