USAID FROM THE AMERICAN PEOPLE

IDFI ინფორმაციის თავისუფლების განვითარების ინსტიტუტი

COUNTERPART INTERNATIONAL
In partnership for results that last.

კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები

თბილისი
აგვისტო, 2020

ავტორები:

მარი მალვენიშვილი, კიბერუსაფრთხოების პოლიტიკის მკვლევარი

ნინი ბალარჯიშვილი, მკვლევარი, ინფორმაციის თავისუფლების განვითარების ინსტიტუტი

რედაქტორები:

ლევან ავალიშვილი
თეონა ტურაშვილი

რეცენზია:

ხავიერ რუის დიაზი, პოლიტიკისა და ადვოკატირების მრჩეველი, Counterpart International

კვლევა მომზადდა ინფორმაციის თავისუფლების განვითარების ინსტიტუტის (IDFI) მიერ. კვლევის შინაარსზე პასუხისმგებელია IDFI. კვლევაში გამოთქმული მოსაზრებები არ ასახავს Counterpart International-ის, ამერიკის შეერთებული შტატების საერთაშორისო განვითარების სააგენტოს (USAID) და ამერიკის შეერთებული შტატების მთავრობის შეხედულებებს.

შინაარსი

შესავალი

თანამედროვე მსოფლიოს უსაფრთხოების არქიტექტურაში კიბერუსაფრთხოების სფეროს მზარდი მნიშვნელობა აუცილებელს ხდის საქართველოში მეტი ყურადღება დაეთმოს კიბერუსაფრთხოების განმტკიცებას. საქართველო არის ქვეყანა, რომელიც არაერთხელ გახდა კიბერშპიონაჟისა და სრულმასშტაბიანი კიბერთავდასხმის ობიექტი. შინაგან საქმეთა სამინისტროს სტატისტიკაზე დაყრდნობით, დღითიდღე მატულობს კიბერდანაშაულის რიცხვი. როგორც უკანასკნელი ათწლეულების ტენდენციები გვაჩვენებს, საქართველოში მკვეთრად იზრდება ინტერნეტ მომხმარებლების რაოდენობა და ინტერნეტის გავლენა სახელმწიფო ცხოვრების ყველა ასპექტზე. შესაბამისად, ეფექტიანი კიბერუსაფრთხოების სისტემის გარეშე, ქვეყნის სტაბილურობა და განვითარება შესაძლოა მუდმივი რისკების წინაშე დადგეს. გარდა ამისა, თუ გავითვალისწინებთ იმ გარემოებას, რომ საქართველოს არსებობა და განვითარება უწევს რეგიონში არსებული დაძაბული გეოპოლიტიკური ვითარების ფონზე, სადაც დღითითღე უფრო აქტიურად მოქმედებენ არასახელმწიფო აქტორები, ამავდროულად შეიმჩნევა პოლიტიკური მიზნით კიბერსივრცის გამოყენების მზარდი ტენდენციაც, საქართველო შესაძლოა მივაკუთვნოთ კიბერშეტევების მაღალი რისკის ქვეშ მყოფი ქვეყნების კატეგორიას.

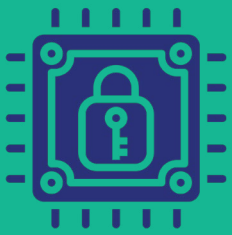
კიბერსაფრთხეების იგნორირება, ან არაადეკვატურად შეფასება ქვეყანას დააყენებს ისეთი რისკების პირისპირ, როგორებიც არის: სახელმწიფო და ეკონომიკური სტრუქტურების მოწყვლადობა; კრიტიკული ინფრასტრუქტურის არასაკმარისი დაცულობა; სამხედრო და ჰიბრიდული საფრთხეებისადმი სისუსტე; თავდაცვისუნარიანობის დაქვეითება. გამომდინარე აქედან, კიბერუსაფრთხოების მაღალ დონეზე უზრუნველყოფა სასიცოცხლოდ აუცილებელია.

კვლევამ აჩვენა, რომ საქართველოს მიერ გატარებული ღონისძიებები და მიმდინარე კიბერპოლიტიკა არასაკმარისია კიბერუსაფრთხოების უზრუნველსაყოფად და თანამედროვე გამოწვევების საპასუხოდ. ვინაიდან, ქვეყანაში არ არის მკაცრად გამიჯნული სახელმწიფო უწყებებს შორის ფუნქცია-მოვალეობები, სრულად დასახვეწია კოორდინაციის, ურთიერთთანამშრომლობისა და ინფორმაციის მიმოცვლის მექანიზმები, არ არის შემუშავებული კრიტიკული ინფრასტრუქტურის სრულყოფილი ნუსხა.

საერთაშორისო გამოცდილება ცხადყოფს, რომ კარგად ორგანიზებული კიბერსივრცის არქიტექტურა, სწორად გადანაწილებული უფლებამოსილებები და ანგარიშვალდებულებისა და კოორდინაციის დახვეწილი მექანიზმები წარმოადგენს კიბერსივრცის გამართული და უსაფრთხო ფუნქციონირების მთავარ წინაპირობას.

კიბერსაფრთხეების დაძლევა, სხვა მრავალ ფაქტორთან ერთად, პოლიტიკურ ნებასა და სწორ მენეჯმენტზეა დამოკიდებული. სწორი მენეჯმენტი, თავის მხრივ, გულისხმობს პასუხისმგებლობების სწორად გადანაწილებას და კოორდინაციის მექანიზმების დახვეწას. როდესაც ქვეყანა მუდმივი კონფლიქტის პირობებში იმყოფება და მასობრივი კიბერშეტევის რისკი მაღალია, ქვეყნის რესურსის მობილიზება უნდა განხორციელდეს არსებული ორგანიზაციული სისტემის დახვეწაზე და გაძლიერებაზე. მით უმეტეს, თუ გავითვალისწინებთ იმ გარემოებას, რომ მოქმედი ორგანიზაციული სისტემა შექმნილია ქვეყნის სტრატეგიული პარტნიორების უშუალო ჩართულობით და სრულად შეესაბამება საერთაშირისოდ აღიარებულ მოდელებს. არსებული რეალობა ცხადყოფს, რომ პრობლემა ორგანიზაციული მოწყობის ნაცვლად, კიბერუსაფრთხოების, როგორც ეროვნული უსაფრთხოების შემადგენელი მნიშვნელოვანი კომპონენტის პრიორიტიზებაშია. ეფექტიანად

დაცული კიბერსივრცის შექმნისთვის აუცილებელია პრობლემისადმი კომპლექსური მიდგომა. ხარვეზების აღმოსაფხვრელად, პირველ რიგში, მნიშვნელოვანია არსებული ნაკლოვანებების იდენტიფიცირება და შესაბამისი ღონისძიებების გატარება.



საქართველოს კიბერუსაფრთხოების არქიტექტურა

ინფორმაციული უსაფრთხოების რეფორმის დეზაღები

2008 წლის რუსეთ–საქართველოს ომის დროს განხორციელებულმა კიბერშეტევებმა, რომელთა მთავარ სამიზნესაც სამთავრობო უწყებები და მედია საშუალებები წარმოადგენდა, საგრძნობლად დააზიანა ქვეყნის კრიტიკული ინფრასტრუქტურა და ნათლად დაგვანახა ამ მიმართულებით მნიშვნელოვანი რეფორმების გატარების აუცილებლობა.

სწორედ 2008 წელს, ესტონელი ექსპერტების დახმარებით, საქართველომ შეადგინა გზამკვლევი (ე.წ. Roadmap) და კიბერსტრატეგიის ჩარჩო. მოგვიანებით, 2011 წელს შეიქმნა **კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი,** რომელსაც საქართველოს კიბერსივრცეში, ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვა დაევალა. პარალელურად, დაიწყო მუშაობა **საქართველოს კანონზე ინფორმაციული უსაფრთხოების შესახებ,** რომელიც ძალაში შევიდა 2012 წელს და რომლის შესაბამისად, დღემდე რეგულირდება კიბერუსაფრთხოების პოლიტიკა, ინფორმაციული უსაფრთხოების სახელმწიფო კონტროლის მექანიზმები, კონტროლის განმახორციელებელი ორგანოების პასუხისმგებლობა და კონტროლის ფარგლები.

ინფორმაციული უსაფრთხოების მართვის სისტემის ინსტიტუციური განაწილება

დღევანდელი მოწესრიგებით, ინფორმაციული უსაფრთხოების წესების შესრულების უზრუნველყოფა და კოორდინაცია წარმოადგენს **ციფრული მმართველობის სააგენტოს (მანამდე, მონაცემთა გაცვლის სააგენტო) კომპეტენციას**[1], თავდაცვის სტრუქტურებში ინფორმაციული უსაფრთხოების მინიმალური სტანდარტის დანერგვასა და დაცვაზე კი თავდაცვის სამინისტროს **კიბერუსაფრთხოების ბიურო** ზრუნავს.[2]

სსიპ - ციფრული მმართველობის სააგენტო (მანამდე, მონაცემთა გაცვლის სააგენტო)

დღეს მოქმედი კანონმდებლობისა და 2016-2018 წლების კიბერუსაფრთხოების სტრატეგიის[3] თანახმად, ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების განსაზღვრასა და ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემაზე პასუხისმგებელ უწყებას წარმოადგენს **ციფრული მმართველობის სააგენტო.** შესაბამისად, აღნიშნული სააგენტოა როგორც **მარეგულირებელი**, ისე პოლიტიკის განხორციელების

1 საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“, მე-3 მუხლი, მე-3 პუნქტი;
2020 წლის 1 მარტის რეორგანიზაციის საფუძველზე, მონაცემთა გაცვლის სააგენტოსა და „სმართ ლოჯიქი“-ს (SMART LOGIC) გაერთიანების შედეგად, ჩამოყალიბდა ახალი სტრუქტურა - ციფრული მმართველობის სააგენტო. 2020 წლის 12 ივნისს მიღებული **საკანონმდებლო ცვლილებების** თანახმად, ახალი ინსტიტუტი წარმოადგენს როგორც მონაცემთა გაცვლის სააგენტოს, ისე SMART LOGIC-ის უფლებამონაცვლეს და ითავსებს ორივე ორგანიზაციის ფუნქციებსა და პასუხისმგებლობებს. შესაბამისად, ინფორმაციული და კიბერუსაფრთხოების განვითარებასა და პოლიტიკის განხორციელებას კოორდინაციას უწევს ციფრული მმართველობის სააგენტო, საკუთარი კომპეტენციისა და უფლებამოსილებების ფარგლებში.

2 საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“, მე- 10[1] მუხლი, 1-ლი პუნქტი

3 საქართველოს მთავრობის 2017 წლის 13 იანვრის №14 დადგენილება საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ. ხელმისაწვდომია **http://gov.ge/files/469_59439_212523_14.pdf**

ზედამხედველობაზე პასუხისმგებელი უწყება.

ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი

სააგენტოს დაქვემდებარებაში ფუნქციონირებს **კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი**, რომელიც საკუთარი კომპეტენციის ფარგლებში, ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვასა და კიბერუსაფრთხოების კუთხით არსებული მნიშვნელოვანი საფრთხეების აღმოფხვრაზეა პასუხისმგებელი.[4]

სახელმწიფო აუდიტის სამსახური

მიუხედავად იმისა, რომ კანონი არ აკონკრეტებს **სახელმწიფო აუდიტის სამსახურის** როლს, სამსახურს გააჩნია ნებისმიერ ორგანიზაციაში IT და ინფორმაციული უსაფრთხოების **აუდიტის ჩატარებისა** და კანონის მოთხოვნების შესაბამისობის დასკვნის საქართველოს პარლამენტისათვის წარდგენის მანდატი.

შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულთან ბრძოლის სამმართველო

2012 წლიდან საქართველოს შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტის დაქვემდებარებაში ფუნქციონირებს **კიბერდანაშაულთან ბრძოლის სამმართველო**, რომელიც პასუხისმგებელია კიბერსივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენაზე, აღკვეთასა და პრევენციაზე, მთელი ქვეყნის მასშტაბით. სამმართველო ასევე წარმოადგენს საერთაშორისო საკონტაქტო პუნქტს, რომელიც ასრულებს საერთაშორისო საპოლიციო თანამშრომლობასთან დაკავშირებულ ფუნქციებს „კიბერდანაშაულის შესახებ“ ევროპის საბჭოს კონვენციის შესაბამისად.

თავდაცვის სამინისტროს სისტემაში შემავალი სსიპ - კიბერუსაფრთხოების ბიურო

2014 წლიდან, თავდაცვის სფეროს კრიტიკული ინფორმაციული სისტემის სუბიექტების უსაფრთხოებასა და კიბერთავდასხმის ან/და კომპიუტერული უსაფრთხოების ინციდენტების განეიტრალებაზე პასუხისმგებელია თავდაცვის სამინისტროს სისტემაში მოქმედი სსიპ - კიბერუსაფრთხოების ბიურო.[5] ბიურო უზრუნველყოფს თავდაცვის სფეროში არსებული ინფრასტრუქტურის შესწავლას, უსაფრთხოების მექანიზმების დანერგვა/განვითარებას.

სახელმწიფო უსაფრთხოების სამსახური

კიბერუსაფრთხოების დაცვის მიმართულებით სახელმწიფო უსაფრთხოების სამსახურის (სუს) როლს მოქმედი კანონმდებლობა არ განსაზღვრავს. ამავდროულად, კიბერუსაფრთხოების მიმართულებით სამსახურის საქმიანობაზე, კიბერინციდენტებისა და შეტე-

4 საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“, მე- 8 მუხლი, 1-ლი პუნქტი;

5 საქართველოს კანონი “ინფორმაციული უსაფრთხოების შესახებ“, მე-101 მუხლი, 1-ლი პუნქტი;

ვების პრევენციისა თუ აღმოფხვრის კუთხით გატარებულ ღონისძიებებზე ყურადღება საერთოდ არ მახვილდება სუს-ის 2018 და 2019 წლების ანგარიშებში. ინფორმაციული და კიბერუსაფრთხოების უზრუნველყოფის მიმართულებით სუს-ის კომპეტენციისა და საქმიანობის შესახებ ზოგადი ინფორმაციის მიღება შეგვიძლია სამსახურის 2015 წლის ანგარიშიდან,[6] რომელშიც ვკითხულობთ: ქვეყნის კიბერსივრცის უსაფრთხოების დაცვა არ განეკუთვნება სამსახურის კომპეტენციას, თუმცა, საფრთხის მასშტაბებისა და მოსალოდნელი შედეგების სიმძიმის გათვალისწინებით, სამსახური ახორციელებს მთელ რიგ ღონისძიებებს აღნიშნული საფრთხეების ნეიტრალიზების, ასევე შედეგების მინიმიზების თვალსაზრისით. გარდა ამისა, სისხლის სამართლის საპროცესო კოდექსის შესაბამისად, სუს-ის **ოპერატიულ-ტექნიკურ სააგენტოს** კომპიუტერული სისტემებთან დაკავშირებული ფარული საგამოძიებო მოქმედებების ჩატარების ექსკლუზიური უფლებამოსილებაც გააჩნია.[7]

საქართველოს ეროვნული ბანკი

კიბერუსაფრთხოების მიმართულებით კომერციული ბანკების დარგობრივ მარეგულირებელს საქართველოს ეროვნული ბანკი წარმოადგენს. ეროვნული ბანკის პრეზიდენტის ბრძანების შესაბამისად დამტკიცებულია კიბერუსაფრთხოების ჩარჩო,[8] რომელიც ეფუძნება ამერიკულ NIST-ს. ჩარჩოს შესაბამისად, ეროვნული ბანკი კომერციულ ბანკებს უწევს ზედამხედველობას, რათა დააკმაყოფილონ ინფორმაციული უსაფრთხოების მათთვის განსაზღვრული მინიმალური სტანდარტი.

სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო

2013 წლის კონსტიტუციური რეფორმის შემდგომ, ეროვნულ უსაფრთხოებასთან დაკავშირებულ საკითხებთან მიმართებით მეტწილად ცენტრალიზებული მიდგომები დაინერგა და კიბერუსაფრთხოების მიმართულებამაც საქართველოს მთავრობის პირდაპირ დაქვემდებარებაში გადაინაცვლა. კერძოდ, კიბერუსაფრთხოების პოლიტიკის ძირითად მაკოორდინირებელ უწყებად განისაზღვრა 2014 წელს ჩამოყალიბებული **სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო.**

კიბერუსაფრთხოების რეგულირების მიზნით, **საბჭოს მოვალეობებში შედიოდა კიბერუსაფრთხოების პოლიტიკის ძირითადი ჩარჩოს შემუშავება და კიბერუსაფრთხოების სისტემის განვითარებასთან დაკავშირებით საქართველოს მთავრობისათვის რეკომენდაციების წარდგენა**. ამავდროულად, საბჭო **კოორდინაციას უწევდა შესაბამის უწყებებს კიბერსაფრთხეების გამოვლენის პროცესში** და შეიმუშავებდა შესაბამის ზომებს საფრთხეების ნეიტრალიზებისა და შემცირების მიმართულებით. კრიზისების მართვის საბჭოს, განსაკუთრებით კრიზისის პერიოდში, ევალებოდა ყველა სააგენტოს მუშაობის კოორდინაცია.

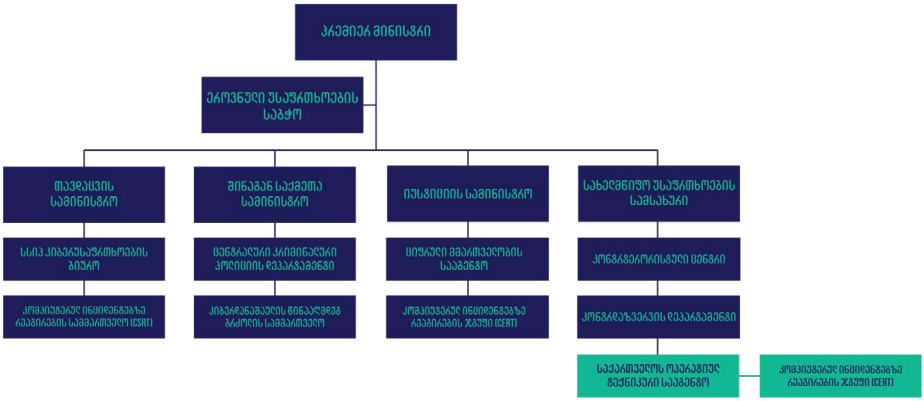
---

6 საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში, 2015. ხელმისაწვდომია **https://bit.ly/3m-9J49G**

7 საქართველოს სისხლის სამართლის საპროცესო კოდექსი, მუხლი 3, ნაწილი 32,მ ქვეპუნქტი „ა“.

8 საქართველოს ეროვნული ბანკის პრეზიდენტის 2019 წლის 22 მარტის №56/04 ბრძანება კომერციული ბანკების კიბერუსაფრთხოების მართვის ჩარჩოს დამტკიცების შესახებ. ხელმისაწვდომია: **https://matsne.gov.ge/document/view/4515476?publication=0**

„ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ“ საქართველოს კანონში[9] შეტანილი ცვლილებების საფუძველზე, 2018 წლის 1-ლი იანვრიდან სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო გაუქმდა და მის ნაცვლად, პრემიერ-მინისტრის დაქვემდებარებაში ჩამოყალიბდა საგანგებო სიტუაციების მართვის სამსახური. 2019 წელს გატარებული საკანონმდებლო ცვლილებების საფუძველზე კი შეიქმნა ეროვნული უსაფრთხოების საბჭო. კანონის შესაბამისად, საბჭოს შექმნის უმთავრეს მიზანია ეროვნული უსაფრთხოებისა და სახელმწიფო ინტერესებისთვის საფრთხის შემცველ საკითხებზე პოლიტიკური გადაწყვეტილებების მომზადების, სტრატეგიულ დონეზე ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის მიზნით, რეკომენდაციებისა და გადაწყვეტილებების მომზადება და პრემიერ-მინისტრის ინფორმირება.[10] ამავე კანონის თანახმად, ინფორმაციული უსაფრთხოება წარმოადგენს ეროვნული უსაფრთხოების პოლიტიკის ერთ-ერთ უმნიშვნელოვანეს მიმართულებას.[11] შესაბამისად, საბჭოს ფუნქციებში შედის ინფორმაციული უსაფრთხოების პოლიტიკის იმპლემენტაციის კოორდინაციაც. საბჭოს ხელმძღვანელობით ხორციელდება კიბერუსაფრთხოების სტრატეგიის პროექტის, როგორც ეროვნული კონცეპტუალური დოკუმენტის შემუშავების პროცესის ორგანიზება, სტრატეგიის პროექტი საქართველოს მთავრობას დასამტკიცებლად წარედგინება სწორედ უსაფრთხოების საბჭოს მხრიდან, ხოლო მის განხორციელებას კოორდინაციას უწევს ციფრული მმართველობის სააგენტო.



9 საქართველოს კანონი ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ. ხელმისაწვდომია **https://matsne.gov.ge/ka/document/view/2764463?publication=9**

10 საქართველოს კანონი “ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ”, მე-191 მუხლი

11 საქართველოს კანონი “ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ”, მე-3 მუხლი

2012 წელს მიღებული კანონის ძირითადი მიმართულებები

ინფორმაციული უსაფრთხოების შესახებ კანონის შესაბამისად, დადგინდა **ინფორმაციული უსაფრთხოების მინიმალური სტანდარტი** (ISO/IEC 27001 საერთაშორისო სტანდარტის ქართულ ენაზე ადაპტირებული ვარიანტი) და მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანებით განისაზღვრა ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები; შემოვიდა „კრიტიკული ინფორმაციული სისტემის სუბიექტის“ ცნება;[12] კრიტიკული ინფრასტრუქტურის სუბიექტებისათვის განისაზღვრა ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები და გაიმიჯნა სამოქალაქო და თავდაცვის სტრუქტურებში ინფორმაციული უსაფრთხოების მაკოორდინირებელი უწყებები.

