კიბერუსაფრთოება და მასთან დაკავშირებული გამოწვევები გლობალური პანდემიის პირობებში

ზურაბ გორგოძე

თომას ჯეფერსონის კვლევითი ცენტრის საერთაშორისო ურთიერთობების

ოფისის ხელმძღვანელი

ფოთი 2020

შესავალი

კიბერუსაფრთხოება ან IT უსაფრთხოება, ეხება ისეთი ტექნოლოგიური მოწყობილობების უსაფრთხოებას, როგორიცაა კომპიუტერები და სმარტფონები, ასევე კომპიუტერული ქსელები, როგორც პირადი და საზოგადოებრივი, ასევე ინტერნეტი. კიბერუსაფრთხოების სფერო მზარდ მნიშვნელობას იძენს უმეტეს საზოგადოებაში კომპიუტერული სისტემებისადმი დამოკიდებულების გამო. ეს ეხება ტექნიკის, პროგრამული უზრუნველყოფის, მონაცემების, ადამიანების დაცვას და ასევე იმ პროცედურებს, რომლითაც სისტემებზე წვდომა ხდება. კომპიუტერული უსაფრთხოების საშუალებები მოიცავს სისტემების ფიზიკურ უსაფრთხოებას და მათზე დაცული ინფორმაციის უსაფრთხოებას.

ზოგადად, უსაფრთხოების კონცეფციაში არსებული 7 ძირითადი მიმართულებიდან, კიბერუსაფრთხოებას პირველი ადგილი უკავია, ვინაიდან მის წინაშე არსებულ გამოწვევებთან უმოქმედობამ შესაძლოა სახელმწიფოს კონვენციური დაპირისპირებასთან შედარებით, უფრო დიდი ზიანი მიაყენოს.

ტექნოლოგიურმა რევოლუციამ და კომპიუტერული ტექნიკის მზარდმა მოხმარებამ, საგრძნობლად გაზარდა კიბერუსაფრთხოების მნიშვნელობა, რის შედეგადაც სახელმწიფოებმა შეიმუშავეს კიბერუსაფრთხოების სტრატეგიები(ევროკავშირისა და ნატოს წევრი ქვეყნებიდან პირველი იყო ესტონეთი, 2007 წელი) და გაზარდეს ბიუჯეტი რათა დაეხვეწათ მათი კიბერ ინფრასტრუქტურა. ამასთან, ევროპარლამენტმა 2016 წლის მაისში, პირველად გამოაქვეყნა ზოგად მონაცემთა დაცვის რეგულაცია(GDPR), რომელიც ევროკავშირის ქვეყნების მოქალაქეთა პირადი ინფორმაციის დაცვას უზრუნველყოფს.

2020 წელს COVID-19 - ახალი კორონა ვირუსის, გლობალურ პანდემიად გამოცხადებამ, შედეგად მოგვიტანა ინტერნეტ სივრცის მოხმარების ზრდა და ტექნოლოგიური განვითარება ახალ ფაზაში შეიყვანა. კორონა ვირუსმა ინფორმაციული ტექნოლოგიები სხვა კუთხით წარმოაჩინა. კომპანიები, კორპორაციები, საჯარო და კერძო დაწესებულებები ონლაინ მუშაობის რეჟიმში გადავიდა, რამაც შეიძლება ითქვას, ამ ტენდენციას სამომავლოდ საკმაოდ მყარი ნიადაგი შეუქმნა. ონლაინ მუშაობის რეჟიმზე გადასვლისა და ინტერნეტის

მოხმარების საგრძნობლად გაზრდის საპირწონედ, გაიზარდა გამოწვევები კიბერდამნაშავეთა მხრიდან, რადგან ინტერნეტ სივრცე არასდროს ყოფილა ისეთი მოწყვლადი, როგორიც დღეს, ამის უგულველსაყოფად და სტაბილურობის შესანარჩუნებლად კი საჭიროა კიბერუსაფრთხოებითი ელემენტების დახვეწა და მათი ეფექტიანად ამუშავება.

