Georgian Scientists
ქართველი მეცნიერები
Vol. 5 Issue 1, 2023
https://doi.org/10.52340/gs.2023.05.01.28

ინფორმაციული უსაფრთხოება და კიბერუსაფრთხოება

გულნარა კოტრიკაძე
საქართველოს ტექნიკური უნივერსიტეტი, ინფორმატიკისა და მართვის სისტემების ფაკულტეტი, ასოცირებული პროფესორი

აბსტრაქტი

ციფრული ტრანსფორმაციის ერაში მნიშნელოვნად გაიზარდა დამოკიდებულება ინფორმაციული ტექნოლოგიების სერვისებზე და პროდუქტებზე. შესაბამისად გაიზარდა გამოწვევები ინფორმაციულ უსაფრთხოებისა და კიბერუსაფრთხოების მიმართულებით.

სოციალური დისტანცია, მიუხედავად იმისა, რომ უმნიშვნელოვანეს როლს ასრულებს COVID-19-ის გავრცელების შეკავების პროცესში, ზრდის სამუშაო სადგურების დაინფიცირების, არასანქცირებული წვდომების, მონაცემთა გაჟონვის, მავნე კოდის გაშვებისა და ყველა იმ ტიპის რისკს, რომელიც თან ახლავს დაუცველ გარემოში მუშაობას.

კომპიუტერული უსაფრთხოება, კიბერუსაფრთხოება ან ინფორმაციული უსაფრთხოება - კომპიუტერული სისტემებისა და ქსელების მართვის წერტილების დაცულობა მისი ხელყოფისგან, არასანქცირებული გამოყენებისგან ან აპარატული უზრუნველყოფის, პროგრამული უზრუნველყოფისა და ელექტრონული მონაცემებისადმი ზიანის მიყენებისგან, აგრეთვე განადგურებისა და დარღვევისგან სერვისებისა, რომლებსაც ისინი მომხმარებელს აწვდიან.

ეს სფერო უფრო და უფრო მნიშვნელოვანი ხდება კომპიუტერულ სისტემებზე, ინტერნეტზე და უკაბელო ქსელებზე, როგორიცაა Bluetooth და wi-fi. მისი კომპლექსურობის გამო, პოლიტიკისა და ტექნოლოგიის კუთხით, კიბერუსაფრთხოება აგრეთვე არის ერთ-ერთი ძირითადი გამოწვევა თანამედროვე ცხოვრებაში.

კიბერუსაფრთხოება დღევანდელ მსოფლიოში ერთ-ერთ ყველაზე მნიშვნელოვანი დარგია. სწორედ, ამ დარგს უკავშირდება ისეთი მოთხოვნადი პროფესიები და სპეციალობები როგორებიცაა: უსაფრთხოების ანალიტიკოსი, უსაფრთხოების ინჟინერი, უსაფრთხოების არქიტექტორი, უსაფრთხოების ადმინისტრატორი, უსაფრთხოების სპეციალისტი, კონსულტანტი და ა.შ.

მავნე პროგრამების სახეობები -

- მალვეარი (*Malware*);
- კომპიუტერული ვირუსი;
- მოძრავი მედია საშუალებები;
- ტროიანი (*Trojan Horse*);
- რუტკიტი;

- ბექდორი (*Backdoor*);
- ვორმი (*Computer worm*);
- კილოგერი (*Keylogger*).

2003 წელს კომპიუტერულმა ვირუსმა Slammer-მა ელექტროგამანაწილებელი ქსელის მართვის სისტემაში შეაღწია და მისი მუშაობა შეანელა, რამაც მართვის სისწრაფის შენელებაც გამოიწვია. შედეგად, ისეთმა მცირე ინციდენტმაც კი, როგორიცაა ელექტროგადამცემ ხაზზე ხის დაცემა, სერიოზული ჯაჭვური რეაქცია აღძრა. კერძოდ, აშშ-ს ოჰაიოს შტატში ძაბვის ცვლილება დაიწყო, ხოლო აპარატურამ, რომელიც კასკადური ეფექტის თავიდან ასაცილებლად იყო დაყენებული, მაღალი ძაბვის რაიონის დროული იზოლირება ვერ მოახერხა. შედეგად, აშშ-ს 8 შტატი, კანადის 2 პროვინცია (სულ 50 მილიონი ადამიანი) ელექტროენერგიისა და მასზე დამოკიდებული სერვისების გარეშე დარჩა.