„კრიტიკული ინფორმაციული სისტემის სუბიექტი“ განიმარტა, როგორც ორგანიზაცია, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის, ეკონომიკური და საზოგადოებრივი უსაფრთხოებისთვის.

მნიშვნელოვანია, რომ დღეს მოქმედი კანონმდებლობით, ინფორმაციული უსაფრთხოების პოლიტიკის იმპლემენტაციის მინიმალური სტანდარტის დანერგვისა და კანონით განსაზღვრული უწყებების წინაშე ანგარიშვალდებულების პასუხისმგებლობა ვრცელდება **მხოლოდ იმ იურიდიულ პირებსა და სახელმწიფო ორგანოებზე, რომლებიც კრიტიკული ინფორმაციული სისტემის სუბიექტებს წარმოადგენენ.**[13]

კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხა დამტკიცებულია საქართველოს მთავრობის 2014 წლის 29 აპრილის დადგენილებით[14] და მოიცავს 39 ორგანიზაციას, მათ შორის, საქართველოს მთავრობისგან ინსტიტუციურად სრულიად დამოუკიდებელ ადმინისტრაციულ ორგანოებს, კერძოდ: საქართველოს პარლამენტს, პრეზიდენტის ადმინისტრაციას, ქალაქ თბილისის მერიას, ცენტრალურ საარჩევნო კომისიას, საქართველოს ეროვნულ ბანკს, საქართველოს რკინიგზას, შპს საქაერონავიგაციასა და სხვა. ცალკე დადგენილებითაა[15] განსაზღვრული თავდაცვის სფეროში მოქმედი კრიტიკული ინფორმაციული სისტემის სუბიექტები.

ინფორმაციული უსაფრთხოების შესახებ კანონის აღსრულებასთან დაკავშირებული გამოწვევები

ინფორმაციული უსაფრთხოების ეფექტური პოლიტიკის გატარება და კომპიუტერული ინციდენტების კუთხით არსებული გამოწვევების აღმოფხვრა, უპირველეს ყოვლისა, ინფორ-

12 საქართველოს კანონი “ინფორმაციული უსაფრთხოების შესახებ”, მე-2 მუხლი, „ზ“ ქვეპუნქტი

13 საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“, მე-3 მუხლი, 1-ლი პუნქტი

14 საქართველოს მთავრობის 2014 წლის 29 აპრილის №312 დადგენილება კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ. ხელმისაწვდომია **https://matsne.gov.ge/ka/document/view/2333175?publication=0**

15 საქართველოს მთავრობის 2014 წლის 29 სექტემბრის №567 დადგენილება თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ. ხელმისაწვდომია **https://matsne.gov.ge/ka/document/view/2521602?publication=0**

მაციული უსაფრთხოების მიმართულებით საკანონმდებლო ბაზის სრულყოფას, კიბერ-უსაფრთხოების გაძლიერების პოლიტიკურ ნებას, გადაწყვეტილების მიმღები პირების მხარდაჭერასა და უწყებათა ინფრასტრუქტურულ თუ საკადრო მზაობას მოით-ხოვს.

ინფორმაციული უსაფრთხოების შესახებ 2012 წლის კანონის აღსრულებასთან დაკავ-შირებული გამოწვევები, უპირველეს ყოვლისა, სწორედ ინფორმაციული უსაფრთხოების სფეროს განვითარების კუთხით რესურსების ნაკლებობას უკავშირდებოდა. გამოწვევები არსებობდა როგორც ინფორმაციული უსაფრთხოების მარეგულირებელი საკანონ-მდებლო აქტებისა და კიბერუსაფრთხოების უზრუნველმყოფი მექანიზმების სრულყოფის, ისე კრიტიკული ინფორმაციული ინფრასტრუქტურის განმსაზღვრელი ნორმატიული ბაზის მიმართულებით. კერძოდ, 2012 წლის კანონი ეფექტურად ვერ ახორციელებდა კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის ფუნქციონირების სამართლებრივ უზრუნველყოფას; კანონის შესაბამისად ვერ განხორციელდა ევროპის საბჭოს 2001 წლის „კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირების შედეგად აღებული ვალდებულებების შესრულება; ამავდროულად, სრულყოფილად არ იყო გაწერილი კიბერუსფრთხოებასთან დაკავშირებული კრიზისული სიტუაციების დროს მოქმედების სარეზერვო გეგმები და პროცედურები.

კანონის დანერგვასა და კოორდინაციასთან დაკავშირებით ერთ-ერთ მთავარ გამოწვე-ვად შეიძლება ჩაითვალოს ის ფაქტი, რომ **იუსტიციის სამინისტროს სსიპ მონაცემთა გაცვლის სააგენტოს (ამჟამად ციფრული მმართველობის სააგენტო) კანონის მოთ-ხოვნების შეუსრულებლობის შემთხვევაში არ გააჩნდა სანქციების დაკისრების არა-ნაირი უფლებამოსილება ან მანდატი.**

ქვეყნის კიბერუსაფრთხოების პოლიტიკის ეფექტიანობა ძირითადად, ხუთი ინდიკატო-რით იზომება, ესენია: საკანონმდებლო ბაზა, ორგანიზაციული მოწყობა, ტექნიკური შესა-ძლებლობები, შესაძლებლობების ამაღლება და თანამშრომლობა. შესაბამისად, საერ-თაშორისო ინდექსებიც აღნიშნულ ინდიკატორებს ეყრდნობა.

დღესდღეობით არსებული რეალობა ცხადყოფს, რომ საქართველომ სათანადოდ ვერ განავითარა კიბერუსაფრთხოების სისტემის კრიტიკულად მნიშვნელოვანი კომპონენტები, რაც კიბერსაფრთხეებზე ეფექტიანი რეაგირების აუცილებელი წინაპირობაა. საერთა-შორისო ინდექსების მიხედვით, გამოწვევად რჩება კიბერუსაფრთხოების სწავლების ინტეგრირება საგანმანათლებლო სისტემაში (დაწყებითი სკოლები, უნივერსიტეტები, სადოქტორო პროგრამები), კიბერინციდენტების რეპორტინგი და კიბერკრიზისის მართვა, ინფორმაციული უსაფრთხოების მართვის სტანდარტის დანერგვა, კიბერსაფრთხეების ანალიზის, ეროვნულ დონეზე კოორდინაციისა და ინფორმაციის მიმოცვლის შესაძლებ-ლობები, საკანონმდებლო და ეროვნული პოლიტიკა.

2012 წელს გატარებული სამართლებრივი რეფორმის არასისტემური ხასიათი და სფეროს განვითარების კუთხით კომპლექსური მიდგომების არარსებობა უარყოფითად აისახა საქართველოს პოზიციაზე ეროვნული კიბერუსაფრთხოების ინდექსის (NCSI)[16] შეფასებაში, რომლის მიხედვითაც ქვეყანამ მე-19 ადგილიდან 47-ე ადგილზე გადაინაცვლა.

ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვისას მენეჯმენტის მხარდაჭერა უმნიშვნელოვანესია როგორც საჯარო, ისე კერძო დაწესებულებაში. განსაკუთრებით, თუ

16 National Cyber Security Index. Available at **https://ncsi.ega.ee/ncsi-index/**

სახელმწიფოში მყიფე კიბერუსაფრთხოების გარემო და ნაკლებად დაცული მექანიზმებია, აუცილებელია სფეროს პრიორიტეტულ მიმართულებად გამოცხადება და სახელმწიფო თუ საერთაშორისო მხარდაჭერის უზრუნველყოფა სისტემური რეფორმების გატარების პროცესში. რეალურად, კანონის აღსრულების ერთ-ერთ უმთავრეს გამოწვევას სახელმწიფო პოლიტიკის ძირითად მიმართულებებს შორის სწორედ ინფორმაციული უსაფრთხოების სფეროს არაპრიორიტეტულობა წარმოადგენდა. ინფორმაციული უსაფრთხოების შესახებ კანონმა ვერ გაამართლა როგორც კანონის დანერგვის, ისე მისი აღსრულებისა და იმპლემენტაციის მონიტორინგის ეტაპზე.

გახშირებული კიბერშეტევების ფონზე, რის ნათელ მაგალითადაც შეგვიძლია მოვიყვანოთ 2019 წლის ოქტომბერში განხორციელებული თავდასხმა,[17] რომლის შედეგადაც გაითიშა საქართველოს პრეზიდენტის, სასამართლოების, საკრებულოებისა და მედიასაშუალებების საიტები, ნათელია, რომ კიბერუსაფრთხოებაზე ზრუნვა სახელმწიფოს ერთ-ერთი მთავარი პრიორიტეტი უნდა გახდეს. მაღალტექნოლოგიური შეტევების თავიდან არიდებისა და საფრთხეების მინიმიზაციის მიმართულებით კი აუცილებელია გადაიდგას ქმედითი ნაბიჯები.

IDFI-მ სახელმწიფო აუდიტის სამსახურიდან 2013-2020 წლებში „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის აღსრულებასთან დაკავშირებით, კრიტიკული ინფორმაციული სისტემების სუბიექტების შემოწმების აქტები და სამსახურის მიერ გაცემული რეკომენდაციები გამოითხოვა. **აუდიტის დასკვნიდან ნათლად იკვეთება, რომ კიბერუსაფრთხოების პოლიტიკის დაცვა და კანონის მოთხოვნების იმპლემენტაცია კრიტიკული ინფორმაციის სუბიექტებად განსაზღვრულ 39 სამთავრობო დაწესებულებაში პრიორიტეტს არ წარმოადგენს.** სამსახურების უმრავლესობის მხრიდან, ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები, აგრეთვე, ინფორმაციული უსაფრთხოების პოლიტიკა არ იყო დამტკიცებული, ხოლო ინფორმაციული უსაფრთხოების მენეჯერი (ასეთის არსებობის შემთხვევაში) წარმოადგენდა ფორმალურ თანამდებობას/პოზიციას და ვერ პასუხობდა კანონით გათვალისწინებულ მოთხოვნებს.

აუდიტის დასკვნიდან იკვეთება, რომ საჯარო უწყებათა უმრავლესობა ვერ აკმაყოფილებს ინფორმაციული უსაფრთხოების მინიმალურ სტანდარტებს. ამასთან, შეიმჩნევა სფეროს რეგულირების მიზნით ქმედითი ნაბიჯების სიმცირე. შესაბამისად, არაეფექტურად ფუნქციონირებს და მხოლოდ ფორმალურად არსებობს კონტროლის მექანიზმები. თვალსაჩინოებისთვის შეგვიძლია მოვიყვანოთ რამდენიმე მაგალითიც:

1. სახელმწიფო ვალის მართვის ინფორმაციული სისტემების ეფექტიანობის აუდიტის დასკვნიდან ირკვევა, რომ სამსახურის მიერ შემუშავებული ინფორმაციული უსაფრთხოების პოლიტიკის სამუშაო ვერსია არ არის დამტკიცებული ხელმძღვანელობის მიერ და ვერ პასუხობს ინფორმაციული უსაფრთხოების მინიმალურ საკანონმდებლო მოთ-ხოვნებს.

2. განათლების მართვის ინფორმაციული სისტემების აუდიტის დასკვნიდან გამოიკვეთა, რომ აშკარა პრობლემებია ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს)

17 “I’LL BE BACK - ბოლო ათი წლის ყველაზე მასშტაბური კიბერთავდასხმა”. რადიო თავისუფლება. ხელმისაწვდომია **https://bit.ly/2RdyBM0**

გავრცელების სფეროს, მმართველობისა და მონიტორინგის ფუნქციების გამიჯვნისა და იუმს-ის დანერგვის პროცესების შესაბამისი ადამიანური რესურსებით უზრუნველყოფის მიმართულებით.

3. სახელმწიფო პენსიის ადმინისტრირების ინფორმაციული სისტემის აუდიტის დასკვნა გვიჩვენებს, რომ სოციალური მომსახურების სააგენტოს არ აქვს შეფასებული სისტემის უწყვეტობასთან დაკავშირებული რისკები და დანერგილი შესაბამისი კონტროლის მექანიზმები. აღნიშნული პრობლემა კი განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცული ხაზით გადაცემის პრობლემურობაში აისახება, თუნდაც, სპეციალური პენიტენციური სამსახურიდან განსაკუთრებული კატეგორიის პერსონალური მონაცემების მიღების პროცესში დაუცველი საკომუნიკაციო არხით სარგებლობაში, რაც სრულად ეწინააღმდეგება საკანონმდებლო ჩარჩოსა და მინიმალური სტანდარტის მოთხოვნებს.

უმნიშვნელოვანესია, რომ სახელმწიფო აუდიტის სამსახურის რეკომენდაციები მიემართება სწორედ კრიტიკული ინფორმაციული სისტემის სუბიექტებს და მოითხოვს არსებული საკანონმდებლო ნორმებით დადგენილი ინფორმაციული უსაფრთხოების მართვის სისტემის შემუშავებასა და პრაქტიკაში დანერგვას. **სახელმწიფო აუდიტის სამსახური, რეკომენდაციის სახით, საქართველოს მთავრობას სთავაზობს:**

- **მონაცემთა გაცვლის სააგენტოს (ამჟამად, ციფრული მმართველობის სააგენტოს) მიენიჭოს დამატებითი უფლებამოსილება ინფორმაციული უსაფრთხოების საკანონმდებლო მოთხოვნების შესრულების უზრუნველსაყოფად, მათ შორის, კრიტიკული ინფორმაციული სისტემის სუბიექტების მიმართ სანქციის გამოყენების შესაძლებლობა;**

- კრიტიკული ინფორმაციული სისტემის სუბიექტების მიმართ **სანქციის გამოყენების მექანიზმის დანერგვა განხორციელდეს მხოლოდ საერთაშორისო პრაქტიკის შესაბამისად და საერთაშორისო გამოცდილებაზე დაყრდნობით;**

- **მოხდეს კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის იდენტიფიცირების რელევანტური მექანიზმისა და კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის პერიოდული გადახედვის მექანიზმის დანერგვა.**

აუდიტის დასკვნის ანალიზიდან დასტურდება, რომ სახელმწიფოში უკვე არსებობს ცოდნა და გამოცდილება ინფორმაციული აუდიტის ჩატარებისა და ინფორმაციული უსაფრთხოების სისტემის მენეჯმენტის მონიტორინგის მიმართულებით. თუმცა, ჩამოთვლილი რეკომენდაციები და სახელმწიფო აუდიტის სამსახურის როლი საერთოდ არ არის გათვალისწინებული 2019 წლის ოქტომბერში ინიცირებულ კანონპროექტში[18] „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის შესახებ, რომელსაც კვლევის შემდეგ ნაწილებში განვიხილავთ.

ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების ეფექტური სისტემის ჩამოყალიბება მხოლოდ იმ შემთხვევაში გახდება შესაძლებელი, თუ სამართლებრივი რეფორმა დაეყრდნობა პრაქტიკაში გამოკვეთილი პრობლემების სიღრმისეულ ანალიზს, საერთაშორისო სამართლებრივი ჩარჩოს კვლევას და მოხდება ეროვნული მიდგომების

18 კანონპროექტი : „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის შესახებ“. ხელმისაწვდომია **https://info.parliament.ge/#law-drafting/18874**

საუკეთესო გამოცდილებასთან ჰარმონიზება. საკანონმდებლო ცვლილებებზე მუშაობის პროცესი და მთლიანად სფეროს მენეჯმენტის ახალი რეალობა, **აუცილებელია, ეფუძნებოდეს პრობლემების ანალიზსა და სახელმწიფოში სფეროს რეგულირების კუთხით უკვე დაგროვილ ცოდნას.** ინფორმაციული უსაფრთხოების სისტემის მართვისა და შეფასების სპეციფიურობიდან გამომდინარე, სასურველი იქნებოდა, სახელმწიფო აუდიტის სამსახურში უკვე არსებული ადამიანური და თეორიული რესურსის გამოყენება და **ზემოთ ჩამოთვლილი რეკომენდაციების გათვალისწინება.**

კანონის პროექტი „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის შესახებ და მასთან დაკავშირებული გამოწვევები

საკანონმდებლო ცვლილებების მიმოხილვა/შეჯამება

ინფორმაციული უსაფრთხოების კანონზე მუშაობა 2019 წლის 2 ოქტომბერს განახლდა, მას შემდეგ, რაც საქართველოს პარლამენტის წევრმა, ირაკლი სესიაშვილმა „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის შესახებ ახალი საკანონმდებლო ინიციატივა წარადგინა. კანონპროექტს ფართო კრიტიკა და დიდი გამოხმაურება მოჰყვა საკითხის ექსპერტების, არასამთავრობო ორგანიზაციებისა და კერძო სექტორის მხრიდან.

წარმოდგენილი კანონპროექტი კრიტიკის ობიექტი რამდენიმე მნიშვნელოვანი გარემოების გამო გახდა: 1. კანონპროექტით შემოტანილი ცვლილებები წარმოშობს ინფორმაციული უსაფრთხოების სისტემის დაუბალანსებელი კონტროლის რისკს; 2. საკანონმდებლო ცვლილებები არ ითვალისწინებს საერთაშორისო პრაქტიკასა და გამოცდილებას; 3. ცვლილებების ინიცირებას წინ არ უძღოდა ფართო კონსულტაციები დაინტერესებულ მხარეებთან, რის გამოც ქვეყნის კიბერუსაფრთხოების არქიტექტურა საერთო კონსესუსის გარეშე იცვლება.

კანონპროექტმა დარეგისტრირებიდან დღემდე გრძელი გზა გაიარა. დაინტერესებულ მხარეებთან პრინციპულ საკითხებზე შეუთანხმებლობის გამო, საკანონმდებლო ცვლილებები მესამე მოსმენიდან მეორე მოსმენის რეჟიმსაც დაუბრუნდა.[19] დღეს არსებული ვერსია მნიშვნელოვნად განსხვავდება თავდაპირველად ინიცირებული ვარიანტისაგან, თუმცა, კვლავ მოიცავს პრობლემურ გარემოებებს, რაც კანონის ეფექტურად აღსრულების კუთხით საკმაოდ ბევრ კითხვას ბადებს.

ინფორმაციული უსაფრთხოების შესახებ კანონში ცვლილებები 3 მთავარი მიმართულებით ხორციელდება: 1. ცვლილებები ეხება კრიტიკული ინფორმაციული სისტემის სუბიექტების კატეგორიზაციას, კანონის მოქმედების არეალი ფართოვდება და მოიცავს კერძო სექტორის სუბიექტებსაც; 2. იცვლება ინფორმაციული უსაფრთხოების სისტემის კოორდინაციისა და მენეჯმენტის სახელმწიფო ღერძი; 3. იცვლება კრიტიკული ინფორმაციული სისტემის სუბიექტების მხრიდან საინფორმაციო და კიბერუსაფრთხოების უზრუნველყოფის მაკოორდინირებელი და ზედამხედველი უწყება.

კრიტიკული ინფორმაციული სუბიექტების კატეგორიზაცია

საკანონმდებლო ცვლილებების მთავარ მიმართულებას წარმოადგენს კრიტიკული ინფორმაციული სისტემების სუბიექტების ახალი კატეგორიზაცია და მათ მიმართ კონტროლისა და ადმინისტრაციულ-სამართლებრივი პასუხისმგებლობის დიფერენცირებული მიდგომების გამოყენება. თუმცა, კანონპროექტიდან ნათლად არ იკვეთება კრიტიკული ინფორმაციული სუბიექტების კატეგორიზაციის საფუძვლები და კრიტერიუმები.

19 “ინფორმაციული უსაფრთხოების შესახებ კანონპროექტი მეორე მოსმენის რეჟიმს დაუბრუნდა”. ინფორმაციის თავისუფლების განვითარების ინსტიტუტი (IDFI). ხელმისაწვდომია **https://idfi.ge/ge/idfis-statement-about-the-draft-law-on-information-security**

ცვლილებები ითვალისწინებს კრიტიკული ინფორმაციული სუბიექტების დაყოფას 3 კატეგორიად:

ა) **პირველი კატეგორიის** სუბიექტებში მოხვდებიან სახელმწიფო ორგანოები, დაწესებულებები, საჯარო სამართლის იურიდიული პირები და სახელმწიფო საწარმოები;

ბ) **მეორე კატეგორიის** სუბიექტებში მოხვდებიან ელექტრონული კომუნიკაციების კომპანიები;

გ) **მესამე კატეგორიის** სუბიექტებში მოიაზრებიან ისეთი კერძო სამართლის იურიდიული პირები, მაგალითად, ბანკები და ფინანსური ინსტიტუტები.

ინფორმაციული უსაფრთხოების პოლიტიკის რეგულირებაში გაჩნდა ახალი სუბიექტი, ოპერატიულ-ტექნიკური სააგენტო (OTA), რომელიც სახელმწიფო უსაფრთხოების სამსახურის (სუს) სსიპ-ია. OTA გაუწევს კოორდინირებას პირველ და მეორე კატეგორიაში შესულ ორგანიზაციებს, ციფრული მმართველობის სააგენტოს მონაცემთა გაცვლის სააგენტოს (ყოფილი, მონაცემთა გაცვლის სააგენტოს) რეგულირების სფეროში კი ნაწილობრივ რჩება მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტები, რამდენადაც კომერციული ბანკების ინფორმაციული უსაფრთხოების უზრუნველყოფის ზედამხედველობასა და რეგულირებას კოორდინაციას გაუწევს ეროვნული ბანკი.