პანდემიის გავლენა ციფრულ ქცევასა და კიბერ ინფრასტრუქტურაზე

დღეს, ყველაფერმა ინტერნეტ სივრცეში ძალიან დიდი დოზით გადაინაცვლა, რისი პროგნოზირებაც გასულ 2019 წელს შეიძლება ითქვას, შეუძლებელიც კი იყო. ინტერნეტის მოხმარებასთან ერთად გამოიკვეთა საფრთხეებიც, რომელიც სამთავრობო კომუნიკაციებსა და მათ შორის, საერთაშორისო ორგანიზაციების ონლაინ ვიდეო კოფერენციების მუშაობის რეჟიმთან არის დაკავშირებული. აღნიშნული, განსაკუთრებით მომხიბვლელი გახდა სპეცსამსახურებისა და ჰაკერებისთვის. ინფორმაციის გავრცელების საფრთხეები, რომელიც შეიძლება ეხებოდეს სახელმწიფო საიდუმლოებას და მსგავს სენსიტიურ თემებს, უფრო მეტად გაიზარდა. ასევე სკოლები და უნივერსიტეტები გადავიდნენ ონლაინ მუშაობის რეჟიმში რამაც გამოიწვია სხვადასხვა აპლიკაციების შექმნა და მათი მოხმარების ზრდა. აღსანიშნავია ის ფაქტი, რომ ნიუ-იორკ-ში სკოლებმა დაბლოკეს „ზუმი“-ს მოხმარება, რადგან კვლევებმა აჩვენა, რომ მისი მოხმარება შესაძლოა მომხმარებელთა პირადი ინფორმაციის მოპარვით დასრულებულიყო.

გამომდინარე იქიდან, რომ მომხმარებლები გადადიან ონლაინ რეჟიმში, ასევე გაიზარდა ელექტრონული კომერციების რიცხვი და მათი შესაბამისად ელექტრონული ტრანზაქციები, რაც ქმნის კონკრეტულ საფრთხეს როგორც თითოეული მომხმარებლისთვის, ასევე დიდი და მცირე, კერძო, თუ საჯარო დაწესებულებებისთვის.

დაავადების გავრცელებამ უდიდესი გავლენა იქონია ინტერნეტის მომხმარებელთა ციფრულ ქცევაზე არა მხოლოდ დაზარალებულ რაიონებში, არამედ მთელ მსოფლიოში. გლობალურ დონეზე, ისეთი ავტორიტეტები, როგორებიც არიან

ჯანდაცვის მსოფლიო ორგანიზაცია(WHO) და ჩინეთის ჯანმრთელობის ეროვნული კომისია(NHC) იყენებენ ციფრულ სისტემებს, ინფექციების ბუნებისა და მასშტაბების შესახებ ინფორმაციის გაგზავნისთვის და მისაღებად, რათა ინფორმირებული ჰყავდეთ მოსახლეობა, თუ როგორ უნდა მოიქცნენ ისინი ვირუსის თავიდან ასაცილებლად და ასევე, თუ რა უნდა გააკეთონ მათ, ინფიცირების შემთხვევაში. უნდა აღინიშნოს ის ფაქტიც, რომ ჩინეთის ხელისუფლებამ გამოაქვეყნა მობილური აპლიკაცია, რომელიც აკონტროლებს ხალხს და აწვდის მათ ინფორმაციას იმის შესახებ, იყვნენ თუ არა ისინი ახლო კონტაქტში კორონავირუსით ინფიცირებულ პირთან.

მსგავსი ტენდენცია შეინიშნა საქართველოშიც, როდესაც მობილური ტელეფონების სხვადასხვა სააპლიკაციო სისტემებში გამოჩნდა აპლიკაცია, სახელწოდებით “Stop Covid”, რომელიც გამოშვებიდან დაახლოებით 24 საათში დაახლოებით 150 000-მა მომხმარებელმა გადმოიწერა. აპლიკაცია არ ითხოვს რეგისტრაციას, მაგრამ ითხოვს ნებართვას მიკროფონსა და ლოკაციაზე, რამაც ძალიან ბევრი ადამიანი დააფიქრა, გამოეყენებინა თუ არა ეს აპლიკაცია, რადგან მათ ეჭვი შეიტანეს მის უსაფრთხოებაში. აღნიშნულის საფრთხის თეორიული რისკი არსებობს, ვინაიდან შესაძლოა მოხდეს აპლიკაციის განახლება და ახალი ფუნქციების დამატება, რამაც შესაძლოა გაზარდოს აპლიკაციის მეშვეობით მომხმარებელთა უფრო მეტ ინფორმაციაზე წვდომა.

