ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №6

2021 წლის 14 დეკემბერი

ქ. თბილისი

საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-8 მუხლის მე-4 პუნქტის, „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტის, „ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონის 25-ე მუხლისა და „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ 2021 წლის 10 ივნისის №632-IVმს-Xმპ საქართველოს კანონის მე-2 მუხლის მე-2 პუნქტის „ვ“ ქვეპუნქტის შესაბამისად, **ვბრძანებ:**

1. დამტკიცდეს „კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის საქმიანობის წესი“.
2. ძალადაკარგულად გამოცხადდეს „კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის უფლებამოსილებისა და საქმიანობის წესის დამტკიცების შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2020 წლის 16 ოქტომბრის №1 ბრძანება.
3. ეს ბრძანება ამოქმედდეს 2021 წლის 30 დეკემბრიდან.

სსიპ ციფრული მმართველობის
სააგენტოს თავმჯდომარე — დავით ნადირაშვილი

კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის საქმიანობის წესი

მუხლი 1. წესის მიზანი

ამ წესით დგინდება საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს (შემდგომ – სააგენტო) კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის – CERT.DGA.GOV.GE (შემდგომ – დახმარების ჯგუფი) კომპეტენცია, მუშაობის პროცედურები, კომპიუტერულ ინციდენტებზე რეაგირების მექანიზმები, მესამე პირებთან ურთიერთობის პრინციპები, აგრეთვე მის საქმიანობასთან დაკავშირებული სხვა წესები.

მუხლი 2. დახმარების ჯგუფის მანდატი

1. დახმარების ჯგუფის უფლებამოსილებას ახორციელებს სააგენტოს კიბერუსაფრთხოების დეპარტამენტი.

2. დახმარების ჯგუფი, საქართველოს კანონმდებლობით განსაზღვრული უფლებამოსილების ფარგლებში, უზრუნველყოფს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის აღსრულებას, საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, აგრეთვე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ და მასთან დაკავშირებულ სხვა საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება.

3. თავისი საქმიანობის განხორციელებისას, დახმარების ჯგუფი ხელმძღვანელობს პრიორიტეტული საფრთხეებით, რომელიც განსაზღვრულია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-8 მუხლის მე-2 პუნქტით, ასევე, საქართველოს კიბერუსაფრთხოების სტრატეგიითა და სამოქმედო გეგმით.

4. დახმარების ჯგუფის უფლებამოსილება მოიცავს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-2 მუხლის „ზ[3]“ ქვეპუნქტით განსაზღვრულ მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების (შემდგომ – მესამე კატეგორიის სუბიექტი) მიერ კიბერუსაფრთხოების უზრუნველყოფასთან დაკავშირებული მოვალეობების შესრულების ზედამხედველობასა და მათ მხარდაჭერას.

5. გარდა ამ წესით გათვალისწინებული ფუნქციების შესრულებისა, დახმარების ჯგუფი ასევე მონაწილეობს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით სააგენტოსთვის დაკისრებული ფუნქციების შესრულებაში.

მუხლი 3. დახმარების ჯგუფის ფუნქციები

1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით გათვალისწინებული უფლებამოსილების ფარგლებში, დახმარების ჯგუფის ფუნქციებია:

ა) კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა ან/და ამავე კანონით გათვალისწინებულ შემთხვევებში სახელმძღვანელო მითითებების გაცემა;

ბ) კომპიუტერული ინციდენტების დროული გამოვლენა;

გ) კომპიუტერულ ინციდენტებზე რეაგირება და მათზე რეაგირების კოორდინაცია;

დ) კომპიუტერული ინციდენტების აღრიცხვა და მათზე რეაგირების პრიორიტეტების დადგენა და კატეგორიზაცია;

ე) კომპიუტერული ინციდენტების ანალიზი;

ვ) კომპიუტერული ინციდენტების შედეგების გამოსწორებისა და ზიანის მინიმუმამდე შემცირების პროცესში დახმარება;

ზ) კომპიუტერული ინციდენტების პრევენციისკენ მიმართული ზომების კოორდინაცია და ამ ზომების დანერგვაში დახმარება;

თ) კიბერუსაფრთხოების საკითხებზე საზოგადოების საგანმანათლებლო კამპანიითა და სათანადო ინფორმაციით უზრუნველყოფა;

ი) შესაძლო საფრთხეების შესახებ მოსახლეობის ფართო წრის გაფრთხილება და მისთვის სათანადო ინფორმაციის მიწოდება;

კ) თავისი კომპეტენციის ფარგლებში საერთაშორისო დონეზე ინფორმაციული უსაფრთხოების საკითხებზე წარმომადგენლობა;

ლ) კიბერუსაფრთხოების საკითხებზე საზოგადოების ცნობიერების ამაღლება.

