ინოვაციებისა და რეფორმების ცენტრი
INNOVATIONS AND REFORMS CENTER

2020/03/13

IRC-ის პოზიცია ინფორმაციული უსაფრთხოების სისტემის მოწყობის შესახებ, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში 2019 წელს ინიცირებულ ცვლილებებთან დაკავშირებით

წინამდებარე დოკუმენტში წარმოდგენილია ინოვაციებისა და რეფორმების ცენტრის (IRC) ზოგადი ხედვა ინფორმაციული უსაფრთხოების სისტემის მოწყობის ცალკეულ საკითხებზე, რაც უკავშირდება 2019 წლის ოქტომბერში საქართველოს პარლამენტის წევრის ირაკლი სესიაშვილის მიერ ინიცირებულ N07-3/401/9 კანონპროექტს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილებების შეტანის თაობაზე“.

დოკუმენტი არ მოიცავს კანონპროექტით შემოთავაზებული ცვლილებების დეტალურ მიმოხილვასა და შეფასებას, არამედ შეეხება მხოლოდ რამდენიმე კონცეპტუალურ საკითხს.

დღეს მოქმედი რედაქციით, „ინფორმაციული უსაფრთხოების შესახებ“ კანონი ითვალისწინებს ორ მარეგულირებელს ამ სფეროში: 1) იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი სსიპ - მონაცემთა გაცვლის სააგენტო და 2) თავდაცვის სამინისტროს მმართველობის სფეროში მოქმედი სსიპ - კიბერუსაფრთხოების ბიურო. მონაცემთა გაცვლის სააგენტო კურირებს ინფორმაციული უსაფრთხოების სეგმენტს (ე.წ. კრიტიკული ინფორმაციული სისტემების სუბიექტებს), ხოლო კიბერუსაფრთხოების ბიურო - თავდაცვის სამინისტროს და თავდაცვის ობიექტებს. ამ ობიექტების სია განისაზღვრება მთავრობის დადგენილებით. აღსანიშნავია, რომ დღეისათვის კრიტიკული ინფორმაციული სისტემების სუბიექტების სია შედგება მხოლოდ საჯარო სექტორის ორგანიზაციებისა და სახელმწიფოს მონაწილეობით შექმნილი ზოგიერთი კომერციული ორგანიზაციისგან (მაგ. საქართველოს რკინიგზა) და არ მოიცავს/არ შედის ისეთი კრიტიკული ორგანიზაციები, როგორიცაა მაგალითად ინტერნეტ სერვის პროვაიდერები და ბანკები.

შემოთავაზებული ცვლილებებით ფართოვდება კრიტიკული ინფორმაციული სისტემების სუბიექტების სია და ის მოიცავს კომერციულ ორგანიზაციებსაც, რაც თავის მხრივ დადებითი მოვლენაა. თავად ორგანიზაციების სია იყოფა სამ ნაწილად/კატეგორიად: პირველი კატეგორია - საჯარო სამსახური, მეორე - ინტერნეტ სერვის პროვაიდერები და კომუნიკაციის კომპანიები, მესამე - კერძო ორგანიზაციები. კანონპროექტით ასევე გათვალისწინებული ახალი

მარეგულირებლის - სახელმწიფო უსაფრთხოების სამსახურის მმართველობის სფეროში შემავალი სსიპ - ოპერატიული ტექნიკური სააგენტო (OTA) შექმნა, რომელსაც დაევალება პირველი და მეორე კატეგორიის სუბიექტებზე ზედამხედველობა, მესამე კატეგორიაზე ზედამხედველობას განხორციელებს მონაცემთა გაცვლის სააგენტო, ხოლო სამხედრო სფეროში უცვლელი რჩება კიბერუსაფრთხოების ბიუროს როლი და ფუნქციები.

იდენტიფიცირებული სისუსტეები

ზემოაღნიშნული ცვლილებებიდან გამომდინარე არსებობს რამდენიმე მნიშნელოვანი მმართველობითი რისკი.

- პროექტით განსაზღვრული მარეგულირებელი ორგანოები (მონაცემთა გაცვლის სააგენტო, ოპერატიულ-ტექნიკური სააგენტო, კიბერუსაფრთხოების ბიურო) არიან კონკრეტული აღმასრულებელი ხელისუფლების ორგანოების დაქვემდებარებაში, ხოლო მათი მანდატი (მარეგულირებელი ფუნქცია) ვრცელდება აღმასრულებელი ხელისუფლების ფარგლებს გარეთ. (მაგ: პარლამენტზე და სასამართლოების სისტემაზე).

- ზოგიერთ ორგანიზაციასთან მიმართებაში უკვე არსებობენ სექტორული მარეგულირებლები, ხოლო კანონპროექტი ამატებს დამატებით კიდევ ერთ მარეგულირებელს. სექტორული მარეგულირებლის არსებობის პირობებში, შესაბამის სექტორში ინფორმაციული უსაფრთხოების საკითხებზე ცალკე მარეგულირებლის შემოყვანა პროცესში არარაციონლაურია როგორც შესაბამისი ბიზნეს ოპერატორის, ისე მარეგულირებლის პერსპექტივიდან;

- უფლებამოსილების და პასუხისგებლობის გამიჯვნა - ერთი და იგივე ორგანო ადგენს თამაშის წესებსაც და ახორციელებს აღსრულებას, აუდიტს და დაჯარიმებას. ორგანიზაციის შიგნით ამ უფლებების და მოვალეობის სეგრეგაცია და მიუკერძოებლების მიღწევა რთულია და ხშირ შემთხვევებში განუხორციელებელი.