კიბერუსაფრთხოება ძირითადად ფოკუსირებულია მომხმარებელთა მონაცემების უნებართვოდ შეცვლის ან გამოყენების თავიდან აცილებაზე, რადგან კიბერთაღლითობები საფრთხეს უქმნიან ციფრული ინფორმაციის კონფიდენციალურობას. სიტყვა კორონავირუსი, ალბათ, დღეს ერთ-ერთი ყველაზე ძებნადი სიტყვაა მთელ ინტერნეტ სივრცეში, ხოლო მიზეზი კი აშკარაა. საძიებო სისტემა, ეს არის პროგრამა, რომელიც ინტერნეტში ან ვებგვერდზე, ტექსტური საკვანძო სიტყვების გამოყენებით მონაცემების უფრო სწრაფ მოძიებაში გვეხმარება. ინტერნეტ საძიებო სისტემები ამჟამად გადატვირთულია სხვადასხვა საკვანძო სიტყვებით, რომლებიდანაც ძირითადად გამოიკვეთება შემდეგი სიტყვები: კორონა, ვირუსი, კორონავვირუსი, COVID-19, ჩინეთი, ვუჰანის დაავადება და სხვა, პანდემიასთან დაკავშირებულ საკვანძო სიტყვებს. კორონავირუსის გავრცელებასთან

დაკავშირებული განახლებული ინფორმაციების სიმრავლემ და მათმა მოძიებამ საგრძნობლად გადატვირთა ინტერნეტ ქსელი, რამაც გაზარდა მავნე კოდური მახასიათებლებით სარგებლობის შესაძლებლობა კიბერ დამნაშავეებისთვის, რაც ამავდროულად ქმნის კორონავირუსთან დაკავშირებული ინფორმაციის შენიღბვას და მისი ავთენტურობის დამახინჯებას.

ადამიანის სენსიტიური და კონფიდენციალური ინფორმაციის შეგროვების ხელოვნება მისივე სისუსტეების გამოყენებით, კიბერსფეროში ცნობილია, როგორც სოციალური ინჟინერია. სოციალური ინჟინერია არის ფსიქოლოგიური ექსპლუატაცია, რომელსაც კიბერსკამერები (პირები, რომლებიც თავდასხმის, კიბერთავდასხის მეშვეობით მოიპოვებენ სხვადასხვა კონფიდენციალურ ინფორმაციებს) იყენებენ ადამიანების ოსტატურად მანიპულირებისთვის და უდანაშაულო ადამიანებზე ემოციური შეტევების ჩასატარებლად. სოციალური ინჟინერიის მეთოდები ფსიქოლოგიურ ხრიკებს იყენებენ მომხმარებლების მოსატყუებლად. სოციალური ინჟინერია ეს არის ფსიქოლოგიური მანიპულაცია და შეტევა, რომლის დროსაც გარეშე პირი სისტემაზე ან ქსელზე მონოპოლირების მოპოვების მიზნით ანხორციელებს მოტყუების გზით მომხმარებლის გამოკითხვას და ამისათვის იყენებს E-mail-ს, სატელეფონო ზარს, პირად მიმოწერას ან პირზე ფსიქოლოგიურ დაკვირვებას. ამ ფორმით ის გებულობს ავტორიზირებული მომხმარებლის მონაცემებს და მათ საფუძველზე ახერხებს სისტემაზე ან ქსელზე წვდომას. კიბერდამნაშავეები კარგად იყენებენ სოციალურ ინჟინერიას, რათა თავს დაესხან დაუცველ მსხვერპლს, მოიპოვონ კონფიდენციალური ინფორმაცია და ამგვარი ინფორმაციის გამოყენებით განახორციელონ სხვა შეტევები. კორონავირუსის შემთხვევაში, კიბერდამნაშავეები ამჟამად იყენებენ ფიშინგის მოწინავე ფორმას, რომელსაც უწოდებენ Spear Phishing, რომელიც მიზნად ისახავს გავლენიანი პიროვნებების ან სხვადასხვა კორპორაციული გაერთიანებებისგან ინფორმაციის მოპოვებას.