2. დახმარების ჯგუფი უფლებამოსილია, შეასრულოს სხვა მოვალეობები, რომლებიც დაკავშირებულია კიბერუსაფრთხოების სფეროში მისთვის დაკისრებული ამოცანების შესრულებასთან და განისაზღვრება კანონით ან სხვა ნორმატიული აქტით.

მუხლი 4. კომპიუტერული ინციდენტების აღმოჩენა

1. დახმარების ჯგუფი კომპიუტერული ინციდენტების შესახებ ინფორმაციას მოიპოვებს შემდეგი არხებით:

ა) „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-10 მუხლის მე-7 პუნქტით გათვალისწინებული კომპიუტერული ინციდენტის შესახებ ინფორმაციის გაზიარების ერთიანი

პლატფორმიდან;

ბ) „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის 8^1 მუხლის პირველი პუნქტის „ვ“ ქვეპუნქტით გათვალისწინებული კიბერინციდენტების გაზიარების პლატფორმიდან – ინციდენტების ავტომატიზებული მართვის სისტემიდან;

გ) მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებისგან სხვადასხვა ტექნიკური საშუალებით, მათ შორის, ელექტრონული ფოსტით, ფაქსით, ტელეფონით და სხვა;

დ) საერთაშორისო პარტნიორი ორგანიზაციების წყაროებისა და სისტემებისგან;

ე) დამოუკიდებლად, საჯაროდ ხელმისაწვდომი წყაროებიდან (ინტერნეტით, ტელევიზიით და სხვა).

2. კომპიუტერული ინციდენტების შესახებ შეგროვებული ინფორმაციის საფუძველზე დახმარების ჯგუფი ქმნის და ადმინისტრირებას უწევს კიბერინციდენტების რეესტრს.

მუხლი 5. ორგანიზაციებისა და სისტემების უსაფრთხოების შეუსაბამობების/სისუსტეების აღმოჩენა და მონიტორინგი

1. ორგანიზაციებისა და სისტემების უსაფრთხოების შეუსაბამობების/სისუსტეების აღმოჩენის მიზნით, დახმარების ჯგუფი ახორციელებს სისტემების მონიტორინგთან დაკავშირებულ საქმიანობას, მათ შორის:

ა) მესამე კატეგორიის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტთან ერთად, ამავე სუბიექტის ქსელური სენსორების კონფიგურაციას, მისი გამართულად ფუნქციონირებისა და მონიტორინგის მხარდაჭერას;

ბ) უსაფრთხოებასთან დაკავშირებული ინფორმაციისა და ხდომილებების მართვის სისტემის კონფიგურაციასა და მისი გამართულად ფუნქციონირების მხარდაჭერას;

გ) უსაფრთხოებასთან დაკავშირებული ინფორმაციისა და ხდომილებების მართვის სისტემიდან მიღებული ინფორმაციის ანალიზს;

დ) სხვადასხვა ქსელური, სერვერულ-ინფრასტრუქტურული მოწყობილობისა და საბოლოო მომხმარებლების კომპიუტერული მოწყობილობების ჩანაწერების (ლოგფაილების) ანალიზს;

ე) ქსელური მოწყობილობების კონფიგურაციის აუდიტს;

ვ) საწყისი პროგრამული კოდის ანალიზს;

ზ) ვებაპლიკაციების შეღწევადობის (პენეტრაციის) ტესტირებას.

2. დახმარების ჯგუფი ახორციელებს კომპიუტერულ ინციდენტებზე რეაგირების პრიორიტეტიზაციას „კომპიუტერული ინციდენტების კლასიფიცირების წესის განსაზღვრის შესახებ“ საქართველოს მთავრობის დადგენილების გათვალისწინებით.