მიუხედავად იმისა, რომ კანონპროექტი გვთავაზობს განსხვავებულ მიდგომებს პირველი, მეორე და მესამე კატეგორიის სუბიექტების პასუხისმგებლობისა და ინფორმაციული უსაფრთხოების სისტემის მართვის ზედამხედველობის მიმართულებით, პრობლემური და ბუნდოვანია შემდეგი ძირითადი ასპექტები:

- შემოთავაზებული ცვლილებებით, პირველი კატეგორიის სუბიექტების შემთხვევაში, ოპერატიულ-ტექნიკურ სააგენტოს ეძლევა შესაძლებლობა, ჰქონდეს სრული წვდომა დაწესებულებების ინფორმაციულ აქტივებზე, ინფორმაციულ სისტემებსა და ინფრასტრუქტურაზე, რამდენადაც, კომპიუტერული ინციდენტების იდენტიფიცირებისთვის თავად ენიჭება ამ დაწესებულებებში განთავსებულ სენსორისა და ქსელის კონტროლის ბერკეტი.

- ბუნდოვანია, რა პრინციპით განისაზღვრნენ კერძო სექტორის წარმომადგენელი ორგანიზაციები მეორე და მესამე კატეგორიის სუბიექტებად. მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტმა, ანუ სატელეკომუნიკაციო კომპანიამ, ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები განსახილველად უნდა წარუდგინოს ოპერატიულ ტექნიკურ სააგენტოს, მესამე კატეგორიის სუბიექტებზე ზედამხედველობას ინარჩუნებს სექტორული მარეგულირებელი ეროვნული ბანკის სახით.

- ელექტრონული კომუნიკაციის კომპანიების კრიტიკული ინფორმაციული სისტემის სუბიექტების კატეგორიად გამოყოფა პირდაპირ წინააღმდეგობაში მოდის ქსელებისა და ინფორმაციული სისტემების (Network and Information Systems (NIS)) დირექტივის ცალკეულ მოთხოვნებთან (რაზეც დეტალურად საუბარი გვექნება საკანონმდებლო ცვლილებების დირექტივასთან და ასოცირების ხელშეკრულებასთან შესაბამისობის ქვეთავში).

- მეორე და მესამე კატეგორიის სუბიექტების დამატებამ კრიტიკული ინფორმაციული

სისტემის სუბიექტების იერარქიაში შესაძლებელია გამოიწვიოს გაზრდილი ბიუროკრატია კერძო სექტორის წარმომადგენლებისათვის. კერძოდ, გარკვეულ შემთხვევებში, ბანკები და ფინანსური ინსტიტუტები ინარჩუნებენ ციფრული მმართველობის სააგენტოსადმი გარკვეულ ანგარიშვალდებულებას. შესაბამისად, იკვეთება ორ მარეგულირებელს, ეროვნულ ბანკსა და ციფრული მმართველობის სააგენტოს შორის რიგ ასპექტებში უფლება-მოვალეობების დუბლირების შესაძლებლობა.

სახელმწიფო უსაფრთხოების სამსახურის სსიპ ოპერატიულ-ტექნიკური სააგენტოს გაზრდილი მანდატი

კანონის მოქმედი რედაქციით მიღება, სახელმწიფო უსაფრთხოების სამსახურს აძლევს სამართლებრივ ბერკეტს, ჰქონდეს მაქსიმალური წვდომა აღმასრულებელი, საკანონმდებლო, სასამართლო ხელისუფლებისა და კერძო სექტორის ზოგიერთი სუბიექტის ინფორმაციულ აქტივზე საზოგადოებრივი ზედამხედველობის, ანგარიშვალდებულებისა და გამჭვირვალობის ეფექტური მექანიზმების გარეშე.

კერძოდ, კარდინალურად იცვლება არსებული კიბერუსაფრთხოების არქიტექტურა და სახელმწიფო უსაფრთხოების სამსახურის სსიპ ოპერატიულ - ტექნიკური სააგენტო (OTA) ფაქტობრივად ხდება საინფორმაციო და კიბერუსაფრთხოების უზრუნველყოფის მთავარი მაკოორდინირებელი და ზედამხედველი უწყება პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციის სუბიექტების შემთხვევაში, რამდენადაც, OTA-ს ენიჭება ფართო უფლებამოსილებები შემდეგი მიმართულებებით:

- ქსელური ნაკადის მონიტორინგის მიზნით, განახორციელოს პირველი და მეორე კატეგორიის (თანხმობის არსებობის შემთხვევაში) კრიტიკული ინფორმაციული სისტემის სუბიექტების ქსელური სენსორის კონფიგურირება და მართვა;
- მოთხოვნისთანავე მიიღოს წვდომა ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე, თუ ამგვარი წვდომა აუცილებელია მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე რეაგირებისთვის პირველი და მეორე კატეგორიის სუბიექტების შემთხვევაში;
- სავალდებულო წესით, გეგმიური ან არაგეგმიური გზით განახორციელოს საინფორმაციო ტექნოლოგიური ინფრასტრუქტურის შემოწმება;
- შემოწმების შედეგად შემუშავებული დასკვნის შეუსრულებლობის შემთხვევაში განსაზღვროს ადმინისტრაციულ სამართლებრივი პასუხისმგებლობა/ სანქცია;
- პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტებისათვის კანონქვემდებარე აქტით დაადგინოს ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები;
- განიხილოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების შემთხვევაში;

- კრიტიკული ინფორმაციული სისტემის სუბიექტისგან გამოითხოვოს ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავებასთან, დანერგვასთან, მონიტორინგსა და გაუმჯობესებასთან დაკავშირებული ინფორმაცია.

შედეგად, სუს-ის სსიპ ოპერატიულ-ტექნიკური სააგენტოს (OTA), პირველი და მეორე კატეგორიის სუბიექტების შემთხვევაში, მიენიჭება მარეგულირებლის, აკრედიტაციის გამტარებლის და აღმასრულებლის ფუნქციები.

გასათვალისწინებელია, რომ პირველ მოსმენაზე წარმოდგენილი კანონპროექტი მიუღებელი აღმოჩნდა მესამე კატეგორიის სუბიექტებისათვის (ფინანსური ინსტიტუტებისთვის), რამდენადაც კერძო ფინანსური ინსტიტუტების ინფორმაციული აქტივები, ფაქტობრივად, დგებოდა ძალოვანი უწყების მხრიდან გაკონტროლებისა და ზედამხედველობის პირდაპირი რისკის ქვეშ.

ამჟამად შემოთავაზებულ ვერსიაში, მესამე კატეგორიის სუბიექტები, კერძოდ, კომერციული ბანკები და კერძო საფინანსო ინსტიტუტები რჩებიან ეროვნული ბანკის, როგორც სექტორული მარეგულირებლის ზედამხედველობის ქვეშ და მხოლოდ მინიმალური ანგარიშვალდებულება აკისრიათ ციფრული მმართველობის სააგენტოს წინაშე. რაც ეროვნული ბანკის მხრიდან წარდგენილი, პენეტრაციის/აუდიტის ტესტის ჩატარებაზე უფლებამოსილი ორგანიზაციების ავტორიზაციას, პენეტრაციის ტესტის დასკვნის ციფრული მმართველობის სააგენტოსათვის გაგზავნაზე და შიდა პოლიტიკის დოკუმენტების გაცნობაზე ვრცელდება.

თუმცა, განახლებულ ვერსიაში შეტანილი ცვლილებები არ შეეხო სატელეკომუნიკაციო სექტორს (მეორე კატეგორიის სუბიექტებს). შესაბამისად, ელექტრონული კომუნიკაციის კომპანიების ინფორმაციული უსაფრთხოების სისტემის მართვის კოორდინაცია და ზედამხედველობა OTA-ს ქოლგის ქვეშ რჩება. ოპერატიულ-ტექნიკური სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი (CERT.OTA.GOV.GE), უფლებამოსილი ხდება, კომპიუტერული ინციდენტის განმეორების საფრთხის თავიდან აცილების მიზნით, იმპერატიულად მოითხოვოს ელექტრონული კომუნიკაციის კომპანიისაგან მის ინფრასტრუქტურაში მსგავსი კომპიუტერული ინციდენტების იდენტიფიცირებისა და ნეიტრალიზებისთვის აუცილებელი ღონისძიებების განხორციელება. ამ ვალდებულების შეუსრულებლობა იწვევს ადმინისტრაციულ-სამართლებრივ პასუხისმგებლობას, რამაც თავის მხრივ, შესაძლებელია მეორე კატეგორიის სუბიექტები უფრო მოწყვლადი გახადოს ოპერატიულ-ტექნიკურ სააგენტოსთან ურთიერთობაში და ჯარიმის თავიდან აცილების მიზნით, მათ საკუთარი ნებით მისცენ ოპერატიულ ტექნიკურ სააგენტოს წვდომა საკუთარ ინფრასტრუქტურასთან, მათ შორის ქსელურ სენსორებთან. ხსენებული ფაქტორები კი ზრდის სახელმწიფო უსაფრთხოების სამსახურის მხრიდან, თანამედროვე ტექნოლოგიების გამოყენებით, განუსაზღვრელ პირთა წრის მიმართ ინფორმაციის, მათ შორის, განსაკუთრებული კატეგორიის მონაცემების მოპოვების, დამუშავებისა და შესწავლის რისკს.

სახელმწიფო უსაფრთხოების სამსახური, რეალურად, წარმოადგენს ძალოვანი უწყებას, რომელსაც, უსაფრთხოების მიზნებიდან გამომდინარე, გააჩნია პირდაპირი ინტერესი, რომ ჰქონდეს მაქსიმალური წვდომა სხვადასხვა ინფორმაციულ ინფრასტრუქტურაზე. იგი ადვილად შეძლებს ამ ინტერესის დაკმაყოფილებას, თუ აღჭურვილი იქნება კანონქვემდებარე აქტების გამოცემის სამართლებრივი მექანიზმებით.

თუ გავითვალისწინებთ არსებულ ჰიბრიდულ საფრთხეებსა და კიბერთავდასხმების გაზრდილ რისკს, **კანონპროექტის მიღების მიზანს უნდა წარმოადგენდეს არა პრევენციული ღონისძიებების მოტივით, ინფორმაციული სისტემისა და აქტივების კონტროლის ფარგლებში მოქცევა, არამედ მსგავსი ინციდენტების გამოძიებისა და აღმოფხვრის მექანიზმების გაძლიერება.** წარდგენილი ცვლილებები კი მთელ რიგ ინსტიტუციურ და ორგანიზაციულ შეუსაბამობას წარმოქმნის, კერძოდ:

ა) იზრდება პირველი და მეორე კატეგორიის სუბიექტების ინფორმაციულ აქტივებზე დაუსაბუთებელი წვდომისა და დაცული ინფორმაციის დამუშავების რისკი, რამდენადაც, OTA-ს ეძლევა შესაძლებლობა, გააჩნდეს **პირდაპირი წვდომა საკანონმდებლო, აღმასრულებელი თუ სასამართლო ხელისუფლების, ცალკეული საჯარო უწყებების, მათ შორის ცესკოს, ასევე სატელეკომუნიკაციო სექტორის ინფორმაციულ სისტემებზე და არაპირდაპირი წვდომა სისტემებში დაცულ პერსონალურ** და **კომერციულ ინფორმაციაზე.**

ბ) კანონპროექტის საფუძველზე, ძალოვან უწყებას ენიჭება სამართლებრივი ბერკეტი, სასამართლოს ნებართვის გარეშე ჰქონდეს წვდომა პერსონალურ მონაცემებთან, რამდენადაც, ნორმათა ბუნდოვანება აჩენს პერსონალურ მონაცემთა არაკანონიერად და არაპროპორციულად დამუშავების რეალურ საშიშროებას.

საკანონმდებლო ცვლილებების შესაბამისობა ევროკავშირთან გაწერილი ასოცირების ხელშეკრულების მოთხოვნებთან

ინფორმაციული უსაფრთხოების შესახებ კანონში ინიცირებული ცვლილებებით **შემოთავაზებული რეგულირების ჩარჩო წინააღმდეგობაში მოდის ქსელებისა და ინფორმაციული სისტემების (Network and Information Systems (NIS)) დირექტივის ცალკეულ მოთხოვნებთან. დირექტივის თანახმად, წევრ სახელმწიფოებს ევალებათ კიბერუსაფრთხოების ეროვნული სტრატეგიის შემუშავება და იმპლემენტაცია.** სტრატეგია უნდა მოიცავდეს უსაფრთხოების ერთიან სტანდარტს, სტრატეგიის დანერგვის საერთო პოლიტიკას და სავალდებულოდ შესასრულებელ რეგულაციებს.

დირექტივის მოთხოვნაა, სტრატეგია განსაზღვრავდეს: მმართველობით ჩარჩოს, რეაგირებისა და სწრაფი აღდგენის ღონისძიებებს, უსაფრთხოების მიმართულებით საჯარო და კერძო სექტორის თანამშრომლობის გეგმას, უსაფრთხოების მიმართულებით ინფორმირებულობის ამაღლების პროგრამებს, რისკების შეფასების გეგმას და სტრატეგიის იმპლემენტაციაზე პასუხისმგებელი პირებისა და ორგანიზაციების სიას.

განსაკუთრებით მნიშვნელოვანია **NIS დირექტივის დამოკიდებულება კრიტიკული ინფორმაციული სისტემის სუბიექტების კატეგორიზაციასთან დაკავშირებით.** დირექტივა გამოყოფს სუბიექტების ორ კატეგორიას და ადგენს **განსხვავებულ მიდგომებსა და ვალდებულებებს ძირითადი სერვისების ოპერატორებისა და ციფრული მომსახურების მიმწოდებლებისათვის.** დირექტივა, ასევე, მოუწოდებს სახელმწიფოებს მიიღონ ობიექტური და რაოდენობრივი ეროვნული კრიტერიუმები კრიტიკული ინფორმაციული სისტემის ობიექტების დასადგენად, რომლებზეც გავრცელდება უსაფრთხოების ვალდებულებები და მოთხოვნები.

დირექტივაში ასევე ხაზგასმულია, რომ **NIS-ის მიზნებისათვის ციფრული მომსახურების მიმწოდებლებად არ ითვლებიან ის ციფრული მომსახურების მიმწოდებელი პირები და ორგანიზაციები, რომლებიც მიეკუთვნებიან „მიკრო საწარმოებისა და მცირე საწარმოების (გააჩნია მიკრო და მცირე ბიზნესის სტატუსი)“ კატეგორიას.** მსგავსი სუბიექტები არ ექვემდებარებიან დირექტივით განსაზღვრულ რეგულაციებს და წესებს უსაფრთხოების სტანდარტისა და კომპიუტერული ინციდენტის შეტყობინების მიმართულებით. ორგანიზაციისათვის მიკრო ან მცირე საწარმოს სტატუსის მინიჭების საფუძვლები განსაზღვრულია 2003 წლის ევროკომისიის რეკომენდაციაში.

დირექტივის შესაბამისად, დადგენილ უსაფრთხოების სტანდარტებსა და ინციდენტების შეტყობინების ვალდებულებას არ ექვემდებარებიან სატელეკომუნიკაციო კომპანიები. მნიშვნელოვანია აღინიშნოს ისიც, რომ დირექტივის თანახმად, სატელეკომუნიკაციო კომპანიები უკვე წარმოადგენენ ელექტრონული საკომუნიკაციო ქსელებისა და მომსახურებების ზოგადი მარეგულირებელი ჩარჩოს შესახებ დირექტივა №2002/21/EC-ის სუბიექტებს და მათზე არ ვრცელდება NIS დირექტივა.

საგულისხმოა, რომ საქართველოს მთავრობის მიერ ჯერ **არ დამტკიცებულა საქართველოს კიბერუსაფრთხოების ახალი ეროვნული სტრატეგია,** რომლის შემუშავებაშიც საერთაშორისო საზოგადოება აქტიურად იყო ჩართული. სტრატეგიის არსებული სამუშაო ვერსიის სამოქმედო გეგმით გათვალისწინებული რიგი აქტივობები წინააღმდეგობაში მოდის კანონპროექტით შემოთავაზებული ცვლილებებთან. კერძოდ:

- სტრატეგიის სამოქმედო გეგმის ერთ-ერთ აქტივობად, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონისა და კანონქვემდებარე აქტების დახვეწა, სწორედ **NIS დირექტივასთან ჰარმონიზაციის მიზნით განისაზღვრა.** მაშინ როცა, კანონპროექტით შემოთავაზებული სუბიექტების კატეგორიზაციის ცალკეული ელემენტები (მაგალითად, სატელეკომუნიკაციო კომპანიებზე კიბერუსაფრთხოების მოთხოვნების გავრცელება) წინააღმდეგობაშია დირექტივის მოთხოვნებთან;

- სტრატეგიის სამუშაო ვერსიით, მარეგულირებელი ჩარჩოს დახვეწასა და დირექტივასთან ჰარმონიზაციაზე პასუხისმგებელ უწყებას მონაცემთა გაცვლის სააგენტო (ამჟამად, ციფრული მმართველობის სააგენტო) წარმოადგენდა, ხოლო სსიპ „კიბერუსაფრთხოების ბიურო“ და სახელმწიფო უსაფრთხოების სამსახური მხოლოდ პარტნიორ უწყებებად მოიაზრებოდნენ. კანონპროექტის მიხედვით კი, სუს-ი, ქვეყნის კიბერუსაფრთხოების არქიტექტურის ერთ-ერთ მთავარ აქტორად იქცევა.

- სტრატეგიის სამოქმედო გეგმის აქტივობების შესრულების ვადად 2021 წლის III კვარტალია დადგენილი, შესაბამისად, კანონის დამტკიცება 2020 წლის სექტემბერში მთლიანად შეცვლის სტრატეგიის პრინციპულ და მნიშვნელოვან ნაწილს.

აქედან გამომდინარე, აშკარაა, რომ კანონპროექტი, შემოტანილი რეგულაციებით, წინააღმდეგობაში მოდის NIS დირექტივის ცალკეულ მოთხოვნებთან, ასოცირების ხელშეკრულებით ნაკისრ ვალდებულებებსა და ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის (General Data Protection Regulation (GDPR)) პრინციპებთან პერსონალური მონაცემების დამუშავებასთან დაკავშირებით გათვალისწინებული პროცედურების ჭრილში. კანონპროექტის შემუშავების პროცესში არ ყოფილა გათვალისწინებული ხსენებულ რეგულაციებთან შესაბამისობის უზრუნველყოფა და ამ მიზნით, დღემდე შესაბამისი ღონისძიებები არ გატარებულა.

კანონპროექტის შემუშავების პროცესში დაინტერესებულ მხარეთა ჩართულობის ნაკლებობა

კანონპროექტის შემუშავების პროცესი არ გახლდათ ინკლუზიური. ცვლილებების ინიცირებას წინ არ უძღოდა დაინტერესებულ მხარეთა, მათ შორის, სამოქალაქო საზოგადოების, დარგის სპეციალისტებისა და კერძო სექტორის მოსაზრებების გაცნობა. ასევე, უცნობია, ცვლილებების შემუშავებამდე მოხდა თუ არა საერთაშორისო პრაქტიკისა და სტანდარტების სიღრმისეული შესწავლა.

კანონპროექტის პირველი მოსმენის შემდგომ, სამოქალაქო სექტორისა და კერძო ორგანიზაციების მხრიდან გამოხატული შენიშვნები და რეკომენდაციები შემოთავაზებულ ცვლილებებში ნაწილობრივ აისახა, მოხდა მხოლოდ მესამე კატეგორიის სუბიექტებში შემავალი კომერციული ბანკების ინტერესების გათვალისწინება, რაც დადებითად უნდა შეფასდეს. თუმცა, ანალოგიური მიდგომა არ გავრცელდა სხვა კერძო სუბიექტებზე. მეორე მოსმენისათვის შემოთავაზებული რედაქციის შესახებ IDFI-მ განცხადებაც[20] გაავრცელა, რომელშიც დეტალურად მიმოიხილა კანონპროექტის ახალ ვერსიაში ასახული რედაქციული და შინაარსობრივი ცვლილებები. რამდენიმე პოზიტიური ნაბიჯის მიუხედავად, რაც მხოლოდ კონკრეტული დეფინიციების დაკონკრეტებაზე გავრცელდა, კანონპროექტის პრინციპულად პრობლემური და მიუღებელი ასპექტები მეორე მოსმენაზეც უცვლელი დარჩა.

20 პარლამენტმა მხარი არ უნდა დაუჭიროს კანონპროექტს ინფორმაციული უსაფრთხოების შესახებ. ინფორმაციის თავისუფლების განვითარების ინსტიტუტი (IDFI). ხელმისაწვდომია **https://idfi.ge/ge/law-on-information-security**

კიბერსივრცის არქიტექტურა - საერთაშორისო გამოცდილება

შესავალი

კვლევის აღნიშნული ნაწილის მიზანია მიმოიხილოს საერთაშორისო გამოცდილება ინფორმაციული უსაფრთხოების არქიტექტურის, კრიტიკული ინფრასტრუქტურის იდენტიფიცირების, საკანონმდებლო ბაზისა და ინფორმაციული უსაფრთხოების რეგულირების მიმართულებით.