პირადი ინფორმაციების მოპოვების მიზნით, ბოლო პერიოდში ყველაზე მოწყვლად ობიექტებად იქცა სამედიცინო დაწესებულებები. კერძო სამედიცინო ობიექტების კომპიუტერული სისტემის დაცვა თვითონ ამ ობიექტის პასუხისმგებლობას წარმოადგენს. აუცილებლად საყურადღებოა სამედიცინო დაწესებულებების კიბერ

ინფრასტრუქტურის დასახვეწად სხვადასხვა რეკომენდაციების შემუშავება და მათთვის უსაფრთხო სამუშაო გარემოს შექმნა, მითუმეტეს მაშინ, როდესაც რეცეპტების, წამლების და სხვადასხვა ოპერაციების შესრულება სამედიცინო დაწესებულებებში ელექტრონულად მიმდინარეობს.

აღსანიშნავია, რომ პანდემიის პირობებში საგრძნობლად გაიზარდა ელექტრონული კომერციები და ონლაინ მაღაზიები, სადაც ძირითადად გადახდა ელექტრონული ტრანზაქციების საშუალებით მიმდინარეობს. სოციალურ მედიაში ბოლო ხანებში ძალიან ბევრი ონლაინ მაღაზიის გვერდი შეიქმნა, რომლებიც შეიძლება ყალბი ან კლონირებული ვებ-გვერდების იმიტაციას წარმოადგენდნენ. ხშირად, მსგავს გვერდებს მასპინძლობენ კიბერკრიმინალები, რომლებმაც შესაძლოა მოიპარონ პირადი ინფორმაცია, გავლენა იქონიენ ფინანსებთან დაკავშირებულ საკითხებზე ან ჩაშალოს სხვადასხვა ციფრული ოპერაციები.

როგორც ზევით აღინიშნა, გლობალური პანდემიის პირობებში უკვე წამოვიდა და კიდევ უფრო გაიზარდა ონლაინ მაღაზიებისა და ელექტრონული კომერციების ტენდენციები, შესაბამისად იზრდება კიბერდამნაშავეთა ინტერესის სფერო აღნიშნული მიმართულებით. ელექტრონული კომერციების ფონზე, ასევე, იზრდება ელექტრონული ტრანზაქციები, მაგრამ მათი უსაფრთხოება დაცული არ არის ისე, როგორც დიდ კორპორაციებში. მაშასადამე, მანამ, სანამ ონლაინ ტრანზაქცია განხორციელდება, აუცილებელია გაითვალისწინოთ, რომ :

- ვებ-გვერდებზე მართლწერისა და გრამატიკული შეცდომები. არათანმიმდევრული გრამატიკული გამონათქვამები სიყალბის ნიშანია.
- უნდა დააკვირდეთ ვებ-გვერდზე ურთიერთსაწინააღმდეგო განცხადებებსა და ორაზროვან ინსტრუქციებს.
- დააკვირდით ინსტრუქციებს, რომლებიც გულისხმობს გადაუდებელ მოქმედებას, განსაკუთრებით ისეთ ცნობილ კრიტიკულ შემთხვევასთან დაკავშირებით, როგორიც არის კორონავირუსის დაავადება.
- ხშირად ვებსაიტზე განთავსებულია ორაზროვანი საკონტაქტო მონაცემები, მათ შორის მიუწვდომელი ტელეფონის ნომრები, არასწორი ელ-ფოსტის მისამართები, ფიზიკური ან იურიდიული მისამართები, არასწორი აღნიშვნები

და მრავალი სხვა დეტალი, რომლების გამოსახულებაც საეჭვოა და ასევე შეიცავს სიყალბის ნიშნებს.