- კრიზისული და საომარი სიტუაციების მართვა - კანონში არ არის განსაზღვრული, კიბერუსაფრთხოების მართვის საკითხების რეგულირება კრიზისულ და საომარ სიტუაციაში.

რეკომენდაციები

ცენტრალური მარეგულირებელი

ინფორმაციული უსაფრთხოების უზრუნველსაყოფად კრიტიკული ინფრასტრუქტურის მიმართ უნდა არსებობდეს ინფორმაციული უსაფრთხოების ერთიანი მინიმალური მოთხოვნები. ორგანო რომელიც ადგენს მსგავს მოთხოვნებს (შემდგომში პირობითად **სპეციალური ორგანო**) უნდა იყოს დამოუკიდებელი, აღმასრულებელი ხელისუფლებისგან გამოცალკევებული ერთეული, რომლის საქმიანობაზეც ვრცელდება საპარლამენტო კონტროლი/ანგარიშვალდებულია საქართველოს პარლამენტის წინაშე და რომლის ხელმძღვანელსაც ირჩევს პარლამენტი. მარეგულირებელი ორგანო შეიძლება არსებობდეს ისეთი მანდატით როგორიცაა მაგ. სახელმწიფო ინსპექტორის ან სახელმწიფო აუდიტის სამსახურები.

საჭირო ადამიანური რესურსების სიმწირის პირობებში, პრაქტიკული იმპლემენტაციის გამარტივებისა და არსებული რესურსების ეფექტიანი გამოყენების თვალსაზრისით, შეიძლება მიზანშეწონილი იყოს სპეციალური ორგანოს შექმნა მონაცემთა გაცვლის სააგენტოსა და ოპერატიულ ტექნიკური სააგენტოს შესაბამისი დეპარტამენტების (განყოფილების) ბაზაზე, მათი რესურსების გამოყენებით.

სექტორული მარეგულირებლები

იმის გათვალისწინებით, რომ სახელმწიფოში არსებობენ სექტორული მარეგულირებლები (ეროვნული ბანკი და კომუნიკაციების მარეგულირებელი ეროვნული კომისია), მიგვაჩნია, რომ კანონის მოთხოვნების აღსრულება ამა თუ იმ სექტორში სწორედ მათი მეშვეობით უნდა განხორციელდეს. ერთიანი მინიმალური მოთხოვნების გარდა, სექტორულმა მარეგულირებლებმა შესაძლებელია განსაზღვრონ დამატებითი, სექტორისათვის სპეციფიკური მოთხოვნები.

აქვე აღსანიშნავია, რომ სექტორულ მარეგულირებლებში შესაბამისი რესურსების ნაკლებობაა და დღეისთვის ეს როლი მხოლოდ ეროვნულმა ბანკმა შეიძლება განახორციელოს

ზემოაღნიშნული მიდგომის დანერგვისთვის საჭიროა მარეგულირებელ ორგანოებში განვითარდეს შესაბამისი ადამიანური რესურსები და ინფრასტრუქტურა. ეროვნული ბანკი უკვე ახორციელებს ინფორმაციული უსაფრთოხების მოთხოვნების მართვას კომერციულ ბანკებში და გააჩნია გარკვეული რესურსი ამ მიმართულებით, თუმცა კომუნიკაციების მარეგულირებელ ეროვნულ კომისიას დღეის მდგომარეობით არ გააჩნია შესაბამისი ადამიანური/ საექსპერტო რესურსი.

შესაბამისი რესურსების ეტაპობრივად განვითარებამდე ეს როლი დროებით შეიძლება აიღოს სპეციალურმა ორგანომ.

კრიტიკული ინფრასტრუქტურის ინფორმაციული უსაფრთხოების აუდიტი

სასურველია, რომ ის ორგანო რომელიც წესებს ადგენს, თავად არ ახორციელებდეს ამავე წესების აუდიტს. აუდიტის მიზნებს და კრიტერიუმებს უნდა ადგენდეს **სპეციალური ორგანო**, ხოლო აუდიტის უნდა განახორციელებენ:

1) სახელმწიფო აუდიტის სამსახური - საჯაროს დაწესებულებებში (საჭიროა განვითარდეს შესაბამისი რესურსები აუდიტის სამსახურში).

2) სექტორული მარეგულირებლები - ეთავიანთ სექტორებში.

3) წინასწარ განსაზღვრული სანდო აუდიტორები - სხვა კომერციული სექტორებში;

აუდიტის ანგარიშები და მნიშვნელოვანი აღმოჩენები უნდა შეიკრიბოს **სპეციალური ორგანოს** ერთიან სიტემაში (კომერციული ინტერესების გათვალისწინებით);

კრიზისული და საომარი სიტუაციების მართვა

სასურველია, „ინფორმაციული უსაფრთხოების შესახებ“ კანონში გაიწეროს კრიზისული და საომარი სიტუაციების დროს ინფორმაციული უსაფრთხოების მართვის საკითხები. კრიზისულ /საომარ სიტუაციაში **სპეციალური ორგანო** უნდა გადავიდეს მუშაობის განსაკუთრებულ რეჟიმზე. (შესამუშავებელია და კანონში გასაწერია ორგანოს როლი და პასუხისგებლობები კრიზისებს და საომარი სიტუაციების პირობებში).