ანალიზი განხორციელდა ღია წყაროებზე დაყრდნობით და მოიცვა შემდეგი ქვეყნები: ამერიკის შეერთებული შტატები, დიდი ბრიტანეთი, ესტონეთი, გერმანია და საფრანგეთი. კვლევაში ასევე გაანალიზებულია ევროკავშირის „ქსელისა და ინფორმაციული სისტემების უსაფრთხოების დირექტივის (NIS Directive)“ ის ნაწილი, რომელიც ეხება უშუალოდ კრიტიკული ინფრასტრუქტურის იდენტიფიცირებასა და მასზე ზედამხედველობის განხორციელებას. ქვეყნები შერჩეულია შემდეგი კრიტერიუმების გათვალისწინებით: კრიტიკული ინფრასტრუქტურის იდენტიფიცირების მოდელი, ინციდენტების მართვისა და რეაგირების შესაძლებლობები, კიბერსივრცის ორგანიზაციული მოწყობა და კოორდინაციის მექანიზმები, გამართული სამართლებრივი ბაზა.

ანალიზმა აჩვენა, რომ ქვეყნის კიბერუსაფრთხოების უზრუნველსაყოფად, კიბერსივრცის არქიტექტურა უნდა მოიცავდეს შემდეგ კომპონენტებს: ორგანიზაციული მოწყობა; კრიტიკული ინფრასტრუქტურის იდენტიფიცირება; ზედამხედველობის, ინფორმაციის მიმოცვლისა და ანგარიშვალდებულების გამჭვირვალე და კარგად ორგანიზებული სისტემა; კიბერინციდენტების კლასიფიცირებისა და რეაგირების დახვეწილი მექანიზმები.

კვლევისას გამოიკვეთა, რომ ორგანიზაციული მოწყობა მოიცავს კიბერუსაფრთხოების ეროვნულ დონეზე მაკოორდინირებელი უწყების არსებობას; კიბერინციდენტებზე რეაგირების ეროვნულ ჯგუფს და თავდაცვის სფეროში, სამხედრო ქსელებისა და სისტემების უსაფრთხოებაზე პასუხისმგებელი უწყების არსებობას.

NIS დირექტივის შესაბამისად, ევროკავშირის ყველა წევრი ქვეყანა ვალდებულია გამოყოს ერთი ან რამდენიმე უწყება, რომელიც პასუხისმგებელია კრიტიკული სუბიექტების გამართულ ფუნქციონირებასა და ზედამხედველობაზე (competent authority). აქვე უნდა აღინიშნოს, რომ დირექტივა არ აკონკრეტებს ეს უნდა იყოს პოლიციური უწყება, უსაფრთხოების ტიპის ორგანიზაცია თუ სამოქალაქო უწყება. ყველა ქვეყანა უფლებამოსილია აღნიშნული ფუნქცია დააკისროს იმ უწყებას, რომელსაც საჭიროდ ჩათვლის. ამერიკის შეერთებული შტატების, დიდი ბრიტანეთის, საფრანგეთის და გერმანიის შემთხვევაში, აღნიშნული ფუნქცია ეკისრება პოლიციურ და უსაფრთხოების ტიპის ორგანიზაციებს, ხოლო ესტონეთის შემთხვევაში - სამოქალაქო უწყებას. აქვე უნდა აღინიშნოს, რომ კვლევაში მონაწილე ყველა ქვეყნის სამხედრო კიბერუსაფრთხოებას კურირებს ქვეყნის თავდაცვაზე პასუხისმგებელი შესაბამისი უწყება.

კვლევის თანახმად, კრიტიკული ინფრასტრუქტურის იდენტიფიცირება და მართვა გულისხმობს ქვეყნის გამართული და უსაფრთხო ფუნქციონირების უზრუნველსაყოფად მნიშვნელოვანი კრიტიკული სექტორების, სერვისებისა და სერვისების მომწოდებლების განსაზღვრას და მათთვის ინფორმაციული უსაფრთხოების შესაბამისი ნორმების დაწესებას. კრიტიკული ინფრასტრუქტურის იდენტიფიცირება ყველა მოცემულ ქვეყანაში ხორციელდება სექტორული პრინციპით, წინასწარ შემუშავებული კრიტერიუმების შესაბამისად, როგორებიც არის კრიტიკული სერვისის მწყობრიდან გამოსვლის ალბათობა და

სავარაუდო ზიანის მასშტაბი. ყველა კრიტიკული სექტორი კი მოიცავს კრიტიკული ინფრასტრუქტურის რამდენიმე სუბიექტს. კრიტიკული ინფრასტრუქტურის რეგულაციები არ ვრცელდება მცირე ბიზნესზე და ორგანიზაციებზე, რომელთა თანამშრომლების რაოდენობა არ აღემატება ორმოცდაათს (ევროკავშირის შემთხვევაში).

კვლევაში მოცემულ ქვეყნებში, კრიტიკული სექტორებისა თუ სუბიექტების ზედამხედველობის, ინფორმაციის მიმოცვლისა და ანგარიშვალდებულების გამჭვირვალე და კარგად ორგანიზებული სისტემაა დანერგილი. აღნიშნული ზედამხედველობა ხორციელდება მკაცრად გაწერილი პროცედურების შესაბამისად, რომელსაც ე.წ. მარეგულირებელი (ზედამხედველი) უწყება ან უწყებები უწესებენ კრიტიკულ სუბიექტებს. მარეგულირებელ უწყებას არ აქვს უფლება ჩაერიოს სუბიექტის საქმიანობაში, რომელიც არ უკავშირდება ინფორმაციული უსაფრთხოების უზრუნველყოფას.

ამასთან, უნდა აღინიშნოს, რომ სუბიექტები თავად არიან ვალდებულნი ინციდენტზე პირველადი რეაგირება მოახდინონ, ხოლო თუ ინციდენტი საფრთხეს უქმნის სუბიექტის გამართულ ფუნქციონირებას, მხოლოდ ამ შემთხვევაში აცნობონ მარეგულირებელს. აქვე უნდა აღინიშნოს, რომ მარეგულირებელი აწესებს უსაფრთხოების მოთხოვნებს და პირდაპირ არ განუსაზღვრავს სუბიექტებს, თუ რა სახის ტექნიკური საშუალებები უნდა იქნეს გამოყენებული ქსელის სეგმენტის მონიტორინგისთვის. მარეგულირებელს არ აქვს წვდომა აღნიშნულ ქსელებზე, გარდა იმ შემთხვევისა, როდესაც ინციდენტი საფრთხეს უქმნის საზოგადოების ჯანმრთელობასა და ეროვნულ უსაფრთხოებას. კვლევაზე დაყრდნობით, მოცემულ ქვეყნებს შემუშავებული აქვთ ინციდენტების კლასიფიცირების მოდელი და განსაზღვრული აქვთ, თუ რა შეიძლება მიჩნეულ იქნეს მნიშვნელოვან და უმნიშვნელო ინციდენტად. მნიშვნელოვანი ინციდენტის რეპორტინგი ხდება დაუყოვნებლივ ან განსაზღვრულ ვადაში, ხოლო უმნიშვნელო ინციდენტებზე რეაგირება და მათი აღმოფხვრა თავად სუბიექტის ვალდებულებაა.

სუბიექტებს ვალდებულება აქვთ დაემორჩილონ მარეგულირებლის მოთხოვნებს, სხვა შემთხვევაში დაეკისრებათ ადმინისტრაციული სახდელი.

ბიუჯეტი და საკითხის პრიორიტეტულობა

კიბერუსაფრთხოების საერთაშორისო გამოცდილების შესწავლისას გამოიკვეთა, რომ ყველა წარმოდგენილი ქვეყანა ბიუჯეტის არსებით ნაწილს უთმობს კიბერუსაფრთხოების უზრუნველყოფას. საქართველოში კი ამ მიმართულებისთვის პრიორიტეტის მინიჭება არა პრაქტიკაში, არამედ კონცეპტუალურ და სტრატეგიულ დოკუმენტებში ხდება. მაშინ როცა, კიბერუსაფრთხოება არის სფერო, რომლის წარმატებულად ოპერირებაც ინვესტირების გარეშე შეუძლებელია.

ეროვნული სტრატეგია

კვლევამ ასევე აჩვენა, რომ განვითარებულ ქვეყნებს აქვთ კიბერუსაფრთხოების ეროვნული სტრატეგია - კიბერუსაფრთხოების უზრუნველმყოფი მთავარი კონცეპტუალური დოკუმენტი, რომელიც მოიცავს არსებულ გამოწვევებს და გამოწვევების დასაძლევად გაწერილ სამოქმედო გეგმას; კიბერსივრცის არქიტექტურას და პასუხისმგებლობებს. საქართველოს ამ ეტაპზე არ აქვს მიღებული კიბერუსაფრთხოების ეროვნული სტრატეგია. მეტიც, „ინფორმაციული უსაფრთხოების შესახებ“ ინიცირებული კანონპროექტი შეუსაბამობაში მოდის სტრატეგიის არსებული სამუშაო ვერსიასთან. კანონპროექტი განსხვავებულად აწესრიგებს პასუხისმგებლობებს კიბერუსაფრთხოების უზრუნველყოფაზე, ცვლის კრიტიკული ინფრასტრუქტურის ნუსხას, შემოაქვს ადმინისტრაციულ-სამართლებრივი სანქციები.

ინსტიტუციური მოწყობა

კვლევაში იკვეთება, რომ კიბერუსაფრთხოების უზრუნველყოფა საერთო პასუხისმგებლობაა და როგორც სახელმწიფო, ისე კერძო სექტორი, ერთიანი ძალისხმევით ახდენს კიბერინციდენტების პრევენციასა და მართვას.

ყველა გამოკვლეულ ქვეყანაში, გარდა ესტონეთისა, ეროვნულ დონეზე, კიბერსივრცის უსაფრთხოებაზე პასუხისმგებელია უსაფრთხოების ტიპის ორგანიზაცია. აშშ-ს შემთხვევაში, ეს ორგანიზაცია (DHS) ექვემდებარება სახელმწიფო მდივანს, დიდ ბრიტანეთში (GCHQ) - საგარეო ოფისს, საფრანგეთის შემთხვევაში (ANSSI) - პრემიერ მინისტრს, გერმანიის შემთხვევაში (BSI) შინაგან საქმეთა მინისტრს, ხოლო ესტონეთში (RIA) ეკონომიკისა და კომუნიკაციების მინისტრს.

კრიტიკული ინფრასტრუქტურის განსაზღვრა

კვლევაში მოყვანილ ქვეყნებში, კრიტიკული სექტორები იდენტიფიცირებულია ქვეყნის გამართულ ფუნქციონირებაზე გავლენის მაჩვენებლის მიხედვით, ხოლო თითოეულ კრიტიკულ სექტორში იდენტიფიცირებულია კრიტიკული ინფრასტრუქტურის სუბიექტები.

ყველა მოცემულ ქვეყანაში, კრიტიკული სუბიექტების იდენტიფიცირებისას გათვალისწინებულია ორგანიზაციის ზომა, მაგალითად ევროკავშირის შემთხვევაში, ციფრული სერვისების პროვაიდერები, რომელთა წლიური ბრუნვა არ სცდება 10 მილიონ ევროს ან/და თანამშრომელთა რაოდენობა არ შეადგენს 50 პირზე მეტს, არ ეხება NIS დირექტივა და შესაბამისად არც აღნიშნული რეგულაცია.

კვლევამ აჩვენა, რომ **კრიტიკული ინფორმაციული სისტემის სუბიექტების არსებული კლასიფიკაცია არ შეესაბამება არც ევროპულ და არც ამერიკულ მოდელს.** ახალი მოდელი ვერ აკმაყოფილებს ევროკავშირის დირექტივის მოთხოვნებს (NIS Directive), რომლის მიხედვითაც, კრიტიკული სუბიექტების კლასიფიკაცია ხდება სახელმწიფოს შეუ-

ფერხებელ ფუნქციონირებაზე გავლენის მაჩვენებლის მიხედვით სექტორული პრინციპის შესაბამისად. შედარებისთვის, საქართველოს ახალი კანონმდებლობის მიხედვით, კრიტიკული ინფორმაციული სისტემის სუბიექტები იყოფა სამ ნაწილად, ხოლო ზოგადად, განვითარებული ქვეყნების კრიტიკული ინფრასტრუქტურა - რამდენიმე სექტორად და ქვესექტორად.

საკანონმდებლო ხარვეზად შეგვიძლია მივიჩნიოთ ასევე კრიტიკული ინფორმაციული სისტემის სუბიექტების იდენტიფიცირების კრიტერიუმების არარსებობა. აღნიშნული სუბიექტების, სექტორებისა თუ სფეროების იდენტიფიცირება ხდება შესაძლო ზიანის ალბათობისა და დამდგარი შედეგის სიმძიმის შესაბამისად, მკაცრად განსაზღვრული კრიტერიუმებით, მაგალითად: ინფორმაციული უსაფრთხოების ინციდენტის შემთხვევაში, კრიტიკული ორგანიზაციის მიერ მომსახურების მიწოდების შეფერხების შედეგად უნდა დადგეს მნიშვნელოვანი ზიანი, ხოლო მნიშვნელოვანი ზიანი განისაზღვრება მომხმარებელთა რაოდენობით, ზიანით რომელიც შესაძლოა მიადგეს ქვეყნის ეკონომიკურ და საზოგადოებრივ საქმიანობასა და უსაფრთხოებას, ორგანიზაციის საბაზრო წილით, გეოგრაფიული გავრცელების არეალით და სხვა. **აღნიშნულ ორგანიზაციებში არ შედიან მცირე ოპერატორები, რომლებიც ვერ აკმაყოფილებენ ზემოთ ჩამოთვლილ კრიტერიუმებს.**

საკანონმდებლო ხარვეზად შეიძლება ჩაითვალოს თავად კანონის და კრიტიკული ინფრასტრუქტურის სახელწოდებაც. როგორც ევროპული, ისე ამერიკული და საერთაშორისო სტანდარტების მიხედვით, ქვეყნის გამართული ფუნქციონირებისთვის მნიშვნელოვანი სფეროები და სექტორები მოქცეულია ერთი საერთაშორისოდ აღიარებული სახელწოდების ქვეშ - **კრიტიკული ინფრასტრუქტურა, რომელიც მოიცავს როგორც ე.წ. ვირტუალურ, ისე ფიზიკურ ინფრასტრუქტურას.** საქართველოს კანონმდებლობის შესაბამისად კი კრიტიკული ინფრასტრუქტურა მოიცავს მხოლოდ ვირტუალურ ინფრასტრუქტურას, რაზეც სახელწოდება - კრიტიკული ინფორმაციული სისტემის სუბიექტებიც მიუთითებს. **ინფორმაციული უსაფრთხოება ფართო ტერმინია და მოიცავს როგორც ფიზიკური, ისე ვირტუალური აქტივების უსაფრთხოებას.** ინფორმაციული უსაფრთხოება ვერ იქნება უზრუნველყოფილი ფიზიკური უსაფრთხოების გარეშე. შესაბამისად, საქართველოს კანონში წარმოდგენილი ტერმინი **კრიტიკული ინფორმაციული სისტემის სუბიექტი** არ ჯდება საერთაშორისოდ აღიარებულ პრაქტიკაში.

ინფრასტრუქტურაზე წვდომა და აუდიტი

მიუხედავად იმისა, რომ კვლევაში მოყვანილი ქვეყნების მთავარი კიბერაქტორების ფუნქცია უსაფრთხოების ტიპის ორგანიზაციებს აკისრია, კვლევიდან არ იკვეთება მათ მიერ, კრიტიკული ინფრასტრუქტურის სუბიექტების კრიტიკულ აქტივებზე უშუალო წვდომისა მართვის ტენდენცია. კვლევამ აჩვენა, რომ ეს უწყებები კრიტიკული ინფრასტრუქტურის სექტორებს უწესებენ უსაფრთხოების მოთხოვნებს, რომელთა შესრულებაც სავალდებულოა უკლებლივ ყველა სუბიექტისთვის, ეს იქნება სახელმწიფო თუ კერძო სუბიექტი.

კვლევაში განხილულ ქვეყნებში, სამთავრობო სექტორს თავად ეროვნული უწყება კურირებს და შესაბამისად, მას აქვს წვდომა სამთავრობო სექტორის კრიტიკულ ინფრასტრუქტურაზე.

სხვა შემთხვევაში, როგორც უკვე აღინიშნა, ეროვნულ მარეგულირებელს წვდომა აქვს კერძო სექტორის ინფრასტრუქტურაზე, თავად ინფრასტრუქტურის მარეგულირებლის გავლით, მხოლოდ ისეთ შემთხვევაში, როდესაც ინციდენტი იმდენად მასშტაბურია, რომ საფრთხე ექმნება ეროვნულ უსაფრთხოებას.

აღნიშნული ორგანიზაციული სტრუქტურა არ ირღვევა არც აუდიტის ჩატარებისას. კრიტიკულ სუბიექტებში აუდიტი ტარდება ეროვნული უწყების მიერ გაწერილი პროცედურების შესაბამისად, სექტორის მარეგულირებლის მიერ, ხოლო სამთავრობო სექტორში - ეროვნული უწყების მიერ, ვინაიდან სამთავრობო სექტორის მარეგულირებელი თავად ეროვნული უწყებაა. აუდიტის პერიოდულობა და პროცედურები გაწერილია ცალკე ბრძანებით და არ არის დაუგეგმავი.

საერთაშორისო გამოცდილების კვლევისას იკვეთება ტენდენცია, რომ საქართველოს ახალი კანონი „ინფორმაციული უსაფრთხოების შესახებ“, რიგ შემთხვევებში, სრულიად აცდენილია საუკეთესო პრაქტიკას.

ინციდენტის კლასიფიკაცია

საკანონმდებლო ხარვეზად შეიძლება ჩაითვალოს ეროვნულ დონეზე, კიბერინციდენტების კლასიფიცირების არარსებობა. საერთაშორისო გამოცდილებით, კრიტიკული ინფრასტრუქტურის ინფორმაციულ სისტემებში იდენტიფიცირებული ყველა ინციდენტის დახარისხება (ინციდენტები კლასიფიცირებულია კრიტიკულობის და შესაძლო ზიანის მიხედვით) და რეაგირება, წინასწარ შემუშავებული ინციდენტებზე რეაგირების შკალისა და გეგმის შესაბამისად ხორციელდება. ხოლო საქართველოში, არ არის განხორციელებული ეროვნულ დონეზე ინციდენტების კლასიფიცირება, რაც თავისთავად, უარყოფითად აისახება უსაფრთხოების ხარისხზე.

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონპროექტის მე-9 მუხლის მეორე პუნქტის „ბ“ ქვეპუნქტის მიხედვით, კომპიუტერული ინციდენტების იდენტიფიცირების შემთხვევაში, კრიტიკული ინფორმაციული სისტემის სუბიექტმა უნდა განახორციელოს შესაბამისი უწყების (სახელმწიფო უსაფრთხოების სააგენტო, ციფრული მმართველობის სააგენტო, კიბერუსაფრთხოების ბიურო) დაუყოვნებლივი ინფორმირება. საერთაშორისო გამოცდილებამ კი აჩვენა, რომ კრიტიკული ინფრასტრუქტურის სუბიექტები, შესაბამისი მაკოორდინირებელი უწყების კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფთან (CSIRT), **ინფორმაციას ცვლიან მხოლოდ იმ კიბერინციდენტებზე, რომელთაც გავლენა აქვთ ამ სუბიექტების ნორმალურ ფუნქციონირებაზე.**

ყველა გამოკვლეულ ქვეყანაში ინციდენტების კლასიფიცირება ხდება ინციდენტის ალბათობისა და შესაძლო ზიანის მიხედვით და შესაბამისად, მაკოორდინირებელს ინფორმაცია მიეწოდება მხოლოდ და მხოლოდ „მნიშვნელოვან“ ინციდენტებზე და არა ყველა კიბერინციდენტზე, ხოლო რომელი ინციდენტია „მნიშვნელოვანი“ და რომელი „ნაკლებ მნიშვნელოვანი“, დამოუკიდებელი სამართლებრივი აქტით განისაზღვრება. აქვე უნდა აღინიშნოს, **რომ არც ოპერატიულ-ტექნიკურ სააგენტოს, არც ციფრული მმართველობის სააგენტოს**

და არც კიბერუსაფრთხოების ბიუროს არ გააჩნია შესაბამისი/საკმარისი ადამიანური და ტექნიკური რესურსი, მიიღოს და გააანალიზოს ყველა კიბერინციდენტი, რომელსაც ადგილი ექნება კრიტიკული ინფორმაციული სისტემის სუბიექტებში, შესაბამისად, აღნიშნული მუხლი საჭიროებს კორექტირებას.