ზემოთ ჩამოთვლილის გათვალისწინებით, თქვენ შეძლებთ თავიდან აირიდოთ თქვენი საბანკო და საფინანსო ინფორმაციის, კიბერდამნაშევათა მხრიდან მოპარვის შესაძლებლობა. არ მიაწოდოთ თქვენი საბანკო ინფორმაცია საეჭვო ვებ-გვერდებს, მანამ სანამ არ დარწმუნდებით მათ ავთენტიკურობაში, რომლის დადგენაც შესაძლებელია, მომხმარებელთა მომსახურების პერსონალთან კონტაქტით ან ელ-ფოსტის მეშვეობით კომუნიკაციით.

დეზინფორმაცია გლობალური პანდემიის პირობებში

ახალი კორონავირუსის გავრცელებამ და მსოფლიო მოსახლეობისთვის დაწესებულმა შეზღუდვებმა, პირადი თავისუფლების, ეკონომიკური საქმიანობისა და საზოგადოებრივი ცხოვრების სფეროების მიმართულებით, თავდაყირა დააყენა მილიარდობით ადამიანის ცხოვრება. მძლავრ ციფრულ პლატფორმებს აქვთ შესაძლებლობა, გაავრცელონ ინფორმაციები ძალიან სწრაფად, ამავე შესაძლებლობების პირობებში, კიბერდამნაშავეებს ასევე შეუძლიათ მიმოქცევაში ყალბი ან მცდარი შინაარსის მქონე ინფორმაციების შემუშავება, რაც კიდევ უფრო დიდ საფრთხეს უქმნის მოსახლეობის კეთილდღეობას. მნიშვნელოვანია ინფორმაციის გადამოწმება რაც შეიძლება მალე, მაგრამ სამწუხაროდ, ყველას ამის შესაძლებლობა არ გააჩნია.

კორონავირუსულმა კრიზისმა გამოიწვია გლობალური, ონლაინ დეზინფორმაციის, კიბერ-შპიონაჟისა და ოპერაციათა ჩაშლის ზრდა. რომელშიც ჩართულია ათეულობით ქვეყანა, მაგრამ ყველაზე მნიშვნელოვნად რუსეთი და ჩინეთი სახელდება. პანდემიის პირობებში, რომელსაც ათობით ათასი ადამიანი ემსხვერპლა, სხვადასხვა ანალიტიკოსებმა შეამჩნიეს, რომ ჰაკერების მხრიდან საერთაშორისო ორგანიზაციებზე (რომლებიც კორონავირუსის წინააღმდეგ რეაგირებას ცდილობენ) თავდასხმის მცდელობების პარალელურად, სოციალურ მედიაში მიზანმიმართული დეზინფორმაციული კამპანიების მკვეთრი ზრდის ტენდენცია შეინიშნებოდა.

Sputnik News - მა 22 იანვარს გამოაქვეყნა სტატია, რომ კორონავირუსის გავრცელება უკავშირდებოდა ნატოს და ეს მათ მიერ შექმნილი იარაღი იყო. ეს გახლდათ კორონა ვირუსის შესახებ პირველი მცდარი ინფორმაცია, რომელიც სოციალურ ქსელებში გავრცელდა. ასევე, Sputnik-ის არაბულმა ვერსიამ, გამოქვეყნა სტატია, რომელიც კორონა ვირუსის შექმნას ამერიკის ლაბორატორიებს აბრალებდა. ამ ინფორმაციების მიზანს წარმოადგენდა, სამიზნე ჯგუფებში კონსპირაციული თეორიის შესახებ სხვადასხვა განწყობების შექმნა და მასების მანიპულაცია დასავლური სამყაროს წინააღმდეგ.

რუსეთი წარმატებით ამუშავებს პროპაგანდისტულ მანქანას და დეზინფორმაციის გავრცელების საშუალებით უკვე წლებია ახდენს სხვადასხვა სახელმწიფოში, გარკვეული სოციალური ჯგუფებზე გავლენას და მათ მანიპულირებას, რაც საფრთხეს უქმნის დემოკრატიის პრინციპებს.