აღნიშნული მაგალითი მეტყველებს, თუ რა შეიძლება მოჰყვეს მცირე დაუდევრობას, უსაფრთხოების საკითხების იგნორირებას, ციფრულ ინფორმაციულ სივრცეში.

დღეს კიბერუსაფრთხოება რისკის ქვეშ დგას ისე, როგორც არასდროს.

საკვანძო სიტყვები: *კიბერუსაფრთხოება, ინფორმაციული უსაფრთხოება, რისკები, არასანქციონირებული გამოყენება, ჰაკერი.*

შესავალი

კიბერუსაფრთხოება თანამედროვე მსოფლიოს ერთ-ერთ მთავარ პრობლემად იქცა. 21-ე საუკუნეში მკვეთრად განვითარდა ინფორმაციის დაგროვების საშუალებები, სწრაფად იმატა დაგროვილი ინფორმაციის მოცულობამ და დახვეწილია მისი ტრანსპორტირების საშუალებები. გლობალურ საინფორმაციო სივრცეში ხშირად ისეთი მონაცემები მოძრაობს, რომელიც მის მფლობელებს კერძო მოხმარებისთვის ჰქონდათ შექმნილი ან სახელმწიფო საიდუმლოს უნდა წარმოადგენდეს, თუმცა ეს მონაცემები ძალიან ხშირად ყველასთვის ღია ხდება. თუნდაც, ცნობილი WikiLeaks.com, რომელზეც მსოფლიოს მრავალი ქვეყნის (პირველ რიგში, ამერიკის შეერთებული შტატების) სამთავრობო და სამხედრო საიდუმლოებების მარტივად გაგება შეიძლება. და მაინც, მომავლის უდიდესი საფრთხე არა ინფორმაციის გამჟღავნებაში, არამედ ლოჯისტიკური, ინფრასტრუქტურული და ენერგეტიკული სისტემების კომპიუტერული საშუალებებით მწყობრიდან გამოყვანაში მდგომარეობს, რომელსაც დედამიწაზე კატასტროფული მოვლენების განვითარება შეუძლია.

ამრიგად, არსებობს დიდი პრობლემა და შესაბამისად, მასთან ბრძოლა აუცილებელია. ინფორმაციული უსაფრთხოების უზრუნველყოფისთვის ბრძოლის მთავარ სივრცეს ციფრული, იგივე კიბერსამყარო წარმოადგენს და ტერმინი „კიბერუსაფრთოებაც“ აქედან მოდის.

ე.წ. ჰაკერები საინფორმაციო ტექნოლოგიებში კარგად გარკვეულ პიროვნებებს წარმოადგენენ, რომლებსაც ინფორმაციის მოპარვა და სხვა მავნე საქმეების კეთება ორგანიზაციაში ფიზიკურად მოხვედრის გარეშეც შეუძლიათ.

ფიშინგი (Phishing) - მომხმარებელს ყალბ ვებგვერდებზე გადაიყვანს და მნიშვნელოვან ინფორმაციას (მაგალითად, საკრედიტო ბარათის ნომერი და CVC-კოდი, სახელი, პაროლი)

გამოსტყუებს. შესაძლებელია, თუ facebook.com-ის ნაცვლად facebok.com არის აკრეფილი (ერთი “o” გამორჩენილი), არ არის გამორიცხული, გარეგნულად „ფეისბუქის“ მსგავს ვებგვერდზე მოხდეს შესვლა და მონაცემების შეყვანა, რომელიც მაშინვე ჰაკერის ხელში მოხვდება.