საომარი მგდომარეობა

კანონპროექტის მე-9 მუხლის მე-5 პუნქტის მიხედვით, საომარი მდგომარეობის დროს, კიბერუსაფრთხოების უზრუნველყოფა და კიბეროპერაციების ჩატარება ხორციელდება **„საომარი მდგომარეობის შესახებ“ საქართველოს კანონის შესაბამისად. „საომარი მდგომარეობის შესახებ“ საქართველოს კანონის საბოლოო ვერსია არ შეიცავს არც ერთ მუხლს, სადაც გაწერილია საომარი მდგომარეობის დროს როგორ ხდება ქვეყანაში კიბერუსაფრთხოების უზრუნველყოფა, პასუხისმგებელი უწყებების კოორდინირება და მასიური კიბერშეტევის მოგერიება,** შესაბამისად, ამ მიმართულებით გარკვეული ღონისძიებების გატარება სასიცოცხლოდ მნიშვნელოვანია, მით უმეტეს, თუ გავითვალისწინებთ იმ გარემოებას, რომ **საქართველო არაერთხელ გახდა მასობრივი კიბერშეტევის მსხვერპლი, ხოლო სახელმწიფო უწყებებმა ვერ აჩვენეს კოორდინაციისა და რეაგირების შესაბამისი დონე.**

პერსონალური მონაცემების დაცვა

ხშირ შემთხვევაში, ინციდენტების შედეგად ხდება პერსონალური მონაცემების კომპრომეტირება. შესაბამისად, ოპერატიულ-ტექნიკურმა სააგენტომ და ციფრული მმართველობის სააგენტომ უნდა ითანამშრომლონ სახელმწიფო ინსპექტორის სამსახურთან, რათა თავიდან იქნეს აცილებული პერსონალურ მონაცემთა ხელყოფა. **საქართველოს კანონში „ინფორმაციული უსაფრთხოების შესახებ“ არ იძებნება ჩანაწერი, სადაც საუბარია პირადი ცხოვრების ხელშეუხებლობასა და პერსონალურ მონაცემთა დაცვაზე.**

NIS დირექტივა ხაზგასმით აღნიშნავს, რომ კრიტიკული სუბიექტების მიერ CSIRT-ებისთვის ინციდენტების შეტყობინება შესაძლოა მოითხოვდეს პერსონალური ინფორმაციის დამუშავებას და ასეთი დამუშავება შესაბამისობაში უნდა მოდიოდეს ევროპარლამენტისა და ევროსაბჭოს 95/46/EC დირექტივასა და 45/2001 რეგლამენტთან. გაცვლილი ინფორმაცია უნდა შემოიფარგლებოდეს მხოლოდ იმ ინფორმაციით, რომელიც შესაბამისი და პროპორციულია ამგვარი გაცვლის მიზნისათვის. ინფორმაციის ასეთი გაცვლისას შენარჩუნებული უნდა იყოს ინფორმაციის კონფიდენციალურობა, ძირითადი სერვისებისა და ციფრული სერვისების პროვაიდერების ოპერატორების უსაფრთხოება და კომერციული ინტერესები.

აუდიტი და შესაბამისობა

საერთაშორისო გამოცდილებამ აჩვენა, რომ კრიტიკული ინფრასტრუქტურის სუბიექტები თავად იღებენ შესაბამის ტექნიკურ და ორგანიზაციულ ზომებს, ქსელებისა და ინფორმაციული სისტემების უსაფრთხოების წინაშე მდგარი რისკების სამართავად, ეს ზომებია:

- ქსელის უსაფრთხოება
- ინციდენტების მართვა
- ბიზნესის უწყვეტობის მართვა
- საერთაშორისო სტანდარტებთან შესაბამისობა
- მონიტორინგი, აუდიტი და ტესტირება

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ინიცირებული ცვლილებების (მე-6 მუხლი) თანახმად, შესაბამისი კატეგორიის სუბიექტის აუდიტს და ტესტირებას ახორციელებს ოპერატიულ-ტექნიკური სააგენტო, ციფრული მმართველობის სააგენტო, ან ციფრული მმართველობის სააგენტოს მიერ ავტორიზებული ორგანიზაცია. **აღნიშნული ჩანაწერი ეწინააღმდეგება როგორც NIS დირექტივას,** ისე საერთაშორისო გამოცდილებას. მაგალითად, ბრიტანეთში კომუნიკაციების უსაფრთხოების ჯგუფი (Communications Electronics Security Group) წარმოადგენს ეროვნულ ტექნიკურ უწყებას, რომლიც კრიტიკული ინფრასტრუქტურის სუბიექტებს აწვდის რჩევებს, რეკომენდაციებს და საჭიროების შემთხვევაში, უწევს დახმარებას, რათა დაცული იყოს მათი კრიტიკული აქტივებისა და ქსელების უსაფრთხოება.

ანგარიშვალდებულება და გამჭვირვალობა

ხელისუფლების ანგარიშვალდებულება და გამჭვირვალობა დემოკრატიული სახელმწიფოს მნიშვნელოვანი პრინციპებია. საქართველოს აქვს ამბიცია გახდეს ევროპული და ევროატლანტიკური ოჯახის სრულუფლებიანი წევრი, შესაბამისად, ქვეყნის ფუნქციონირება უნდა დაეფუძნოს აღნიშნულ პრინციპებს. კიბერუსაფრთხოება ეროვნული უსაფრთხოების მნიშვნელოვანი კომპონენტია და შესაბამისად, მაღალია საზოგადოების ინტერესი ამ სფეროში მიმდინარე პროცესებზე. მნიშვნელოვანია საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“ მოიცავდეს ოპერატიულ-ტექნიკური სააგენტოს, ციფრული მმართველობის სააგენტოსა და კიბერუსაფრთხოების ბიუროს ანგარიშვალდებულების პროცედურებს, რათა ქვეყანაში კიბერუსაფრთხოების უზრუნველყოფა განხორციელდეს გამჭვირვალედ, საუკეთესო საერთაშორისო პრაქტიკისა და გამოცდილების შესაბამისად, სამოქალაქო სექტორის მაქსიმალური ჩართულობით.

რეკომენდაციები

საქართველოს პარლამენტის წევრის, ირაკლი სესიაშვილის მიერ ინიცირებული საკანონმდებლო ცვლილებები სრულიად ცვლის ქვეყნის კიბერუსაფრთხოების არქიტექტურას და ახლებურად აწესრიგებს კრიტიკული ინფრასტრუქტურის მართვის საკითხებს. საერთაშორისო სტანდარტებისა და პრაქტიკის კვლევის საფუძველზე, გამოვყოფთ იმ საკითხებს, რაც საჭიროებს დახვეწას და რომელთა გათვალისწინებაც ხელს შეუწყობს მეტად დაცული კიბერსივრცის უზრუნველყოფას.

კიბერუსაფრთხოების ეროვნული სტრატეგიისა და საკანონმდებლო ბაზის შესაბამისობა

საერთაშორისო პარტნიორებისა და ყველა დაინტერესებული მხარის აქტიური ჩართულობით, შემუშავებულია კიბერუსაფრთხოების ეროვნული სტრატეგიის სამუშაო ვერსია, რომელიც პასუხობს კიბერუსაფრთხოების სფეროში, ქვეყნის წინაშე მდგარ გამოწვევებს და მოიცავს ღონისძიებებს, რომელთა გატარებაც ხელს შეუწყობს კიბერსივრცის დაცვას. მნიშვნელოვანია რომ, პირველ რიგში, მოხდეს აღნიშნული სტრატეგიის დამტკიცება. რის შემდეგად, ნებისმიერი ახალი საკანონმდებლო ინიციატივა, მათ შორის, კანონპროექტი „ინფორმაციული უსაფრთხოების შესახებ“ უნდა შეესაბამებოდეს და გამომდინარეობდეს ეროვნული სტრატეგიიდან.

კიბერუსაფრთხოების უზრუნველყოფის მოდელი

ქვეყნის კიბერუსაფრთხოების პოლიტიკის შემუშავებასა და გატარებაზე, კიბერკრიზისების მართვასა და უწყებების კოორდინირებაზე დღეს პასუხისმგებელია ეროვნული უსაფრთხოების საბჭო, თუმცა აუცილებელია საბჭოში შეიქმნას და კიბერუსაფრთხოების სპეციალისტებით დაკომპლექტდეს სპეციალიზებული დანაყოფი, რომლის ფუნქციაც უშუალოდ კიბერუსაფრთხოების საკითხების კოორდინირება გახდება.

ამავე დროს, იმ შემთხვევაში, თუ განხორციელდება ციფრული მმართველობის სააგენტოს შესაბამისი ტექნიკითა და პროგრამული უზრუნველყოფით აღჭურვა, კადრებით დაკომპლექტება, აღსრულების მექანიზმის შემოღება - სააგენტო შეძლებს უზრუნველყოს ქვეყნის კრიტიკული ინფრასტრუქტურის უსაფრთხოება, სახელმწიფო უსაფრთხოების სამსახური კი განახორციელებს სახელმწიფო უსაფრთხოების დაცვას ციფრული მმართველობის სააგენტოსთან, კიბერუსაფრთხოების ბიუროსა და ეროვნული უსაფრთხოების საბჭოსთან კოორდინაციით.

შესაბამისად, მნიშვნელოვანია დარჩეს კიბერუსაფრთხოების უზრუნველყოფის არსებული მოდელი და ქვეყნის კრიტიკული ინფრასტრუქტურის ზედამხედველობის ფუნქცია დაეკისროს ციფრული მმართველობის სააგენტოს. ოპერატიულ-ტექნიკური სააგენტოსთვის აღნიშნული ფუნქციის დაკისრებით, სააგენტოს მიეცემა საზოგადოების კონტროლის დამატებითი ბერკეტი, რამაც შესაძლოა გაზარდოს ინტერნეტ სივრცეში, პირადი უფლებებისა და თავისუფლებების შეზღუდვის ან/და დარღვევის საფრთხე.

კიბერინციდენტების კლასიფიკაცია და შეტყობინება

აუცილებელია განხორციელდეს კიბერინციდენტების კლასიფიცირება ინციდენტის ალბათობისა და შესაძლო ზიანის საფუძველზე, ამასთან, შემუშავდეს კიბერინციდენტების შეტყობინების პროცედურები. ზედამხედველ უწყებებსა და კრიტიკული ინფრასტრუქტურის სუბიექტებს შორის ინფორმაციის მიმოცვლის უსაფრთხო არხების შექმნა, ინციდენტების მართვის მნიშვნელოვანი წინაპირობაა.

კრიტიკული ინფრასტრუქტურის იდენტიფიცირება

ძალზედ მნიშვნელოვანია კრიტიკული ინფრასტრუქტურის იდენტიფიცირების კრიტერიუმების განსაზღვრა და აღნიშნული ნუსხის იდენტიფიცირება სექტორული პრინციპით, რაც კონკრეტული სფეროების უფრო ეფექტიანად დაცვის საშუალებას მოგვცემს. კრიტიკული ინფრასტრუქტურის იდენტიფიცირებისას მნიშვნელოვანია გათვალისწინებულ იქნეს შემდეგი კრიტერიუმები: ორგანიზაციის (სახელმწიფო, ან კერძო) მნიშვნელობა და როლი სოციალური ან/და ეკონომიკური საქმიანობის განხორციელება-შენარჩუნებისთვის; დამოკიდებულება ქსელსა და ინფორმაციულ სისტემებზე; ინფორმაციული უსაფრთხოების ინციდენტის შემთხვევაში, ორგანიზაციის მიერ მომსახურების მიწოდების შეფერხების შედეგად დამდგარი ზიანის დონე. კრიტიკული ინფრასტრუქტურის იდენტიფიცირებისას მნიშვნელოვანია გათვალისწინებულ იქნეს NIS დირექტივის მოთხოვნები როგორებიც არის: კრიტიკული სერვისის მწყობრიდან გამოსვლის ალბათობა და სავარაუდო ზიანის მასშტაბი. კრიტიკული ინფრასტრუქტურის რეგულაციები კი არ უნდა გავრცელდეს მცირე ბიზნესზე და ორგანიზაციებზე, რომელთა მწყობრიდან გამოსვლა საფრთხეს არ შეუქმნის ქვეყნის გამართულ ფუნქციონირებას და არ დააზიანებს მის ინტერესებს.

ეროვნული უსაფრთხოების საბჭოს როლი და კრიზისების მართვა

ეროვნული უსაფრთხოების საბჭოს საქმიანობის ერთ-ერთი მთავარი მიმართულებაა ინფორმაციული უსაფრთხოების პოლიტიკის ანალიზი, საფრთხეების იდენტიფიცირება და შეფასება, პოლიტიკის დაგეგმვა და კოორდინაცია. საბჭო ასევე უზრუნველყოფს კრიზისული ვითარების დროს, სახელმწიფო უწყებების კოორდინაციას. მნიშვნელოვანია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონპროექტი მოიცავდეს მუხლს, სადაც ხაზგასმული იქნება საბჭოს, როგორც ქვეყნის კიბერაქტორების მაკოორდინირებლის როლი და ფუნქციები. ამით საბჭო რეალურად განახორციელებს მასზე დაკისრებული უფლებამოსილებებს, რაც კრიზისულ სიტუაციებში, კოორდინირებული და სინქრონიზებული მოქმედებების განხორციელების მნიშვნელოვანი ხელშემწყობი ფაქტორი გახდება.

პერსონალურ მონაცემთა დაცვა

ინფორმაციული უსაფრთხოების ინციდენტების შედეგად ხდება პერსონალური მონაცემების კომპრომეტირება. შესაბამისად, კიბერუსაფრთხოების პოლიტიკის აღმასრულებელმა უწყებებმა უნდა ითანამშრომლონ სახელმწიფო ინსპექტორის სამსახურთან, რათა თავიდან

იქნეს აცილებული პერსონალურ მონაცემთა ხელყოფა. მნიშვნელოვანია კანონპროექტი „ინფორმაციული უსაფრთხოების შესახებ“ მოიცავდეს პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ ჩანაწერს.

კიბერუსაფრთხოების სფეროს პრიორიტიზირება და შესაბამისი ფინანსური რესურსის გამოყოფა

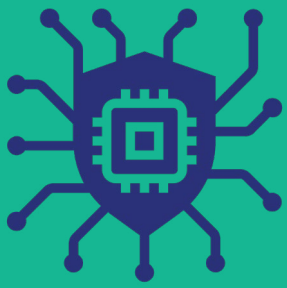
მნიშვნელოვანია კიბერუსაფრთხოება გახდეს სახელმწიფოს პრიორიტეტული მიმართულება და მეტი ფინანსური და ინტელექტუალური რესურსი მოხმარდეს მის განვითარებას.

საზოგადოებრივი კონტროლის მექანიზმების უზრუნველყოფა

მაღალი საზოგადოებრივი ინტერესის გათვალისწინებით, არანაკლებ მნიშვნელოვანია არსებობდეს საზოგადოებრივი კონტროლის მექანიზმები კიბერუსაფრთხოების უზრუნველყოფაში ჩართულ უწყებებზე. აღნიშნული შესაძლოა განხორციელდეს შემდეგი ღონისძიებების გატარებით:

- სახელმწიფო უწყებებმა საქმიანობა განახორციელონ ღია-მმართველობის პრინციპზე დაყრდნობით
- უზრუნველყოფილ იქნეს ყველა დაინტერესებული მხარის, მათ შორის, არასამთავრობო სექტორის ჩართულობა კიბერუსაფრთხოების პოლიტიკისა და საკანონმდებლო ცვლილებების შემუშავებისას
- განხორციელდეს სისტემატური ანგარიშგება განხორციელებული საქმიანობის შესახებ
- განხორციელდეს კერძო და არასამთავრობო სექტორში არსებული რესურსის გამოყენება ტრენინგებსა და კიბერსავარჯიშოებში
- მოეწყოს სისტემატური შეხვედრები და მოხდეს ინფორმაციის მიმოცვლა ახალ ინიციატივებთან დაკავშირებით
- განხორციელდეს არასამთავრობო და კერძო სექტორის ჩართულობა სხვადასხვა საგანმანათლებლო და ცნობიერების ამაღლებისკენ მიმართულ ღონისძიებებში

აღნიშნული ღონისძიებების გატარება და კიბერშესაძლებლობების მუდმივი განვითარება, საქართველოს მის წინაშე არსებული კიბერსაფრთხეების მიმართ თავდაცვისუნარიანს გახდის.



დანართი 1: კიბერუსაფრთხოების მარეგულირებელი ჩარჩო - საერთაშორისო პრაქტიკა

ამერიკის შეერთებული შტატები

კიბერუსაფრთხოების უზრუნველყოფა და კოორდინაცია ეროვნულ დონეზე

აშშ-ში კიბერუსაფრთხოების უზრუნველყოფა გადანაწილებულია უწყებების ფართო სპექტრზე. ძირითადი პოლიტიკის საკოორდინაციო როლს ასრულებს თეთრ სახლში არსებული **ეროვნული უშიშროების საბჭოს ინფორმაციისა და კომუნიკაციების ინფრასტრუქტურის უწყებათაშორისი პოლიტიკის კომიტეტი** (ICI-IPC). ICI-IPC–ს თანათავმჯდომარეობენ შიდა უსაფრთხოების საბჭო (Homeland Security Council) და კიბერუსაფრთხოების კოორდინატორი (Cyber Security Coordinator) ეროვნული უსაფრთხოების საბჭოს კიბერუსაფრთხოების ოფისი. კიბერუსაფრთხოების კოორდინატორი ხელმძღვანელობს კიბერუსაფრთხოების ეროვნული სტრატეგიისა და პოლიტიკის შემუშავებას უწყებათაშორის დონეზე და ზედამხედველობას უწევს სააგენტოების მიერ ამ პოლიტიკის განხორციელებას.

თეთრ სახლში არსებული დანაყოფების გარდა, **შიდა უსაფრთხოების დეპარტამენტი** (DHS) არის ძირითადი ინსტიტუტი, რომელიც პასუხისმგებელია ამერიკის შეერთებული შტატების კიბერუსაფრთხოებაზე. DHS შეიქმნა 2002 წლის შიდა უსაფრთხოების აქტით და მას დაეკისრა პასუხისმგებლობა ინფორმაციული ტექნოლოგიებისა (IT) და კომუნიკაციების სექტორებში კრიტიკული ინფრასტრუქტურის დაცვაზე. შიდა უსაფრთხოების დეპარტამენტის ერთ-ერთი ძირითადი ამოცანაა კიბერუსაფრთხოების უზრუნველყოფა, რაც მოიცავს შემდეგი ფუნქციების განხორციელებას: კრიტიკული ინფრასტრუქტურის უსაფრთხოების და მდგრადობის გაძლიერება; ფედერალური სამოქალაქო სააგენტოების დახმარება კიბერუსაფრთხოების უზრუნველყოფასთან დაკავშირებულ შესყიდვებზე; კანონის დაცვის გაძლიერება და ინციდენტზე რეაგირება. DHS-ში შექმნილი კიბერუსაფრთხოებისა და ინფრასტრუქტურის უსაფრთხოების სააგენტო (CISA) კი წარმოადგენს უწყებას, რომელიც პასუხისმგებელია gov. დომენის დაცვაზე, კიბერსაფრთხეების აღმოფხვრაზე, კიბერშეტევებზე რეაგირებასა და სხვა სახელმწიფო უწყებებისთვის რეკომენდაციების გაცემაზე.

DHS-ს ექვემდებარება **კიბერინციდენტებზე რეაგირების ჯგუფი (US-CERT),** რომელიც წარმოადგენს ეროვნული მასშტაბით, კიბერინციდენტებზე რეაგირების მთავარ ორგანოს.

ეროვნული უსაფრთხოების სააგენტოს (NSA) მნიშვნელოვანი როლი აქვს ქვეყნის კიბერუსაფრთხოების უზრუნველყოფაში. სააგენტო ახორციელებს კიბერსაფრთხეების შეფასებასა და ანალიზს, გასცემს რეკომენდაციებს თანამედროვე კიბერსადაზვერვო და სხვა ტექნიკური საშუალებების დანერგვაზე, შეიმუშავებს ქსელის უსაფრთხოებისა და სხვა ტექნიკური "გადაწყვეტილებების" სახელმძღვანელოებს.

სახელმწიფო დეპარტამენტი (DoS) არის მთავარი ორგანო, რომელიც უზრუნველყოფს პრეზიდენტის კიბერუსაფრთხოების პოლიტიკის საერთაშორისო დონეზე კომუნიკაციასა და კოორდინაციას.

იუსტიციის დეპარტამენტი (DOJ) პასუხისმგებელია კიბერუსაფრთხოებასთან დაკავშირებული საკანონმდებლო ბაზის შემუშავებაზე, კიბერდანაშაულის გამოძიებასა და სამართლებრივ დევნაზე, სადაზვერვო ინფორმაციის შეგროვებასა და სხვა უწყებებისთვის იურიდიულ და პოლიტიკურ დახმარებაზე. იუსტიციის დეპარტამენტი იძიებს და აღკვეთს კიბერდანაშაულს მისი იურისდიქციის ფარგლებში; წარმართავს საშინაო ეროვნული უსაფრთხოების ოპერაციებს კიბერსაფრთხეებთან დაკავშირებით, მათ შორის, საგარეო დაზვერვის, ტერორიზმის ან სხვა ეროვნული უსაფრთხოების წინაშე არსებული საფრთხე-

ების აღკვეთით; დეპარტამენტი ასევე ახორციელებს კიბერსაფრთხეების შესახებ ინფორმაციის შეგროვებას, ანალიზს და გავრცელებას.

თავდაცვის დეპარტამენტის ამოცანაა „.mil“ დომენისა და თავდაცვის დეპარტამენტის გლობალური ინფორმაციული ინფრასტრუქტურის კიბერშეტევებისგან დაცვა. გარდა ამისა, თავდაცვის დეპარტამენტი პასუხისმგებელია საგარეო კიბერსაფრთხეების შესახებ ინფორმაციის შეგროვებაზე, ეროვნული უსაფრთხოებისა და სამხედრო სისტემის დაცვაზე და იურისდიქციის ფარგლებში, კიბერდანაშაულის გამოძიებაზე.

თავდაცვის დეპარტამენტს ექვემდებარება აშშ-ს კიბერსარდლობა (USCYBERCOM), რომლის ძირითადი ამოცანაა კიბერსივრცის ოპერაციების ცენტრალიზებული მართვა და კონტროლი, სინქრონიზაციის, დაგეგმვისა და შესრულების ჩათვლით.