რუსეთისა და ჩინეთის დუეტს, ემატება ირანიც, რომელიც ამ ორ ქვეყანასთან ერთად COVID-19-ის გლობალურ პანდემიასთან დაკავშირებით დეზინფორმაციას ავრცელებს. ეს შესაძლოა იყოს კომპლექსური კამპანია, რომელიც მიმართულია დასავლეთის ქვეყნების მიმართ მსოფლიო საზოგადოების ნდობის შემცირებისკენ. აღსანიშნავია, რომ პანდემიის პირობებში სამივე სახელმწიფო მსგავს ყალბ ნარატივებს ავრცელებს.

გაცვეთილი რუსული პროპაგანდის სტილში სპუტნიკი წერდა, რომ პენტაგონის მიერ დაფინანსებული ბიოლოგიური ლაბორატორიები მთელ მსოფლიოში იყვნენ ჩართული COVID-19-ის შექმნაში. როგორც მოსალოდნელი იყო, ამ ხშირად გამეორებული კონსპირაციული თეორიის ცენტრში აღმოჩნა საქართველოში არსებული ლუგარის ლაბორატორიაც. ამ ამბავმა სხვადასხვა ენაზე მასობრივი გავრცელების სახე მიიღო ტვიტერზე, ფეისბუქსა და სხვა სოციალური მედიის პლატფორმებზე.

სინამდვილეში, საქართველოში არსებული ლუგარის ლაბორატორია არის COVID-19-ის პანდემიის წინააღმდეგ ბრძოლის მთავარი საყრდენი. ლაბორატორია გაიხსნა 2011 წელს, შეერთებული შტატების დახმარებით, ინფექციურ დაავადებებთან საბრძოლველად. ლუგარის ლაბორატორია არის კრიტიკულად მნიშვნელოვანი

დაწესებულება პოტენციურად სასიკვდილო ვირუსების აღმოჩენისა და რეაგირებისთვის, მათ გავრცელებამდე. საქართველოს მთავრობა ეცადა მოეწვია რუსი ექსპერტები ლაბორატორიის დასათვალიერებლად, თუმცა მოსკოვმა უარი თქვა ამ ვიზიტზე, რადგან ამით ხელი შეეშლებოდა კრემლის პროპაგანდის დღის წესრიგს.

თანამედროვე ტექნოლოგიურ სამყაროში, დეზინფორმაცია ერთ-ერთი ყველაზე მძლავრი იარაღია, რომელიც ხშირად სახელმწიფოს შიგნით ახდენს კონფლიქტების გენერირებას, რაც საფრთხეს უქმნის, როგორც ლოკალურ, ასევე ქვეყნის ეროვნულ ინტერესებს. დეზინფორმაცია ძალიან დიდი გამოწვევაა, როგორც ადამიანის უსაფრთხოების, ასევე, ეროვნული უსაფრთხოებისთვისაც. გლობალურმა პანდემიამ და მსოფლიო მოსახლეობის ინტერნეტზე დამოკიდებულებამ ამ გამოწვევას, რეალიზების კიდევ უფრო მძლავრი შესაძლებლობა მისცა, რადგან სწორედ ამ პირობებში ცდილობს გააქტიურებას დეზინფორმატორთა და კიბერდამნაშავეთა ჯგუფები. დეზინფორმაციის უმეტესობა დაკავშირებულია კორონა ვირუსთან. ზოგიერთი დეზინფორმაცია დაკავშირებულია ვაქცინის შექმნასთან, ზოგიერთი სხვადასხვა სამკურნალო საშუალებებთან კორონა ვირუსის წინააღმდეგ. მაგალითისთვის შეიძლება მოვიყვანოთ ადამიანი, რომელმაც ცხელი წყალი დალია იმ მიზნით, რომ ეგონა, ეს იქნებოდა ვირუსთან ბრძოლის ერთ-ერთი მექანიზმი. იგივე შეიძლება ითქვას არყით მკურნალობასთან დაკავშირებულ ინფორმაციებზე, რომლებიც ძირითადად საზოგადოების შეცდომაში შეყვანას ემსახურება.