მუხლი 6. კომპიუტერულ ინციდენტებზე რეაგირება

1. დახმარების ჯგუფი:

ა) აანალიზებს ინციდენტს და ამზადებს შესაბამის ანგარიშს;

ბ) დახმარებას უწევს მესამე კატეგორიის სუბიექტს კომპიუტერული ინციდენტების შედეგების გამოსწორებისა და ზიანის მინიმუმამდე შემცირების პროცესში.

2. კომპიუტერულ ინციდენტის გაანალიზების პროცესში დახმარების ჯგუფმა შესაძლოა კომპიუტერულ ინციდენტებზე მოიპოვოს მტკიცებულებები და ჩაატაროს ექსპერტიზა. ექსპერტიზის

შედეგად დახმარების ჯგუფის მიერ მომზადებული ანგარიში შესაძლოა მოიცავდეს სავალდებულო მითითებებს, რომელიც წარედგინება მესამე კატეგორიის სუბიექტს. შესასრულებლად სავალდებულო მითითება არ შეიძლება ითვალისწინებდეს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელურ სენსორზე ან ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე წვდომის ვალდებულებას.

3. კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია გონივრულ ვადაში მოახდინოს დახმარების ჯგუფის შესასრულებლად სავალდებულო მითითებაზე რეაგირება და განახორციელოს შესაბამისი ღონისძიებები. განხორციელებული ღონისძიებების შესახებ ინფორმაციას მესამე კატეგორიის სუბიექტი წარუდგენს დახმარების ჯგუფს.

4. კომპიუტერულ ინციდენტებზე რეაგირების პროცესში დახმარების ჯგუფი ხელმძღვანელობს „კომპიუტერული ინციდენტების კლასიფიცირების წესის განსაზღვრის შესახებ“ საქართველოს მთავრობის დადგენილებით.

მუხლი 7. ურთიერთობა კრიტიკული ინფორმაციული სისტემის სუბიექტთან

1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის III თავის მოთხოვნათა დაცვით, დახმარების ჯგუფი კომუნიკაციას ამყარებს მესამე კატეგორიის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერთან/კომპიუტერული უსაფრთხოების სპეციალისტთან.

2. დახმარების ჯგუფი უფლებამოსილია, მოითხოვოს და მესამე კატეგორიის სუბიექტის თანხმობის შემთხვევაში, ჰქონდეს წვდომა ამ სუბიექტის ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე, თუ ასეთი წვდომა აუცილებელია მესამე კატეგორიის სუბიექტის სისტემაში მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე რეაგირებისთვის.

3. დახმარების ჯგუფის მოთხოვნა მესამე კატეგორიის სუბიექტის ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე წვდომაზე განსახილველად მიეწოდება სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერს. ინფორმაციული უსაფრთხოების მენეჯერი მოთხოვნის გონივრულ ვადაში განხილვის შემდეგ დახმარების ჯგუფს დაუყოვნებლივ აცნობებს აღნიშნულ წვდომაზე თანხმობის ან უარის შესახებ.

4. კომპიუტერული ინციდენტის იდენტიფიცირების ან/და მასზე რეაგირების მიზნით დახმარების ჯგუფი უფლებამოსილია მესამე კატეგორიის სუბიექტის თანხმობით ჰქონდეს წვდომა ამ სუბიექტის ქსელურ სენსორზე. ქსელური სენსორის კონფიგურირებასა და მართვას დახმარების ჯგუფი და მესამე კატეგორიის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტი ერთობლივად ახორციელებენ.

5. სააგენტო ვალდებულია დაიცვას იმ ინფორმაციის კონფიდენციალურობა, რომელიც შესაძლოა მისთვის ცნობილი გახდეს ამ მუხლით გათვალისწინებულ შემთხვევებში.

6. თუ კომპიუტერული უსაფრთხოების სპეციალისტი ან ინფორმაციული უსაფრთხოების მენეჯერი ვერ ასრულებს მასზე დაკისრებულ მოვალეობას, მესამე კატეგორიის სუბიექტმა უნდა განსაზღვროს შესაბამისი თანამშრომელი (თანამშრომლები), რომელსაც მიენიჭება გადაუდებელი ღონისძიებების განხორციელების უფლებამოსილება.