ძირითადი ნაწილი

1.1.კიბერუსაფრთხოების გამოწვევები

2019 წლის 1 აპრილიდან ძალაში შევიდა საქართველოს ეროვნული ბანკის პრეზიდენტის ბრძანება, კომერციული ბანკების კიბერ უსაფრთხოების მენეჯმენტის ჩარჩოების დამტკიცების შესახებ. ახალი რეგულაციები ავალდებულებს საქართველოში მოქმედ კომერციულ ბანკებს, როგორც ადგილობრივ, ისე უცხოურ კომერციულ ბანკთა ფილიალებს, ჰქონდეთ კიბერუსაფრთხოების მართვის ჩარჩოები, რომელიც უნდა შეესაბამებოდეს კომერციული ბანკების ზომასა და სირთულეს და შეესაბამებოდეს კომერციული ბანკის მომსახურებას. კიბერუსაფრთხოების მენეჯმენტის ჩარჩოები სრულად უნდა იყოს ინტეგრირებული კომერციული ბანკის რისკების მართვის მთლიან პროცესში.

დღეის მდგომარეობით, საქართველოში ბანკები ეფექტურად უმკლავდებიან კიბერუსაფრთხოების გამოწვევებს, მაგრამ ყოველი ახალი რეგულაცია ქმნის ახალ სივრცეებს, რაც მოითხოვს სრულ განაკვეთს, ადამიანურ და მატერიალურ რესურსებს. იუჯითის დახმარებით, კომერციულ ბანკებს საშუალება აქვთ მოკლე დროში მიაღწიონ სრულ შესაბამისობას ინფორმაციის უსაფრთხოების, დოკუმენტაციის დამუშავების, კონტროლის ზოგიერთი მექანიზმის დანერგვის თვალსაზრისით და უზრუნველყონ ორგანიზაციის მომსახურების კიდევ უფრო მაღალი ხელმისაწვდომობა, უწყვეტობა და უსაფრთხოება.

ინფორმაციული უსაფრთხოება და კიბერუსაფრთხოება ის მიმართულებებია, რომლებშიც იუჯითი თქვენი სანდო და გამოცდილი პარტნიორია. მათთან ერთად შეძლებთ მინიმუმამდე დაიყვანოთ უსაფრთხოების რისკები და შეინარჩუნოთ დაცული და საიმედო ტექნოლოგიური გარემო.

ინფორმაციული უსაფრთხოება არის საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას.

ინფორმაციული უსაფრთხოების მართვის სისტემა (იუმს) დაფუძნებულია ბიზნეს რისკებზე, რომლის ფარგლებში მინიმუმამდეა დაყვანილი დანაკარგები და უზრუნველყოფილია ორგანიზაციის მაღალი რეპუტაცია, იუმს ინერგება ISO/IEC 2701 სტანდარტის და „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის შესაბამისად.

UGT გვთავაზობს ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვას, რომელიც მოიცავს შემდეგი კომპონენტების დანერგვას:

- ინფორმაციული უსაფრთხოების მმართველობითი ჩარჩოს შემუშავება;
- რისკების მართვის პროცესის მოწყობა;
- კონტროლის მექანიზმების შემუშავება;

- მუდმივი გაუმჯობესების პროცესის მხარდაჭერა;
- თანამშრომელთა ტრენინგები ცნობიერების ამაღლების მიმართლებით.

1.2. მოქმედების სფერო

კიბერუსაფრთხოების სფეროში რიგით მესამე ეროვნული სტრატეგია მნიშვნელოვანია იმ მხრივაც, რომ მასში გაერთიანდა, როგორც კიბერ და ინფორმაციული უსაფრთხოების გარემოს გაუმჯობესების, ისე კიბერდანაშაულთან ბრძოლისა და კიბერთავდაცვითი შესაძლებლობების გაძლიერებისკენ მიმართული კონკრეტული კომპონენტები. ხშირ შემთხვევაში, საკმაოდ რთულია გამიჯვნა, რადგან საქართველოს კიბერსივრცის უსაფრთხოებისკენ გადადგმული ნაბიჯები, უმრავლეს შემთხვევაში, თანაბრად ემსახურება როგორც კიბერთავდაცვითი გარემოს განვითარებას, ისე კიბერდანაშაულთან ეფექტიან გამკლავებას.