საინტერესოა ის ფაქტიც, რომ ზოგიერთი ვებ-გვერდი მომხმარებელს თხოვს რეგისტრაციას, რათა ნახონ კორონა ვირუსთან დაკავშირებული ესა თუ ის ინფორმაცია, რაც საფრთხის შემცველია და მომხმარებლებს მათი პირადი ინფორმაციის გაცემისკენ უბიძგებს. გამომდინარე აქედან, ინტერნეტ სივრცის მომხმარებლებმა, აუცილებლად უნდა დაიცვან კიბერჰიგიენა, რადგან არ გახდნენ კიბერშეტევების მსხვერპლნი, რამაც შესაძლოა მათი ფინანსური ან ფსიქიკური მდგომარეობის დაზიანება გამოიწვიოს.

დაკვნა

დასკვნის სახით, შეიძლება ითქვას, რომ გლობალური პანდემიის პირობებში ინტერნეტ სივრცეზე დამოკიდებულების ზრდიდან გამომდინარე, საგრძნობლად შეიცვალა თითოეული ინდივიდის ცხოვრების სტილი და სხვადასხვა დაწესებულებების, ორგანიზაციების, კომპანიებისა და კორპორაციების მოქმედებათა ხასიათი. გლობალურმა გამოწვევამ, COVID-19-ის სახით შექმნა საზოგადოებრივი განწყობა მთელი მსოფლიოს მასშტაბით, რომ მსოფლიო აღარ იქნება ისეთი, როგორც იყო პანდემიამდე. აღნიშნული მდგომარეობის გამოყენება და ათვისება კარგად შეძლო კიბერდამნაშავეებმა და შესაბამისად, კიბერდანაშაულის დონეც წინა წლებთან შედარებით გაიზარდა. ნაშრომში განხილული საკითხებიდან გამომდინარე ნათლად ჩანს, რომ კომპანიები, ორგანიზაციები და სხვადასხვა საჯარო თუ კერძო დაწესებულებები პოსტ-პანდემიურ რეალობაში, მოქმედების სრულიად ახალ ეტაპზე გადავლენ და ეცდებიან ახალი ტენდენციების დანერგვას.

პირადი მონაცემების გავრცელების თავიდან აცილების მიზნით, აუცილებელია, მომხმარებლებმა დაიცვან კიბერჰიგიენა, რათა თავიდან აიცილონ კიბერთავდასხმით გამოწვეული პრობლემები.

გლობალური პანდემია გახდა დეზინფორმატორთათვის საუკეთესო მოვლენა, რომლემაც შესაძლოა საფრთხე შეუქმნას ინდივიდუალურ, ლოკალურ და ეროვნულ უსაფრთხოებას.

გამოყენებული ლიტერატურა

- B. Atkins and W. Huang, "A study of social engineering in online frauds," Open Journal of Social Sciences- 2013.
- Tackling the Cybersecurity impacts of the Coronavirus outbreak as a challenge to internet safety – Kenneth Okereafor – National Health Insurance Scheme. Olajide Adebola – The University of Edinburgh.
- COVID-19: Impact on the Cyber Security Threat Landscape – Francois Mouton – Noroff University College. Arno de Coning – North West University South Africa.
- https://e-estonia.com/estonia-as-an-international-cybersecurity-leader/
- https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/
- https://www.cnbc.com/2020/02/10/china-launches-coronavirus-app-to-detect-whether-users-have-come-in-close-contact-with-the-sick.html.
- https://pia.ge/ka/news/covid-19/stop-covid-aplikatsia-24-saatshi-150-000-ze-metma-pirma-gadmotsera/
- https://netgazeti.ge/news/444042/
- https://en.unesco.org/news/disinformation-silent-weapon-times-pandemic
- https://www.dw.com/en/disinformation-and-propaganda-during-the-coronavirus-pandemic/a-52970643
- https://euvsdisinfo.eu/disinformation-can-kill/
- https://www.gfsis.org/ge/blog/view/1067
- https://techcrunch.com/2020/04/05/zoom-new-york-city schools/?fbclid=IwAR1OePLOBSclQiibhOh6QfuWuseu4pk_Fv0QVKgh8-ee6rdutqoMpRbOaNs.