კრიტიკული ინფრასტრუქტურა და მასზე ზედამხედველობა

ამერიკის შეერთებულ შტატებში კრიტიკული ინფრასტრუქტურის 16 სექტორია, რომელთა აქტივები, სისტემები და ქსელები, იქნება ეს ფიზიკური თუ ვირტუალური, სასიცოცხლოდ მნიშვნელოვანია შეერთებული შტატების ეროვნული და ეკონომიკური უსაფრთხოების, საზოგადოებრივი კეთილდღეობისა და თავდაცვის სისტემის გამართული ფუნქციონირებისთვის. **ყველა კრიტიკულ სექტორს გააჩნია მარეგულირებელი უწყება (ზედამხედველი უწყება), თუმცა სექტორების უმეტესობის, მათ შორის, სამთავრობო სექტორის კიბერუსაფრთხოების უზრუნველყოფაზე პასუხისმგებელია DHS.**

კანონი კრიტიკული ინფრასტრუქტურის შესახებ (Critical Infrastructure Information Act) აწესრიგებს DHS-ისა და კრიტიკული ინფრასტრუქტურის სექტორებს შორის ინფორმაციის მიმოცვლის პროცედურებს. აღნიშნული კანონის თანახმად, DHS-ში შექმნილია ინფორმაციის ანალიზისა და ინფრასტრუქტურის დაცვის დირექტორატი (დირექტორატის ხელმძღვანელს, სენატთან შეთანხმებით ნიშნავს პრეზიდენტი), რომელიც პასუხისმგებელია მიიღოს და დაამუშაოს ინფორმაცია კრიტიკული ინფრასტრუქტურის სუბიექტებისგან.

კანონის შესაბამისად, სუბიექტებისგან მიღებული ნებისმიერი ინფორმაცია დაცულია უნებართვო გამჟღავნებისგან და გამოიყენება მხოლოდ და მხოლოდ სამსახურებრივი მოვალეობის შესრულების, კიბერსაფრთხეების პრევენციის, იდენტიფიცირებისა და რეაგირების მიზნით. კრიტიკულ ინფრასტრუქტურასთან დაკავშირებული ნებისმიერი სადაზვერვო ინფორმაციის მიღება, დამუშავება და გამოყენება ხდება ცენტრალური სადაზვერვო სააგენტოს (CIA) თანხმობით, ხოლო საგამოძიებო მასალების - გენერალური პროკურორის თანხმობით.

დირექტორატი უფლებამოსილია შექმნას და ოპერირება გაუწიოს უსაფრთხო ინფორმაციულ და საკომუნიკაციო ინფრასტრუქტურას (ქმნის ინფორმაციის მიმოცვლის უსაფრთხო არხებს), გამოიყენოს სხვადასხვა მოწინავე ანალიტიკური და ტექნიკური საშუალებები, რათა წვდომა ჰქონდეს, მიიღოს და გააანალიზოს მონაცემები შემდგომი რეაგირებისთვის. დირექტორატი აღნიშნულ უფლებამოსილებას ახორციელებს პერსონალურ მონაცემთა უსაფრთხოების სრული ნორმების დაცვით.

დირექტორატს წვდომა აქვს კრიტიკული ინფრასტრუქტურის სუბიექტებში დაცულ ყველა სახის ინფორმაციაზე, რასაც საჭიროდ ჩათვლის, მათ შორის, ანგარიშებზე, შეფასების დოკუმენტებზე, ყველა სახის ანალიტიკურ მასალაზე, სადაზვერვო ინფორმაციის ჩათვლით, აგრეთვე ყველა იმ ინფორმაციაზე, რაც კრიტიკულ ინფრასტრუქტურას და ნებისმიერ ფედერალურ უწყებას ეხება.

სამდივნოს მიერ აღნიშნული ინფორმაციის მოპოვება ხდება მოთხოვნის საფუძველზე, ან ნებაყოფლობით. „ნებაყოფლობით“ - ამ შემთხვევაში გულისხმობს კრიტიკულ სუბიექტში, თავად სუბიექტის მიერ გამოვლენილი ინფორმაციული უსაფრთხოების მნიშნელოვანი ინციდენტის შესახებ ინფორმაციას. სენსიტიური ინფორმაციის მიწოდება, მაგალითად საბანკო სექტორის შემთხვევაში, უნდა აკმაყოფილებდეს საბანკო სენსიტიური ინფორმაციის მიმოცვლის რეგულაციებს და DHS ვალდებულია დაემორჩილოს აღნიშნულ რეგულაციებს. მიღებული ინფორმაციის დამუშავება და გამოყენება დამატებითი სამართლებრივი აქტით რეგულირდება. მიწოდებული ინფორმაცია არაავტორიზებული წვდომისგან მაქსიმალურად დაცულია და მისი გამჟღავნება ისჯება კანონით.

ფედერალური კანონმდებლობა ავალდებულებს ყველა კრიტიკული ინფრასტრუქტურის სუბიექტს დანერგოს შესაბამისი უსაფრთხოების მექანიზმები და დაემორჩილოს DHS-ის მიერ გაწერილ ვალდებულებებს. აღნიშნული ვალდებულებების არშესრულება ისჯება ფედერალური კანონით, რიგ შემთხვევაში, **სისხლის სამართლის კანონმდებლობით, გააჩნია გაწერილი წესების დარღვევის მნიშვნელობას და დამდგარ შედეგს.**

აშშ-ს კრიტიკული ინფრასტრუქტურის სექტორები და პასუხისმგებელი უწყებები:

სექტორი	პასუხისმგებელი უწყება
ქიმიური	DHS
საკომუნიკაციო	DHS
კაშხალები	DHS
გადაუდებელი დახმარების სერვისი	DHS
საფინანსო	ფინანსთა სამინისტრო
სახელმწიფო დაწესებულებები	DHS
საინფორმაციო ტექნოლოგიები	DHS
ტრანსპორტი	DHS
კომერციული დაწესებულებები	DHS
სახელმწიფო მნიშვნელობის საწარმოები	DHS
თავდაცვის ინდუსტრია	თავდაცვის სამინისტრო
ენერგოსექტორი	ენერგეტიკის სამინისტრო
კვების პროდუქტები და სოფლის მეურნეობა	სოფლის მეურნეობის სამინისტრო და ჯანდაცვის სამინისტრო ერთდროულად
საზოგადოებრივი ჯანდაცვა	DHS
ბირთვული რექტორები და ნარჩენები	გარემოს დაცვის სამინისტრო

კიბერინციდენტის კლასიფიკაცია

საინტერესოა აშშ-ს კიბერინცინდენტის კლასიფიკაციის მოდელი. „კიბერინციდენტების კოორდინაციის შესახებ“ ამერიკის შეერთებული შტატების პრეზიდენტის დირექტივის შესაბამისად, აშშ-ში, კიბერინციდენტები კლასიფიცირებულია შემდეგნაირად:

ინციდენტი	განმარტება
კიბერინციდენტი	*შემთხვევა, რომელსაც აღგიღი აქვს კომპიუტერულ ქსელში, ან ხორციელდება კომპიუტერული ქსელის მეშვეობით და საფრთხეს უქმნის, (ან აუცილებლად შეუქმნის) კომპიუტერების, ინფორმაციის ან კომუნიკაციების სისტემების, ქსელების, კომპიუტერების ან ინფორმაციული სისტემების მეშვეობით კონტროლირებადი ფიზიკური ან ვირტუალური ინფრასტრუქტურის კონფიდენციალობას, მთლიანობას ან ხელმისაწვდომობას.*
მნიშვნელოვანი კიბერინციდენტი	*ინციდენტი (ან ინციდენტების ერთობლიობა), რომელმაც შესაძლოა განსაკუთრებული ზიანი მიაყენოს ქვეყნის ეროვნულ ინტერესებს, საერთაშორისო ურთიერთობებს, შეერთებული შტატების ეკონომიკას, საზოგადოებას, ამერიკელი ხალხის ჯანმრთელობას, უსაფრთხოებასა და თავისუფლებას.*

აშშ-ს კიბერუსაფრთხოების ფედერალურმა ცენტრმა შეიმუშავა კიბერინციდენტების ხუთდონიანი კლასიფიკაცია, რომელიც საერთოა ქვეყნის ყველა კრიტიკული სუბიექტისთვის. სახელმწიფო უწყებაზე განხორციელებული კიბერშეტევების კლასიფიცირება ხდება ქვემოთ მოცემული სქემის შესაბამისად:

კიბერინციდენტის დონე	განმარტება
დონე - 5 კრიტიკული	გარდაუვალ საფრთხეს უქმნის კრიტიკული ინფრასტრუქტურის სერვისების გამართულ ფუნქციონირებას, მთავრობის სტაბილურობას ან აშშ-ს მოქალაქეების სიცოცხლეს.
დონე - 4 განსაკუთრებით მძიმე	სავარაუდოდ, მნიშვნელოვან საფრთხეს შეუქმნის საზოგადოებრივ ჯანმრთელობას ან უსაფრთხოებას, ეროვნულ უსაფრთხოებას, ეკონომიკურ უსაფრთხოებას, საერთაშო რისო ურთიერთობებს, ან ადამიანთა თავისუფლებებს.
დონე - 3 მაღალი	სავარაუდოდ, საგრძნობ საფრთხეს შეუქმნის საზოგადოებრივ ჯანმრთელობას ან უსაფრთხოებას, ეროვნულ უსაფრთხოებას, ეკონომიკურ უსაფრთხოებას, საერთაშორისო ურთიერთობებს, ადამიანთა თავისუფლებებს, საზოგადოების თავდაჯერებულობას.
დონე - 2 საშუალო	შესაძლოა გავლენა იქონიოს საზოგადოებრივ ჯანმრთელობაზე ან უსაფრთხოებაზე, ეროვნულ უსაფრთხოებაზე, ეკონომიკურ უსაფრთხოებაზე, საერთაშორისო ურთიერთობებზე, ადამიანთა თავისუფლებებზე, საზოგადოების ნდობაზე.
დონე-1 დაბალი	ნაკლებ სავარაუდოა, რომ საფრთხე შეუქმნას საზოგადოებრივ ჯანმრთელობას ან უსაფრთხოებას, ეროვნულ უსაფრთხოებას, ეკონომიკურ უსაფრთხოებას, საერთაშორისო ურთიერთობებს, ადამიანთა თავისუფლებებს, საზოგადოების თავდაჯერებულობას.
დონე - 0 საბაზისო	უსაფუძვლო და არათანმიმდევრული შემთხვევა.

აღნიშნული სქემის მიხედვით, მესამე დონის (და ზევით) ინციდენტი მიეკუთვნება „მნიშვნელოვანი ინციდენტების“ კატეგორიას, რომლის დროსაც იქმნება **ერთიანი კოორდინაციის ჯგუფი,** რომელიც წარმოადგენს ეროვნულ მაკოორდინირებელ მექანიზმს ქვეყნის კიბერუსაფრთხოების უზრუნველყოფაში ჩართულ სახელმწიფო უწყებებს შორის (მნიშვნელოვანი კიბერინციდენტის შემთხვევაში). ჯგუფის კომპეტენციას ასევე განეკუთვნება კერძო სექტორის წარმომადგენლებისა და სახელმწიფო, ადგილობრივი და ტერიტორიული ორგანოების კოორდინაცია „მნიშვნელოვან კიბერინციდენტზე“ რეაგირების მიზნით. ერთიანი კოორდინაციის ჯგუფი შედგება ქვეყნის კიბერუსაფრთხოებაზე პასუხისმგებელი უწყებების ხელმძღვანელებისგან.

დიდი ბრიტანეთი

კიბერუსაფრთხოების უზრუნველყოფა და კოორდინაცია ეროვნულ დონეზე

დიდ ბრიტანეთში, კიბერუსაფრთხოების უზრუნველყოფაზე პასუხისმგებლობები შემდეგნაირადაა გადანაწილებული:

1. მთავრობის აპარატის (Cabinet Office) ეროვნული უსაფრთხოების სამდივნო - ეროვნულ დონეზე, კიბერუსაფრთხოების მართვა და კოორდინაცია

2. ეროვნული უსაფრთხოებისა და დაზვერვის სამსახურის (GCHQ) ეროვნული კიბერუსაფრთხოების ცენტრი (NCSC) - კიბერუსაფრთხოების უზრუნველყოფა ეროვნულ დონეზე

3. თავდაცვის სამინისტრო - კიბერთავდაცვა

4. საგამოძიებო უფლებამოსილების კომისრის ოფისი (Investigatory Powers Commissioner's Office) - სადაზვერვო უწყებების ზედამხედველობა

კიბერუსაფრთხოების სტრატეგიული მართვა ეკისრება მთავრობის აპარატს (Cabinet Office), სამინისტროს, რომელიც პასუხისმგებელია სამთავრობო უწყებების კოორდინირებასა და კიბერუსაფრთხოების ეროვნული სტრატეგიის შემუშავებაზე. მთავრობის აპარატი (Cabinet Office) უშუალოდ ექვემდებარება პრემიერ-მინისტრს. მთავრობის აპარატში (Cabinet Office) შექმნილი ეროვნული კიბერუსაფრთხოების სამდივნო (NSS), რომელსაც ხელმძღვანელობს ეროვნული უსაფრთხოების მრჩეველი, პასუხისმგებელია ეროვნული უსაფრთხოების საბჭოსთან, რომელიც შედგება პრემიერ-მინისტრისა და ეროვნული უსაფრთხოების უზრუნველყოფაზე პასუხისმგებელი სხვა მინისტრებისგან.

ოპერატიულ დონეზე, კიბერუსაფრთხოების უზრუნველყოფა ევალება NCSC-ს, რომელიც ასევე ითავსებს ეროვნული CERT-ის როლს.

NCSC-ის ფუნქციებში შედის კიბერუსაფრთხოების მიმართულებით საგანმანათლებლო საქმიანობა, ცნობიერების ამაღლება და ტრენინგი, კერძო სექტორის წარმომადგენლებთან თანამშრომლობა ინფორმაციის გაცვლისა და საუკეთესო პრაქტიკის გაზიარების მიზნით, კიბერუსაფრთხოების ტექნიკური შესაძლებლობების გაუმჯობესება, სამართალდამცავ უწყებებთან და საერთაშორისო პარტნიორებთან კოორდინაცია. NCSC პასუხისმგებელია სამთავრობო ქსელის უსაფრთხოების უზრუნველყოფასა და მონიტორინგზე.

GCHQ, რომელსაც ექვემდებარება NCSC, ფორმალურად პასუხისმგებელია საგარეო ოფისთან, თუმცა, აქტიურად თანამშრომლობს მთავრობის აპარატთან (Cabinet Office) და სხვა სამთავრობო უწყებებთან, მათ შორის, თავდაცვის სამინისტროსთან, ინფორმაციის მიმოცვლისა და საფრთხეების მართვის კუთხით.

ბრიტანეთის სადაზვერვო სამსახურები, სადაზვერვო ინფორმაციას (მათ შორის, კიბერსადაზვერვო ინფორმაციას) მთავრობას აწვდიან დამოუკიდებელი ორგანოს, გაერთიანებული სადაზვერვო კომიტეტის მეშვეობით (Joint Intelligence Committee).

თავდაცვის სამინისტრო პასუხისმგებელია კიბერთავდაცვით ღონისძიებებსა და სამხედრო მიზნებისთვის კიბერსივრცის გამოყენებაზე.

კრიტიკული ინფრასტრუქტურა და მასზე ზედამხედველობა

დიდ ბრიტანეთში კრიტიკული ინფრასტრუქტურა მოიცავს ინფრასტრუქტურის იმ კრიტიკულ ელემენტებს (ობიექტები, სისტემები, საიტები, ქონება, ინფორმაცია, ხალხი, ქსელები და პროცესები), რომელთა კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფამ შესაძლოა გამოიწვიოს მძიმე ეკონომიკური ან სოციალური შედეგი, ან სიცოცხლის დაკარგვა.

დიდი ბრიტანეთის ინფრასტრუქტურა 13 კრიტიკული სექტორისგან შედგება, რომელთაც ინდივიდუალური მარეგულირებელი (competent authority) ჰყავთ. ინდივიდუალური მარეგულირებლები ჰყავთ ქვესექტორებსაც.

კრიტიკული სექტორები და მათი მარეგულირებელი უწყებები:

სექტორი	მარეგულირებელი უწყება
ქიმიური	ბიზნესის, ენერგიისა და ინდუსტრიული სტრატეგიის დეპარტამენტი
ბირთვული (სამოქალაქო)	ბიზნესის, ენერგიისა და ინდუსტრიული სტრატეგიის დეპარტამენტი
კომუნიკაციები	კულტურის, მედიისა და სპორტის დეპარტამენტი
თავდაცვა	თავდაცვის სამინისტრო
გადაუდებელი დახმარების სერვისები	ჯანდაცვის დეპარტამენტი/ტრანსპორტის დეპარტამენტი/ შიდა საქმეების დეპარტამენტი (Home Office) - ერთობლივად
ენერგოსექტორი	ბიზნესის, ენერგიისა და ინდუსტრიული სტრატეგიის დეპარტამენტი
საფინანსო სექტორი	ეკონომიკისა და ფინანსთა სამინისტრო
საკვები პროდუქტები	გარემოს, კვებისა და აგრარულ საქმეთა დეპარტამენტი
სამთავრობო სექტორი	მთავრობის აპარატი (Cabinet Office)
ჯანდაცვა	ჯანდაცვის დეპარტამენტი
კოსმოსი	დიდი ბრიტანეთის კოსმოსის სააგენტო
ტრანსპორტი	ტრანსპორტის დეპარტამენტი
წყალი	გარემოს, კვებისა და აგრარულ საქმეთა დეპარტამენტი

ეროვნულ დონეზე, კრიტიკული ინფრასტრუქტურის დაცვაზე პასუხისმგებელია NCSC, რომელიც აღნიშნულ უფლებამოსილებას ახორციელებს კრიტიკული სექტორების მარეგულირებლების მეშვეობით და არა პირდაპირი არხებით. NCSC-ს აღნიშნული უფლებამოსილების განხორციელებაში დახმარებას უწევს ეროვნული ინფრასტრუქტურის დაცვის ცენტრი (CPNI). კრიტიკული სექტორის სუბიექტები ანგარიშვალდებულნი არიან

სექტორის მარეგულირებლებთან, ხოლო სექტორის მარეგულირებლები კი NCSC- თან. NCSC განსაზღვრავს ქვეყნის კრიტიკული ინფრასტრუქტურის რეგულირების მთავარ ჩარჩოს, რომლის შესაბამისად, ყველა მარეგულირებელი ვალდებულია მისი კომპეტენციის ფარგლებში დაქვემდებარებულ კრიტიკულ სექტორს განუსაზღვროს ვალდებულებები, გაუწეროს შესასრულებლად სავალდებულო ნორმები და უზრუნველყოს მათი ზედმიწევნით აღსრულება.

ეროვნული CERT პასუხისმგებელია სახელმწიფოს მასშტაბით ინციდენტების რეაგირებასა და მართვაზე, თუმცა, **მას არ აქვს წვდომა კრიტიკული ინფრასტრუქტურის სუბიექტების ინფორმაციულ სისტემებზე.** აღნიშნულ ინფორმაციას CERT იღებს სექტორის შესაბამისი მარეგულირებლისგან, ხოლო სექტორის მარეგულირებელი - მის დაქვემდებარებაში მყოფი სუბიექტისგან, გარდა ჯანდაცვის სექტორისა, სადაც ყველა დონის კიბერინციდენტზე რეაგირება ეროვნული ჯანდაცვის ციფრული სერვისების ორგანოს პასუხისმგებლობაა (NHS Digital).

2018 წელს მიღებული ქსელებისა და ინფორმაციული სისტემების შესახებ (Security of Network & Information Systems Regulation) რეგულაციის შესაბამისად, რომელიც ეფუძნება NIS დირექტივას, კრიტიკული ინფრასტრუქტურის სექტორებს ვალდებულება აქვთ მნიშვნელოვანი კიბერინციდენტის მოხდენიდან 72 საათის განმავლობაში შეატყობინონ NCSC-ს შესაბამის დანაყოფს. აღნიშნული რეგულაციის დაუმორჩილებლობა, ინციდენტისგან მიღებული შედეგის შესაბამისად **იწვევს სუბიექტის 17 მილიონ ფუნტ სტერლინგამდე დაჯარიმებას.** ჯარიმის ოდენობა განისაზღვრება ყველა კონკრეტული შემთხვევის შესაბამისად. ჯარიმა უნდა იყოს დარღვევის პროპორციული. კრიტიკული სუბიექტები ვალდებულნი არიან NCSC-ს მიაწოდონ ინფორმაცია ყველა მნიშვნელოვან ინციდენტზე, რომელიც საფრთხეს უქმნის სუბიექტის უსაფრთხოებას. თუ ინციდენტი შეიცავს სისხლის სამართლის დანაშაულის ნიშნებს, პროცესში ერთვება შესაბამისი სამართალდამცავი უწყებაც.

კრიტიკული ინფრასტრუქტურის სუბიექტები ვალდებულები არიან დაემორჩილონ NCSC-ს რეგულაციებს. NCSC ასევე ვალდებულია ჩაატაროს პერიოდული აუდიტი კრიტიკული ინფრასტრუქტურის სუბიექტებში. აუდიტის პერიოდულობა და პროცედურები გაწერილია ცალკე ბრძანებით და არ არის დაუგეგმავი.