2010 წლიდან დღემდე ქვეყნის მიერ ინსტიტუციური და შესაძლებლობების გაძლიერების, კრიტიკული ინფორმაციული სისტემების დაცულობის, საერთაშორისო ასპარეზზე კონტაქტების დამყარებისა და საერთაშორისო ინიციატივებში ჩართულობის მიმართულებით გადადგმული ნაბიჯები იძლევა საფუძველს, რომ წინამდებარე სტრატეგიის ფარგლებში საქართველომ მიზნად დაისახოს მიღწეული შედეგების განმტკიცება და ახალი საფრთხეებისა და გამოწვევების საპასუხოდ კიბერ და ინფორმაციული უსაფრთხოების გარემოს მდგრადობის უზრუნველყოფა. ეს ყოველივე შესაძლებელია საჯარო და კერძო სექტორის, აკადემიური წრეების აქტიური ძალისხმევითა და კომპლექსური მიდგომების გამოყენებით.

ამდენად, კიბერსივრცეში საფრთხეებსა და ინციდენტებთან დროულად და ეფექტიანად გასამკლავებლად, წინამდებარე სტრატეგია მიზნად ისახავს კიბერუსაფრთხოების, კიბერთავდაცვისა და კიბერდანაშაულის სფეროებში კიბერკულტურისა და კიბერგანათლების განვითარებას, მმართველობითი სისტემის მდგრადობის უზრუნველყოფას, საჯარო-კერძო თანამშრომლობის გაძლიერებას, ძლიერი ადამიანური რესურსების შექმნასა და საერთაშორისო ასპარეზზე საქართველოს, როგორც უსაფრთხო და დაცული ქვეყნის როლის გაძლიერებას.

1.3. არსებული მდგომარეობის მიმოხილვა

კიბერუსაფრთხოების უზრუნველყოფა 21-ე საუკუნის ერთ-ერთი ყველაზე დიდი გამოწვევაა განვითარებული სამყაროსთვის.

ისევე როგორც მთელ მსოფლიოში, საქართველოშიც საკმაოდ გაიზარდა ინტერნეტით დაფარვის მასშტაბები. გაერო-ს საერთაშორისო სატელეკომუნიკაციო გაერთიანების (ITU) ოფიციალური სტატისტიკის თანახმად, საქართველოს მოსახლეობის 70%-ზე მეტს აქვს წვდომა ინტერნეტთან. თუმცა, ქვეყნის სხვადასხვა შიდა გამოკითხვით (e-readiness survey) ეს მაჩვენებელი გაცილებით მაღალ ნიშნულს აღწევს: საქართველოს სტატისტიკის ეროვნული

სამსახურის (საქსტატი) მონაცემებით, კომპანიებთან მიმართებით ის თითქმის 98%-ს შეადგენს.

კიბერუსაფრთხოება საქართველოს მთავრობის უსაფრთხოების პოლიტიკის სტრატეგიული მიმართულებაა და მთავრობის მხრიდან დიდი ყურადღება ეთმობა მის განვითარებაზე ზრუნვას. კერძოდ, საქართველოს მთავრობა მიიჩნევს, რომ სახელმწიფოს პრეროგატივაა, ქვეყანაში შექმნას ინფორმაციული საზოგადოების, ციფრული ეკონომიკისა და ელექტრონული მმართველობის ხელსაყრელი გარემო, ჩამოაყალიბოს ისეთი სტრატეგიული, ინსტიტუციურ-ორგანიზაციული და სამართლებრივ-მარეგულირებელი ჩარჩოები, რაც ხელს შეუწყობს ელექტრონულ სივრცეში მოქალაქეების, კერძო და საჯარო სექტორების უსაფრთხო ფუნქციონირებასა და ონლაინ სივრცის დაცულად გამოყენებას.