7. თუ დახმარების ჯგუფი ან/და მესამე კატეგორიის სუბიექტი საჭიროდ ჩათვლის, დახმარების ჯგუფისა და ინფორმაციული უსაფრთხოების მენეჯერის ან/და კომპიუტერული უსაფრთხოების სპეციალისტის ურთიერთობა ხორციელდება დაცული კავშირის, დაშიფრული გზავნილების ან/და ინფორმაციის დაცვის სხვა საშუალებებით.

8. ამ წესით განსაზღვრული, ასევე სხვა დაკავშირებული საკითხების განსაზღვრის მიზნით, სააგენტოსა და მესამე კატეგორიის სუბიექტს შორის შესაძლებელია გაფორმდეს თანამშრომლობის მემორანდუმი.

მუხლი 8. ცნობიერების ამაღლება, საგანმანათლებლო საქმიანობა, შესაძლებლობების ზრდა და კონსულტაცია

1. დახმარების ჯგუფი ჩართულია ეროვნულ დონეზე კიბერუსაფრთხოების სფეროში საგანმანათლებლო და ცნობიერების ამაღლების კამპანიების, აგრეთვე ამ სფეროების სპეციალისტების შესაძლებლობების ზრდის მიზნით ერთობლივი კიბერსავარჯიშოებისა და კიბერსწავლების ღონისძიებების ჩატარების პროცესში, და საამისოდ იგი ახორციელებს:

ა) საქართველოს კიბერუსაფრთხოების ფორუმის კოორდინაციასა და ორგანიზაციულ მხარდაჭერას;

ბ) ინფორმაციული უსაფრთხოების და კიბერუსაფრთხოების საკითხებზე საზოგადოების საგანმანათლებლო კამპანიას და სათანადო ინფორმაციით მის უზრუნველყოფას;

გ) ტრენინგების, სემინარებისა და საჯარო ლექციების ორგანიზებას, მათ შორის, კიბერჰიგიენის და კიბერინციდენტებზე რეაგირების საბაზისო ტრენინგების ჩატარებას;

დ) ეროვნული კიბერსავარჯიშოების ჩატარებას კერძო და საჯარო სექტორისთვის;

ე) ეროვნული კიბეროლიმპიადის, კიბერ კლასის ჩატარებას სტუდენტებისთვის და სკოლის მოსწავლეებისთვის;

ვ) შესაძლო საფრთხეების, სისუსტეებისა და განახლებების შესახებ მოსახლეობის ფართო წრისა და ორგანიზაციების გაფრთხილებას და სათანადო ინფორმირებას სხვადასხვა არხის (მათ შორის, სოციალური ქსელის) საშუალებით;

ზ) კიბერუსაფრთხოების საკითხებზე საზოგადოების ცნობიერების ამაღლებას.

2. დახმარების ჯგუფი მესამე კატეგორიის სუბიექტებს აძლევს რეკომენდაციას, უზიარებს გამოცდილებას და კანონით გათვალისწინებულ შემთხვევებში გასცემს შესასრულებლად სავალდებულო მითითებებს.

მუხლი 9. საერთაშორისო წარმომადგენლობა

დახმარების ჯგუფი, საერთაშორისო წარმომადგენლობის უზრუნველყოფის მიზნით, უფლებამოსილია:

ა) თავისი კომპეტენციის ფარგლებში, ურთიერთობა დაამყაროს კიბერუსაფრთხოების სფეროში მოქმედ ადგილობრივ, საერთაშორისო და უცხო ქვეყნების ორგანიზაციებთან, საჯარო დაწესებულებებსა და კერძო სამართლის სუბიექტებთან, თანამშრომლობის ფარგლებში ჩაერთოს ინფორმაციის ურთიერთგაცვლის პროცესში, ასევე მონაწილეობა მიიღოს კიბერუსაფრთხოების საერთაშორისო ღონისძიებებში;

ბ) კიბერუსაფრთხოების სფეროში მიმდინარე ადგილობრივ, რეგიონულ და საერთაშორისო პროგრამებსა და პროექტებში მონაწილეობით ხელი შეუწყოს ამ სფეროში საქართველოს მიღწევების პოპულარიზაციას;

გ) ითანამშრომლოს კიბერუსაფრთხოების სფეროში მოქმედ საერთაშორისო და რეგიონულ ორგანიზაციებთან, უცხო ქვეყნის შესაბამის სტრუქტურებთან.