ესტონეთი

კიბერუსაფრთხოების უზრუნველყოფა და კოორდინაცია ეროვნულ დონეზე

ესტონეთის რესპუბლიკაში კიბერაქტორების კოორდინაციას ახორციელებს ესტონეთის მთავრობის უშიშროების კომიტეტის კიბერუსაფრთხოების საბჭო, რომელიც პასუხისმგებელია კიბერუსაფრთხოების ეროვნული სტრატეგიით გათვალისწინებული ვალდებულებების შესრულების მონიტორინგზე. საბჭო სტრატეგიის სამოქმედო გეგმით გაწერილი აქტივობების შესრულებაზე ყოველწლიურად ამზადებს ანგარიშს და წარუდგენს მას მთავრობას.

ესტონეთში კიბერუსაფრთხოების პოლიტიკის ეროვნულ დონეზე მართვა **ეკონომიკისა და კომუნიკაციების სამინისტროს** პრეროგატივაა. სამინისტრო, ასევე, უზრუნველყოფს ელექტრონული სერვისების დანერგვასა და განვითარებას, ქვეყნის ინფორმაციული სისტემების გაძლიერებას და ესტონეთის, როგორც ინფორმაციული ტექნოლოგიების განვითარების კუთხით მოწინავე ქვეყნად ჩამოყალიბებას.

ეკონომიკისა და კომუნიკაციების სამინისტროს დაქვემდებარებაშია Estonian Information System Authority (RIA) **ესტონეთის ინფორმაციული სისტემების ორგანო.** აღნიშნული ორგანო უზრუნველყოფს სახელმწიფოს ინფორმაციული სისტემების ადმინისტრირებას, კოორდინირებას, განვითარებას, მათ შორის, კიბერინციდენტებზე რეაგირებასა და საგანგებო მზადყოფნას. RIA პასუხისმგებელია ესტონეთის ელექტრონული მმართველობის პლატფორმის ზედამხედველობაზეც, მათ შორის, ეროვნული ელექტრონული პერსონალური იდენტიფიცირების ინფრასტრუქტურასა და მონაცემთა გაცვლის ინფრასტრუქტურაზე (X-Road). გარდა ამისა, აღნიშნული ორგანო უზრუნველყოფს ადგილობრივი და სახელმწიფო უწყებებისთვის ინტერნეტ სერვისების მიწოდებას.

RIA-ს დაქვემდებარებაშია **ესტონეთის კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფი (CERT-EE),** რომელიც უზრუნველყოფს ესტონეთის კომპიუტერული ქსელების მონიტორინგსა და კიბერინციდენტებზე რეაგირებას. გარდა ამისა, CERT-EE უზრუნველყოფს მომხმარებელთა ცნობიერების ამაღლებას კიბერუსაფრთხოების სფეროში, მართავს მონაცემთა გაცვლის ინფრასტრუქტურას, ამზადებს ანგარიშებს ქვეყნის კიბერსივრცეში არსებულ საფრთხეებსა და განხორციელებულ ინციდენტებზე.

CERT-EE ადმინისტრირებას უწევს ე.წ. ვირტუალური სიტუაციების ოთახს (VSR). VSR წარმოადგენს კრიზისების მართვის პლატფორმას, რომლის მეშვეობით შესაძლებელია ინფორმაციის ერთ სივრცეში მიმოცვლა, როგორც კრიტიკული სერვისების ოპერატორების, ისე სახელმწიფო უწყებების მხრიდან. პლატფორმა მონაცემების ვიზუალიზაციის საშუალებასაც იძლევა, რაც აადვილებს მასზე არსებული ინფორმაციის აღქმადობას. VSR-ის მეშვეობით კრიზისის დროს, უწყებების მიერ განხორციელებული კომუნიკაციისა და არსებული სიტუაციის სრულად ჩაწერა ხდება, რაც სიტუაციისა და დაშვებული შეცდომების ანალიზისთვის გამოიყენება, რათა შემდგომი კრიზისული ვითარებისას იგივე შეცდომა არ განმეორდეს. გარდა ამისა, აღნიშნული პლატფორმა გამოიყენება ტრენინგების ჩასატარებლადაც.

ესტონეთის თავდაცვის სამინისტრო ეროვნულ დონეზე კოორდინირებას უწევს ქვეყნის კიბერთავდაცვას, ხოლო **კიბერთავდაცვის დეპარტამენტი,** რომელიც თავდაცვის სამინისტროში 2014 წლიდან ფუნქციონირებს, უშუალოდ პასუხისმგებელია თავდაცვის სისტემაში ინფორმაციული უსაფრთხოების პოლიტიკის დაგეგმვაზე, დანერგვასა და

ინფორმაციული და კომუნიკაციების ტექნოლოგიების განვითარებაზე.

ესტონეთის კიბერთავდაცვის დანაყოფი წარმოადგენს პროფესიონალთა კავშირს, რომელიც ანაზღაურების გარეშე (თუმცა, სხვა ბენეფიტების სანაცვლოდ) ემსახურება ქვეყნის კიბერთავდაცვას. მშვიდობის პერიოდში მისი მთავარი ფუნქციაა კიბერსაფრთხეებთან მიმართებით საზოგადოების ცნობიერების ამაღლება, ხოლო კრიზისის დროს დანაყოფი ეროვნულ CERT-EE-სთან ერთად იცავს ქვეყნის კიბერსივრცეს. დანაყოფის წევრებს არ მოეთხოვებათ, სპეციფიკური ტექნიკური ცოდნა და უნარები, გარდა გამონაკლისისა. მისი წევრები არიან სხვადასხვა სფეროს წარმომადგენლები, რომელთა ცოდნა და გამოცდილება კავშირშია კიბერუსაფრთხოებასთან.

2011 წელს, ესტონეთის თავდაცვის ლიგის დაქვემდებარებაში შეიქმნა **კიბერთავდაცვის დანაყოფი**, რომლის მიზანია მოხალისეთა ჩართვა ეროვნული კიბერთავდაცვის უზრუნველყოფაში. 2013 წელს მიღებული კანონის თანახმად, ლიგა წარმოადგენს საჯარო სამართლის იურიდიულ პირს, რომელიც ესტონეთის თავდაცვის ძალების შემადგენლობაში შევიდა, როგორც მოხალისეებისგან შემდგარი სამხედრო ორგანიზაცია, რომელიც ოპერირებს ესტონეთის თავდაცვის ძალების ზედამხედველობისა და მმართველობის ქვეშ.

2017 წლის დასაწყისში, ესტონეთის მთავრობამ დაამტკიცა „ეროვნული თავდაცვის განვითარების გეგმა 2017-2026“, რომლის თანახმადაც, ესტონეთის თავდაცვის ძალების შემადგენლობაში შეიქმნა **კიბერსარდლობის დანაყოფი**. ახალი დანაყოფი აღჭურვილია სამხედრო კიბეროპერაციების განხორციელების ტექნიკური და პროგრამული უზრუნველყოფის შესაძლებლობებით. დანაყოფის ფუნქციაა როგორც თავდაცვითი, ისე თავდასხმითი შესაძლებლობების განვითარება.

კრიტიკული ინფრასტრუქტურა და მასზე ზედამხედველობა

ესტონეთში, კრიტიკულ ინფრასტრუქტურას კურირებს (RIA), რომელიც წარმოადგენს არა-პოლიციურ, სამოქალაქო დაწესებულებას.

RIA უშუალოდ ზედამხედველობს ესტონეთის ყველა კრიტიკულ სექტორს, თუმცა აღნიშნული ზედამხედველობა არ მოიცავს სუბიექტების კონტროლს სხვადასხვა ტექნიკური საშუალებების მეშვეობით. ყველა კრიტიკული სუბიექტი ვალდებულია დაემორჩილოს უსაფრთხოების ნორმებს, რომლებსაც უწესებს RIA. ეს უკანასკნელი უფლებამოსილია შეამოწმოს, თუ რამდენად აკმაყოფილებს სუბიექტის ტექნიკური საშუალებები და ინფორმაციული უსაფრთხოების დოკუმენტაცია გაწერილ ნორმებს. საჭიროების შემთხვევაში, RIA ასევე უფლებამოსილია, ჰქონდეს წვდომა კრიტიკული სუბიექტის ინფორმაციულ სისტემაზე, თუ ეს წვდომა ემსახურება უშუალოდ ინციდენტის აღმოფხვრას და მასთან დაკავშირებულ პროცედურებს.

კრიტიკული სუბიექტი ვალდებულია დაუყოვნებლივ და არაუგვიანეს 24 საათისა შეატყობინოს ინფორმაცია RIA-ს მხოლოდ იმ ინციდენტებზე, რომლებმაც შესაძლოა გავლენა იქონიონ ეროვნულ უსაფრთხოებაზე ან შეაფერხონ სერვისის მიწოდება.

RIA-ს მიერ გაწერილი ვალდებულებების არშესრულება იწვევს კრიტიკული სუბიექტის დაჯარიმებას 20.000 ევრომდე.

ესტონეთის კრიტიკული ინფრასტრუქტურა მოიცავს შემდეგ სექტორებს:

1. ენერგეტიკა და ქსელები: ელექტროენერგია, ნავთობისა და გაზის საცავები, გადამცემი და სადისტრიბუციო სისტემები;

2. კომუნიკაცია და ინფორმაციული ტექნოლოგიები: სატელეკომუნიკაციო, გადაცემის და შეტყობინების სისტემები, პროგრამული უზრუნველყოფა, აპარატურა და ქსელები, მათ შორის, ინტერნეტის ინფრასტრუქტურა;

3. საფინანსო სისტემა: ბანკები, ინვესტიციები;

4. ჯანდაცვა: საავადმყოფოები, ჯანდაცვის ობიექტები, ლაბორატორიები და მედიკამენტები, საძიებო, სამაშველო და სასწრაფო დახმარების სამსახურები;

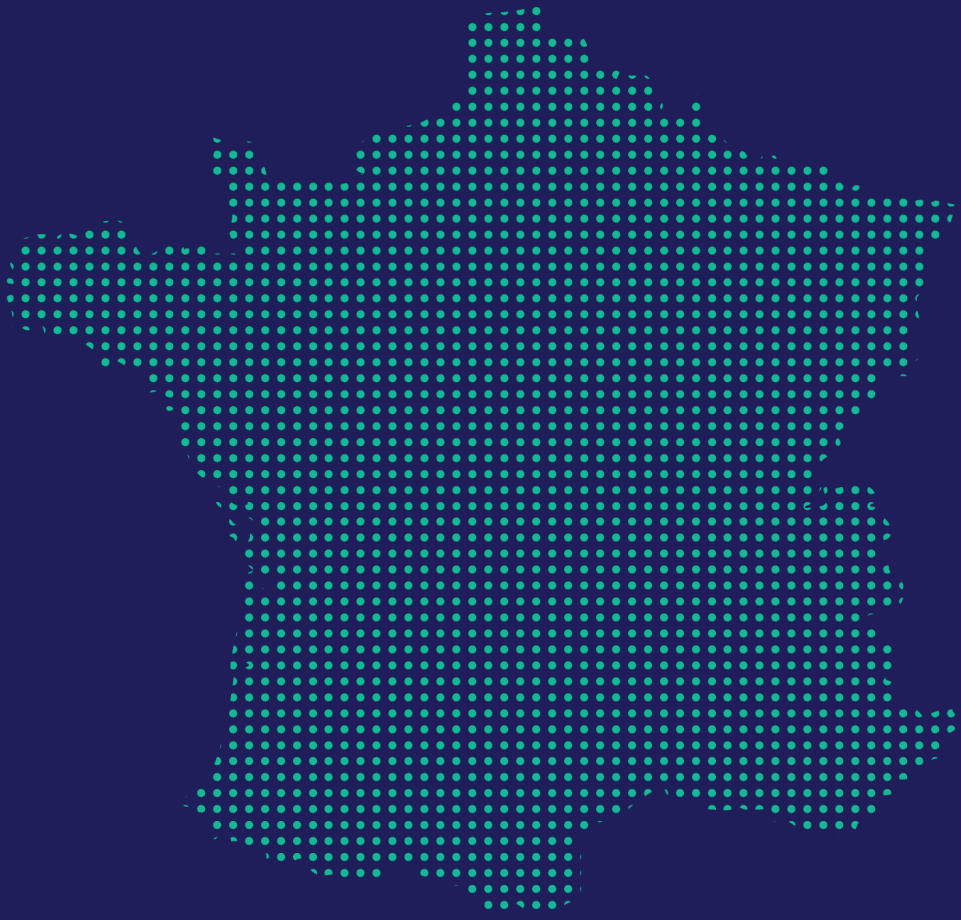
5. სურსათი: უსაფრთხოება, წარმოების საშუალებები, საბითუმო და კვების მრეწველობა;

6. წყალმომარაგება: წყალსაცავები, წყალსადენი და წყლის ქსელები

7. სატრანსპორტო სისტემა: აეროპორტები, პორტები, შუალედური სატრანსპორტო საშუალებები, სარკინიგზო და მასობრივი სატრანზიტო ქსელები, მოძრაობის მართვის სისტემები;

8. სახიფათო საქონლის წარმოება, შენახვა და ტრანსპორტირება: ქიმიური, ბიოლოგიური, რადიოლოგიური და სხვა სახიფათო მასალები;

9. სახელმწიფო ორგანოები: კრიტიკული სერვისები, სახელმწიფო ობიექტები, საინფორმაციო ქსელები, რომლებიც უზრუნველყოფენ ეროვნულ უსაფრთხოებასა და თავდაცვას, რესურსები, მონაცემთა ბაზები და სასამართლო რეესტრების ჩანაწერები, ეროვნული მნიშვნელობის კულტურული აქტივები.



საფრანგეთი

კიბერუსაფრთხოების უზრუნველყოფა და კოორდინაცია ეროვნულ დონეზე

საფრანგეთში, კიბერუსაფრთხოების პოლიტიკის განხორციელებაზე და ინფორმაციული სისტემების უსაფრთხოების წესების შემუშავებაზე პასუხისმგებელია პრემიერ-მინისტრი. ბრძანება, რომლის თანახმადაც შეიქმნა **საფრანგეთის ეროვნული ქსელებისა და ინფორმაციული უსაფრთხოების სააგენტო** (ANSSI) საფრანგეთის კიბერუსაფრთხოების პოლიტიკის ზოგადი ხელმძღვანელობის ფუნქციას აკისრებს ი**ნფორმაციული სისტემების უსაფრთხოების სტრატეგიულ კომიტეტს**. თავდაცვისა და ეროვნული უსაფრთხოების გენერალური მდივნის ზედამხედველობით, აღნიშნული კომიტეტი კოორდინაციას უწევს და ახორციელებს ინფორმაციული სისტემების უსაფრთხოებასთან დაკავშირებულ ღონისძიებებს.

გარდა თავდაცვისა და ეროვნული უსაფრთხოების გენერალური მდივნისა, ინფორმაციული სისტემების უსაფრთხოების სტრატეგიული კომიტეტის შემადგენლობაში შედიან:

- გენერალური შტაბის უფროსი;
- შინაგან საქმეთა სამინისტროს გენერალური მდივანი;
- საგარეო საქმეთა სამინისტროს გენერალური მდივანი;
- თავდაცვის შესყიდვების სააგენტოს დირექტორი;
- საგარეო დაზვერვის დირექტორატის დირექტორი;
- თავდაცვის ინფორმაციული და საკომუნიკაციო სისტემების დირექტორი;
- სახელმწიფოს ინფორმაციული და საკომუნიკაციო სისტემების დირექტორი;
- საზოგადოებრივი პოლიტიკის მოდერნიზაციის დირექტორი;
- შიდა დაზვერვის დირექტორატის დირექტორი;
- ეკონომიკის, ინდუსტრიის, ენერგეტიკისა და ტექნოლოგიების ეროვნული საბჭოს თანათავმჯდომარე;
- ეროვნული ქსელებისა და ინფორმაციული უსაფრთხოების სააგენტოს დირექტორი.

ANSSI წარმოადგენს ორგანიზაციას, რომელიც პასუხისმგებელია ინფორმაციული სისტემების უსაფრთხოებასთან დაკავშირებული ღონისძიებების კოორდინაციაზე. იგი აყალიბებს მთავრობის ელექტრონული უსაფრთხოების სტანდარტებს, ატარებს ინფორმაციული უსაფრთხოების სენსიტიური სახელმწიფო ინფრასტრუქტურის აუდიტს, კოორდინირებას უწევს კიბერინციდენტებზე სწორ რეაგირებას და მათ აღმოჩენას, ახორციელებს საერთაშორისო თანამშრომლობას და უტარებს ტრეინინგებს ადმინისტრაციის პერსონალს.

ANSSI-ის შემადგენლობაში შედის **საფრანგეთის კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი** (CERT), რომელიც პასუხისმგებელია ეროვნული მასშტაბით კიბერინციდენტების აღმოფხვრაზე. CERT რეგულარულად მონაწილეობს გამოძიებებში, როგორც იუსტიციის სისტემის დამხმარე ელემენტი.

საფრანგეთში, სამხედრო კიბერუსაფრთხოებას კურირებს თავდაცვის სამინისტრო. კიბერთავდაცვის გაერთიანებული დოქტრინის თანახმად, კიბერთავდაცვის დაგეგმვა შედის გენერალური შტაბის უფროსის ფუნქციებში.

კრიტიკული ინფრასტრუქტურა და მასზე ზედამხედველობა

საფრანგეთის კრიტიკული ინფრასტრუქტურის სექტორებზე ზედამხედველობას ახორციელებს - **ANSSI, რომელიც ექვემდებარება პრემიერ მინისტრს**, ხოლო სუბიექტებში უსაფრთხოების ნორმების დანერგვასა და შესრულებაზე პასუხისმგებელია სექტორის შესაბამისი სამინისტრო. სამინისტროები წარმოადგენენ კრიტიკული სუბიექტების მთავარ საკონტაქტო და ზედამხედველ უწყებებს. თითოეულ კრიტიკულ სუბიექტს, ინფორმაციული უსაფრთხოების ინდივიდუალური სტრატეგია და სამოქმედო გეგმა აქვს. სუბიექტი ვალდებულია დანიშნოს უსაფრთხოების სამოკავშირეო ოფიცერი, **რომელსაც ექნება საიდუმლო ინფორმაციაზე დაშვება და უშუალო კონტაქტი ANNSI-სთან.**

ANSSI ახორციელებს პერიოდულ ინსპექციას სუბიექტებში "Trust Service Providers" სისტემის მეშვეობით. Trust Service Providers წარმოადგენენ ANSSI-ს მიერ აკრედიტებულ ორგანიზაციებს და ინდივიდუალურ პირებს, რომლებიც იყოფიან 4 მიმართულებად: კიბერუსაფრთხოების აუდიტის სერვის პროვაიდერები, ინციდენტების აღმოჩენის სერვის-პროვაიდერები, ინტეგრაციაზე რეაგირების სერვის-პროვაიდერები და არქიტექტურის სერვის-პროვაიდერები. თავისთავად, აუდიტის პროცესი წინასწარ იგეგმება და თანხმდება სუბიექტთან.

საფრანგეთის არც ერთ საკანონმდებლო აქტში არ არის გაწერილი ANSSI-ის მიერ, ტექნიკური ზედამხედველობის პროცედურები. კრიტიკული სუბიექტები ვალდებულნი არიან თავად დანერგონ ქსელის მონიტორინგის ის საშუალებები, რაც უზრუნველყოფს ტრაფიკის კონტროლს და შესაბამისობაში იქნება ზედამხედველი უწყების მიერ გაწერილ მოთხოვნებთან.

საფრანგეთში, კრიტიკული ინფრასტრუქტურა დაყოფილია 4 მთავარ მიმართულებად, რომელიც მოიცავს 12 კრიტიკულ სექტორს. ყველა კრიტიკულ სექტორს ჰყავს მაკოორდინირებელი უწყება - სექტორის შესაბამისი სამინისტრო. სუვერენიტეტის მიმართულებაში შედის სამთავრობო სექტორი, რომლის კრიტიკული სისტემების უსაფრთხოებაზე უშუალოდ პასუხისმგებელია ANSSI.

საფრანგეთის კრიტიკული ინფრასტრუქტურის მიმართულებები და სექტორები:

ადამიანის ძირითადი საჭიროებები	სუვერენიტეტი	ეკონომიკა	ტექნოლოგიები
საკვები პროდუქტები	სამოქალაქო სფერო	ენერგოსექტორი	საკომუნიკაციო ტექნოლოგიები და ტელემაუწყებლობა
წყალმომარაგება	სამართლებრივი სფერო	საფინანსო სექტორი	ინდუსტრია
ჯანდაცვა	სამხედრო სფერო	ტრანსპორტი	კოსმოსი, კვლევა

გერმანია

კიბერუსაფრთხოების უზრუნველყოფა და კოორდინაცია ეროვნულ დონეზე

ინფორმაციული უსაფრთხოების ფედერალური ოფისი (BSI) წარმოადგენს გერმანიის მთავარ სამთავრობო უწყებას, რომელიც უზრუნველყოფს ქვეყნის ინფორმაციულ და კიბერუსაფრთხოებას ეროვნულ დონეზე. მის პასუხისმგებლობას განეკუთვნება:

- კრიტიკული ინფრასტრუქტურის დაცვა;
- კიბერუსაფრთხოების უზრუნველყოფა;
- კრიპტოგრაფია;
- უსაფრთხოების პროდუქტების სერტიფიცირება;
- უსაფრთხოების პროდუქტების ტესტირების ლაბორატორიების აკრედიტაცია.

BSI-ს ექვემდებარება **კიბერინციდენტებზე რეაგირების ეროვნული ჯგუფი** (CERT-BUND), რომლის ფუნქციებია:

- კიბერინციდენტების ანალიზი და მათზე რეაგირება;
- რეკომენდაციების შემუშავება შესაბამისი უწყებებისთვის;
- სხვა უწყებების დახმარება კიბერინციდენტების დროს;
- შესაბამისი უწყებების დროული გაფრთხილება მნიშვნელოვან კიბერსაფრთხეებზე.