საქართველოს მთავრობა აქტიურად ისწრაფვის ღია, უსაფრთხო და დაცული კიბერსივრცის უზრუნველყოფისკენ, რათა კიდევ უფრო მეტად განვითარდეს ინფორმაციული საზოგადოება, შეიქმნას საჯარო და კერძო სექტორში ელექტრონული კომერციის, ინფორმაციულ-საკომუნიკაციო ტექნოლოგიებისა და ტრანზაქციების, ასევე, ელექტრონული მმართველობის მომსახურებისთვის სანდო გარემო.

1.4. ძლიერი მხარეები

კიბერუსაფრთხოება სახელმწიფოს პრიორიტეტი 2008 წლის რუსეთ-საქართველოს ომის შემდგომ გახდა, როდესაც ფართომასშტაბიანი კიბერშეტევების სამიზნედ იქცნენ როგორც სამთავრობო, ისე საბანკო და მედიასექტორები. შესაბამისად, კიბერუსაფრთხოების სფეროში სხვადასხვა აქტორი მოქმედებს, რომელთა მიზანი, სხვა საკითხებთან ერთად, სწორედ ამგვარ საფრთხეებთან გამკლავებაა.

საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი სსიპ – ციფრული მმართველობის სააგენტოს საქმიანობის მიზანია საკუთარი კომპეტენციის შესაბამისად, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების განვითარება და უზრუნველყოფა. სააგენტო, საკუთარი უფლებამოსილების ფარგლებში, ზედამხედველობას უწევს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით გათვალისწინებული ვალდებულებების შესრულებას.

სააგენტო ქმნის სამუშაო ჯგუფებს და წარმართავს მათ საქმიანობას აღნიშნულ სფეროში პოლიტიკის, სტანდარტების და მეთოდოლოგიის შესამუშავებლად. ის კოორდინაციას უწევს საგანმანათლებლო და ცნობიერების ამაღლების კამპანიებს ეროვნულ დონეზე, ასევე, სფეროს სპეციალისტების შესაძლებლობების გაზრდის მიზნით, ერთობლივი კიბერსავარჯიშოებისა და კიბერსწავლების ღონისძიებების ჩატარებას. სააგენტო ქმნის და ადმინისტრირებას უწევს კიბერინციდენტების რეესტრს.

საკუთარი კომპეტენციის შესაბამისად, სააგენტო, საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, აგრეთვე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ, მასთან დაკავშირებულ სხვა საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას

ემსახურება, ახორციელებს მისი კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის (CERT.DGA.GOV.GE) მეშვეობით.

სსიპ –კიბერუსაფრთხოების ბიუროს საქმიანობის სფერო მოიცავს თავდაცვის სამინისტროს სისტემაში არსებული/მოქმედი კრიტიკული ინფორმაციული სისტემის სუბიექტების ინფორმაციული და კიბერუსაფრთხოების პოლიტიკის შემუშავებასა და მისი განხორციელების ხელშეწყობას. თავდაცვის სფეროში კომპიუტერული უსაფრთხოების ინციდენტების, სისუსტეებისა და შესაბამისი მტკიცებულებების დამუშავებას, ანალიზს, რეაგირების მხარდაჭერასა და კოორდინაციას ახორციელებს ბიუროს ერთ-ერთი სტრუქტურული ქვედანაყოფის, კერძოდ კიბერუსაფრთხოების ოპერაციების დეპარტამენტის ფარგლებში მოქმედი, კომპიუტერულ ინციდენტებზე რეაგირების სამმართველო.