BSI ოპერირებას უწევს **ინფორმაციული ტექნოლოგიების საინფორმაციო ცენტრს.** ცენტრის ფუნქციებია:

- კიბერინციდენტების შესახებ დროული შეტყობინების უზრუნველყოფა;
- კიბერინციდენტზე რეაგირება CERT-BUND-თან კოორდინაციით;
- კიბერსაფრთხეების შეფასება და საჯარო/კერძო სექტორის კოორდინირება საფრთხის აღმოჩენისას;

ცენტრი ახორციელებს სამთავრობო და პარტნიორი უწყებების ქსელების მონიტორინგს სპეციალური სენსორების მეშვეობით და 24/7 რეჟიმში ხელმისაწვდომია ფედერალური უწყებებისთვის და კრიტიკული სერვისების ოპერატორებისთვის.

2017 წელს გერმანიის მთავრობამ შექმნა კიბერ და ინფორმაციული დომენის სერვისი, რომელიც თავდაცვის სამინისტროს ექვემდებარება. აღნიშნული უწყების მთავარი ფუნქციაა სამხედრო ინფრასტრუქტურის წინააღმდეგ მიმართული კიბერთავდაცვითი ღონისძიებების განხორციელება.

კრიტიკული ინფრასტრუქტურა და მასზე ზედამხედველობა

გერმანიაში, კრიტიკული ინფრასტრუქტურა 7 სექტორს მოიცავს, რომლებიც თავის მხრივ მოიცავენ კრიტიკული ინფრასტრუქტურის სუბიექტებს. ეს კრიტიკული სექტორებია:

- ენერგეტიკა
- ინფორმაციული ტექნოლოგიები და ტელეკომუნიკაცია
- წყალი
- საკვები
- ჯანდაცვა
- ფინანსები და დაზღვევა
- ტრანსპორტი
- გერმანიაში, კრიტიკული ინფრასტრუქტურის უსაფრთხოებაზე პასუხისმგებელია პოლიციური ფუნქციების მქონე სახელმწიფო უწყება BSI, რომელიც ანგარიშვალდებულია გერმანიის შინაგან საქმეთა სამინისტროსთან.

BSI-ს უფლება აქვს კრიტიკული სუბიექტებისგან მოითხოვოს ინფორმაცია, გაანალიზოს მონაცემები და დაიწყოს საგამოძიებო საქმიანობა, საჭიროების შემთხვევაში მოიპოვოს წვდომა კრიტიკული სუბიექტის აქტივებზე, ქსელის მონიტორინგის ტექნიკურ და არატექნიკურ საშუალებებზე. ამგვარი წვდომა ხორციელდება კორპორატიული და პერსონალური ინფორმაციის დაცვით, არსებული კანონმდებლობის შესაბამისად. BSI-ს გააჩნია უფლებამოსილება საჭიროების შემთხვევაში განახორციელოს სუბიექტების ინფორმაციული სისტემების დისტანციური წვდომა და მართვა, თუ ამას მოითხოვს ინციდენტი, აღნიშნული უფლებამოსილება არ ხორციელდება თვითნებურად და დაუსაბუთებელი საფუძვლის გარეშე.

იმ შემთხვევაში, თუ კრიტიკული სუბიექტი დაარღვევს BSI-ს მოთხოვნებს, ადმინისტრაციული სახდელის მაქსიმალური ოდენობა განისაზღვრება 20 მილიონი ევროთი.

დანართი 2: ევროკავშირის კიბერუსაფრთხოების ჩარჩო

NIS დირექტივა

2016 წელს ევროპარლამენტმა მიიღო NIS დირექტივა, რომელიც მიზნად ისახავს კიბერუსაფრთხოების უზრუნველყოფის გაუმჯობესებას ევროკავშირის წევრ ქვეყნებში.

დირექტივის მიხედვით, ევროკავშირის ყველა წევრი ქვეყანა ვალდებულია:

- ეროვნული კანონმდებლობა მოიყვანოს დირექტივასთან შესაბამისობაში;
- მოახდინოს კრიტიკული სერვისების მომწოდებლების იდენტიფიცირება;
- შექმნას კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების დანაყოფი (CSIRT);
- შექმნას ეროვნულ კიბერუსაფრთხოებაზე პასუხისმგებელი ერთი ან რამდენიმე უწყება;
- წევრი ქვეყნები ვალდებულნი არიან ითანამშრომლონ ერთმანეთთან, შექმნან CSIRT-ის ქსელი, რომლის საშუალებითაც მოხდება ინფორმაციის მიმოცვლა ინციდენტებსა და კიბერრისკებზე;
- განსაზღვროს **კრიტიკული სექტორები** (ტრანსპორტი, წყალმომარაგება, ფინანსური მომსახურება, ჯანდაცვა) და კრიტიკული სერვისების მომწოდებლები, რომლებიც ოპერირებენ აღნიშნულ სექტორებში. **კრიტიკული სერვისების მომწოდებლები** და ციფრული მომსახურების მსხვილი მომწოდებლები ვალდებულნი არიან დანერგონ შესაბამისი უსაფრთხოების ზომები და კიბერუსაფრთხოების უზრუნველყოფაზე პასუხისმგებელ ეროვნულ უწყებას მიაწოდონ ინფორმაცია სერიოზული კიბერინციდენტების შესახებ. უნდა აღინიშნოს, რომ ელექტრონული კომუნიკაციებისა და სერვისების პროვაიდერები, არ წარმოადგენენ კრიტიკული ინფრასტრუქტურის სუბიექტებს და შესაბამისად, მათზე არ ვრცელდება ეს დირექტივა. აღნიშნული პროვაიდერების საქმიანობას არეგულირებს 2002/21/EC დირექტივა, რომელიც მათ ავალდებულებს მოთხოვნისთანავე მიაწოდონ ეროვნულ მარეგულირებელ უწყებას ნებისმიერი სახის ინფორმაცია (მათ შორის ფინანსური). ეროვნული მარეგულირებელი კი თავის მხრივ, ვალდებულია დაიცვას კონფიდენციალობის ყველა წესი და განუმარტოს სერვისის პროვაიდერებს, თუ რა მიზნით ითხოვს ინფორმაციას. ელექტრონული კომუნიკაციებისა და სერვისების პროვაიდერები ასევე ვალდებულნი არიან დაემორჩილონ GDPR-ის მოთხოვნებს პერსონალურ მონაცემთა დაცვის მიმართულებით. აღნიშნული დირექტივა არ მოიცავს კიბერუსაფრთხოების მარეგულირებელ ნორმებს პროვაიდერებისთვის.

დირექტივის მიხედვით, ევროკავშირის ყველა წევრი ქვეყანა ვალდებულია კრიტიკული სერვისების მიმწოდებლების იდენტიფიცირებისას გაითვალისწინოს შემდეგი კრიტერიუმები:

- ორგანიზაცია (სახელმწიფო, ან კერძო) უნდა უზრუნველყოფდეს ისეთი მომსახურების მოწოდებას, რომელიც აუცილებელია კრიტიკული სოციალური ან/და ეკონომიკური საქმიანობის განხორციელება-შენარჩუნებისთვის;
- აღნიშნული მომსახურების განხორციელება დამოკიდებული უნდა იყოს ქსელსა და ინფორმაციულ სისტემებზე;
- ინფორმაციული უსაფრთხოების ინციდენტის შემთხვევაში, აღნიშნული ორგანიზაციის

მიერ მომსახურების მიწოდების შეფერხების შედეგად უნდა დადგეს მ**ნიშვნელოვანი ზიანი**;

ამავე დირექტივით, **მნიშვნელოვანი ზიანი** განისაზღვრება შემდეგი გარემოებების გათვალისწინებით:

- იმ მომხმარებელთა რაოდენობა, რომლებიც დამოკიდებულნი არიან აღნიშნულ მომსახურებაზე;
- სხვა სექტორების დამოკიდებულება მოცემულ მომსახურებაზე;
- ზიანი, რომელიც შესაძლოა მიადგეს ქვეყნის ეკონომიკურ და საზოგადოებრივ საქმიანობასა და უსაფრთხოებას;
- ორგანიზაციის საბაზრო წილი;
- გეოგრაფიული გავრცელების არეალი;
- ინციდენტის შემთხვევაში, მომსახურების გაწევის ალტერნატიული გზების უზრუნველყოფის უნარი.

აღნიშნული კრიტერიუმების გათვალისწინებით, ევროპარლამენტის მიერ წარმოდგენილი კრიტიკული ინფრასტრუქტურის სექტორებისა და კრიტიკული მომსახურების მომწოდებლების სქემა მოიცავს შემდეგ მიმართულებებს:

სექტორი	ქვესექტორი	ორგანიზაციის ტიპი
1. ენერგოსექტორი	ა) ენერგომომარაგება	ენერგომომწოდებლები
		სადისტრიბუციო სისტემების ოპერატორები
		გადამცემი სისტემების ოპერატორები
	ბ) ნავთობი	ნავთობის სადისტრიბუციო მილსადენების ოპერატორები
		ნავთობის წარმოების, გადამუშავებისა და დამუშავების ობიექტები, შენახვისა და გადაცემის ოპერატორები
	გ) გაზი	მომმარაგებელი საწარმოები
		სადისტრიბუციო სისტემის ოპერატორები
		გადამცემი სისტემის ოპერატორები
		შემნახველი სისტემის ოპერატორები
		ბუნებრივი გაზის საწარმოები
		ბუნებრივი გაზის გადამამუშავებელი და გამწმენდი ნაგებობების ოპერატორები

2. სატრანსპორტო სექტორი	ა) საჰაერო ტრანსპორტი	საჰაერო გადამზიდები
		აეროპორტების მართვის ორგანოები; აეროპორტები და იურიდიული პირები, რომლებიც ახორციელებენ საინსტალაციო სამუშაოებს აეროპორტებში
		საჰაერო ტრანსპორტირების მართვაში ჩართული ოპერატორები
	ბ) რკინიგზა	სარკინიგზო ინფრასტრუქტურის მართვის ორგანოები
		სარკინიგზო ინფრასტრუქტურის საწარმოები, მათ შორის, მომსახურების მომწოდებელი ოპერატორები
	გ) საზღვაო ტრანსპორტი	შიდა, საზღვაო და სანაპირო სამგზავრო, ასევე საზღვაო ტვირთის გადამზიდი კომპანიები, ამავე კომპანიების მიერ ოპერირებული ცალკეული გემების გარდა
		პორტის მენეჯმენტი, მათ შორის საპორტო დაწესებულებები და ის ორგანიზაციები, რომლებიც უზრუნველყოფენ პორტის მუშაობასა და მის აღჭურვას
		სატვირთო გემების მიმოსვლის უზრუნველყოფაზე პასუხისმგებელი იურიდიული პირები
	დ) სახმელეთო ტრანსპორტი	ორგანოები, რომლებიც პასუხისმგებელნი არიან მოძრაობის მართვის კონტროლზე
		'ჭკვიანი სატრანსპორტო სისტემების' ოპერატორები
3. საბანკო სექტორი		საკრედიტო ინსტიტუტები
4. ფინანსური ბაზრის ინფრასტრუქტურა		სავაჭრო ობიექტების ოპერატორები
		მათი პარტნიორები
5. ჯანდაცვის სექტორი	ჯანდაცვის დაწესებულებები (მათ შორის საავადმყოფოები და კერძო კლინიკები)	სამედიცინო მომსახურების მიმწოდებლები

6. სასმელი წყლის მიწოდება და განაწილება		სასმელი წყლის მომმარაგებლები და დისტრიბუტორები, გარდა იმ დისტრიბუტორი კომპანიებისა, რომლებისთვისაც წყლისა და სხვა პროდუქტის მომარაგება ყოველდღიური საქმიანობაა და შესაბამისად, არ წარმოადგენს სასიცოცხლო მნიშვნელობის სერვისს
7. ციფრული ინფრასტრუქტურა		IXP (Internet Exchange Point) - ინტერნეტის მიმოცვლის წერტილი
		DNS (Domain Name System) - დომენური სახელების სისტემის პროვაიდერები
		TLD (Top-Level Domain) - იერარქიულად უმაღლესი დონის დომენების რეგისტრატორები

NIS დირექტივა ვრცელდება ორი ტიპის ორგანიზაციებზე: კრიტიკული სერვისების ოპერატორებზე და ციფრული სერვისების პროვაიდერებზე. კრიტიკული სერვისების ოპერატორები წარმოადგენენ ორგანიზაციებს, რომელთა მიერ მოწოდებული სერვისი მნიშვნელოვანია ეკონომიკური კეთილდღეობისა და საზოგადოების ნორმალური ფუნქციონირებისთვის და მოიცავს ისეთ კრიტიკულ ინფრასტრუქტურას, როგორებიც არის: ჯანდაცვა, ტრანსპორტირება, წყალმომარაგება, საფინანსო სექტორი და ა.შ.

ციფრული სერვისების პროვაიდერები კი წარმოადგენენ იმ ორგანიზაციებს, რომლებიც ოპერირებენ ციფრული სერვისების სფეროში, მაგალითად ონლაინ საძიებო სისტემები, ონლაინ გაყიდვებში ჩართული კომპანიები და ე.წ. „ღრუბლოვანი ტექნოლოგიების“ მომწოდებლები. NIS დირექტივა არ ვრცელდება ციფრული სერვისების იმ მომწოდებლებზე, რომელთა თანამშრომლების რაოდენობა არ აღემატება 50-ს ან/და წლიური ბრუნვა 10 მილიონ ევროს.

NIS დირექტივის შესრულება ხორციელდება **სექტორზე პასუხისმგებელი უწყებების მიერ (sector-specific competent authorities).** სექტორზე პასუხისმგებელი უწყება იგივეა რაც მარეგულირებელი უწყება (regulatory body). **მარეგულირებელ უწყებაში იგულისხმება სექტორის კიბერუსაფრთხოებაზე პასუხისმგებელი უწყება და არა სექტორის ბიზნეს საქმიანობის „მარეგულირებელი“ (შესაძლოა სექტორის საქმიანობის მარეგულირებელი არ იყოს ამ სექტორის კიბერუსაფრთხოებაზე პასუხისმგებელი. მაგალითად, საქართველოს მაგალითზე, არ არის აუცილებელი „სემეკი“ იყოს ენერგეტიკისა და წყალმომარაგების სექტორის კიბერუსაფრთხოებაზე პასუხისმგებელი უწყება.** ახალი კანონის შესაბამისად, კერძო სექტორის, მათ შორის საბანკო სექტორის კიბერუსაფრთხოებაზე პასუხისმგებელია ციფრული მმართველობის სააგენტო, შესაბამისად, სააგენტო არის ამ სექტორის მარეგულირებელი და არა ეროვნული ბანკი. ეროვნული ბანკი საბანკო სექტორის ბიზნეს საქმიანობის მარეგულირებელია). ყველა კრიტიკულ სექტორს

ერთი ან რამდენიმე მარეგულირებელი ჰყავს. კვლევაში წარმოდგენილ ქვეყნებში, სამთავრობო სექტორის მარეგულირებელს წარმოადგენს ის უწყება, რომელიც ეროვნულ დონეზე უზრუნველყოფს კიბერუსაფრთხოებას.

NIS დირექტივა აყალიბებს ინციდენტების რეპორტინგის ზოგად ჩარჩოს და კონკრეტულად არ განსაზღვრავს თუ როგორ უნდა იყოს ორგანიზებული ინციდენტების შეტყობინება ეროვნულ დონეზე. ევროკავშირის ქვეყნებში იკვეთება ინციდენტების შეტყობინების სამი ძირითადი მოდელი: კრიტიკული სერვისების ოპერატორები და ციფრული სერვისების პროვაიდერები **მნიშვნელოვანი** ინციდენტის შესახებ ინფორმაციას აწვდიან უშუალოდ **ეროვნულ CSIRT-ს;** კრიტიკული სერვისების ოპერატორები და ციფრული სერვისების პროვაიდერები მნიშვნელოვანი ინციდენტის შესახებ ინფორმაციას აწვდიან **სექტორის მარეგულირებელს, რომელიც, შემდგომ აღნიშნულ ინფორმაციას აწვდის ეროვნულ CSIRT-ს**; და მესამე მოდელი, როდესაც ერთ ქვეყანაში, სექტორების ნაწილს ინდივიდუალური მარეგულირებლები ჰყავთ და მათ ატყობინებენ ინციდენტებს. ამავდროულად, სექტორების ნაწილი ინფორმაციას ინციდენტების შესახებ უშუალოდ აწვდის ეროვნულ CSIRT-ს. კვლევაში მოყვანილი ქვეყნების კრიტიკულ სექტორებს ჰყავთ ინდივიდუალური მარეგულირებლები, და ინციდენტები პირველ რიგში მათ მიეწოდებათ.

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR)

2018 წლის 25 მაისს ძალაში შევიდა ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია, რომელიც ვრცელდება ევროკავშირში რეგისტრირებულ ნებისმიერ ორგანიზაციაზე, რომელიც საქმიანობის ფარგლებში ამუშავებს პერსონალურ მონაცემებს. გარდა ამისა, რეგულაცია ვრცელდება იმ ორგანიზაციებზეც, რომლებიც არ არიან რეგისტრირებული ევროკავშირში, თუმცა ამუშავებენ ევროკავშირში მყოფი პირების მონაცემებს. აღნიშნული რეგულაციის მიხედვით, მონაცემთა დამუშავება კანონიერია, თუ გათვალისწინებულია შემდეგი გარემოებები:

- პირმა გამოხატა თანხმობა მისი მონაცემების ერთი, ან მეტი კონკრეტული მიზნით დამუშავებაზე;
- დამუშავება აუცილებელია პირთან დადებული ხელშეკრულების შესასრულებლად, ან მისივე თხოვნით ხელშეკრულების მოსამზადებლად;
- დამუშავება აუცილებელია ორგანიზაციისთვის კანონმდებლობით დაკისრებული მოვალეობის შესასრულებლად;
- დამუშავება აუცილებელია პირის სასიცოცხლო ინტერესების დასაცავად;
- დამუშავება აუცილებელია საჯარო ინტერესიდან გამომდინარე ფუნქციების, ან ორგანიზაციისთვის, კანონით მინიჭებული უფლებამოსილების განსახორციელებლად;
- დამუშავება აუცილებელია ორგანიზაციის ან მესამე პირის კანონიერი ინტერესების დასაცავად.

რეგულაციის მიხედვით, მონაცემთა უსაფრთხოების დარღვევა არის ინციდენტი, რომელ-

მაც გამოიწვია პერსონალურ მონაცემთა შემთხვევითი ან არაკანონიერი განადგურება, დაკარგვა, შეცვლა, გამჟღავნება, ან მათზე უკანონო წვდომა.

ევროკავშირის ყველა წევრი ქვეყანა ვალდებულია განსაზღვროს პერსონალურ მონაცემთა დაცვაზე პასუხისმგებელი უწყება/უწყებები. **იმ შემთხვევაში, თუ ირღვევა მონაცემთა უსაფრთხოება, ორგანიზაციამ დარღვევის აღმოჩენიდან არაუგვიანეს 72 საათისა უნდა შეატყობინოს პერსონალურ მონაცემთა დაცვაზე პასუხისმგებელ ორგანოს** და იმ პირებს, რომელთაც შეეხოთ აღნიშნული ინციდენტი. ამასთან, იმ შემთხვევაში, თუ პერსონალურ მონაცემთა უსაფრთხოების დარღვევას თან ახლავს კიბერინციდენტი, მისი შეტყობინება ხორციელდება NIS დირექტივით გაწერილი პროცედურების შესაბამისად.

პერსონალურ მონაცემთა უსაფრთხოების დარღვევისას, პერსონალურ მონაცემთა დაცვაზე პასუხისმგებელი ორგანოსათვის შეტყობინება უნდა მოიცავდეს:

- მონაცემთა უსაფრთხოების დარღვევის ხასიათს და დაზარალებულთა რაოდენობას;
- მონაცემთა უსაფრთხოების დარღვევის სავარაუდო შედეგებს;
- ორგანიზაციის მიერ გატარებულ ღონისძიებებს;
- ინციდენტის შესახებ მეტი ინფორმაციის მისაღებად საკონტაქტო პირის მონაცემებს.

ორგანიზაციები ვალდებულნი არიან აღრიცხონ მონაცემთა უსაფრთხოების დარღვევის ყველა შემთხვევა და მიღებული ზომები. ორგანიზაციებს ასევე ევალებათ მონაცემთა უსაფრთხოების პოლიტიკის შემუშავება, ინციდენტების გამოვლენისა და მათზე რეაგირების გეგმები.

რეგულაციის წესების დარღვევა იყოფა ორ ძირითად კატეგორიად: 1. თუ ორგანიზაციამ დაარღვია შეტყობინების ვალდებულებები; 2. თუ ორგანიზაციამ დაარღვია პირის თანხმობასთან დაკავშირებული წესები. პირველ შემთხვევაში, ჯარიმის მაქსიმალური ოდენობა შეადგენს 10 მილიონ ევროს, ან წლიური ბრუნვის 2%-ს, ხოლო მეორე შემთხვევაში, ჯარიმის მაქსიმალური ოდენობაა 20 მილიონი ევრო, ან ორგანიზაციის წლიური ბრუნვის 4%.

ინფორმაციის თავისუფლების განვითარების ინსტიტუტი (IDFI)

ტ. შევჩენკოს ქ. 20, თბილისი 0108; + 995 32 2 92 15 14

info@idfi.ge www.idfi.ge