2021 წ. 10 ივნისს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში განხორციელებული ცვლილების შედეგად, საკანონმდებლო დონეზე მკაფიოდ განისაზღვრა საქართველოს სახელმწიფო უსაფრთხოების სამსახურის უფლებამოსილებები ქვეყნის კიბერ და ინფორმაციული უსაფრთხოების უზრუნველყოფის პროცესში. შესაბამისი კანონმდებლობის საფუძველზე, კრიტიკული ინფორმაციული სისტემის სუბიექტების კატეგორიზაციის შემდეგ, პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების დაცვაზე პასუხისმგებლობა, საქართველოს სახელმწიფო უსაფრთხოების სამსახურის მმართველობის სფეროში შემავალ საჯარო სამართლის იურიდიულ პირს, საქართველოს ოპერატიულ-ტექნიკურ სააგენტოს დაეკისრება.

საკუთარი კომპეტენციის შესაბამისად, სააგენტო, საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, აგრეთვე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ, მასთან დაკავშირებულ სხვა საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, მისი კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის (CERT.OTA.GOV.GE) მეშვეობით განახორციელებს.

საქართველოს შინაგან საქმეთა სამინისტროში, ცენტრალური კრიმინალური პოლიციის დეპარტამენტში, ორგანიზებულ დანაშაულთან ბრძოლის მთავარი სამმართველოს ფარგლებში, ფუნქციონირებს კიბერდანაშაულთან ბრძოლის სამმართველო. ამასთან, კიბერდანაშაულთან ბრძოლაში, საკუთარი უფლებამოსილების ფარგლებში, ჩართულია საქართველოს პროკურატურა.

სახელმწიფო ინსპექტორის სამსახური ახორციელებს ქვეყანაში პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლს და პასუხისმგებელია მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის შესრულებაზე. სახელმწიფო ინსპექტორის სამსახური კონტროლს უწევს კიბერსივრცეში ფარული საგამოძიებო მოქმედებების განხორციელების პროცესს.

საქართველოს ეროვნული ბანკი უფლებამოსილია, მისი ზედამხედველობის ქვეშ მოქმედ, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკს დაუდგინოს დამატებითი სტანდარტები და მოთხოვნები როგორც ინფორმაციული უსაფრთხოების პოლიტიკის, ისე ინფორმაციული აქტივების მართვისა და შინასამსახურებრივი გამოყენების წესების მიმართ. ეროვნული ბანკი უფლებამოსილია,

კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკს მოსთხოვოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების განსახილველად წარდგენა, აგრეთვე, მიიღოს ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის დასრულების შედეგად მომზადებული სამოქმედო გეგმა და მისი შესრულების გრაფიკი და მათი შეფასების საფუძველზე, გასცეს რეკომენდაციები ან/და შესასრულებლად სავალდებულო მითითებები. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკის მიმართ ადმინისტრაციული სამართალდარღვევის საქმის განხილვისა და ადმინისტრაციული სახდელის დადების უფლებამოსილება ეროვნულ ბანკს გააჩნია.

2019 წ. საქართველოში ეროვნული უსაფრთხოების საბჭო შეიქმნა, რომლის ფუნქციონირებასაც საბჭოს აპარატი უზრუნველყოფს. „ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ“ საქართველოს კანონის შესაბამისად, საბჭო ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვის მაკოორდინირებელ უწყებას წარმოადგენს. ეროვნული უსაფრთხოების საბჭოს აპარატი, საინფორმაციო-ანალიტიკურ საქმიანობასთან ერთად, ეროვნული უსაფრთხოების სფეროში, ეროვნული დონის კონცეპტუალური დოკუმენტების შემუშავების პროცესის ორგანიზებასა და კოორდინაციას უზრუნველყოფს. საბჭოს აპარატი რეგულარულად იღებს და ამუშავებს ინფორმაციას ეროვნული უსაფრთხოების წინააღმდეგ მიმართული კიბერსაფრთხეების შესახებ, რის შედეგადაც, საინფორმაციო-ანალიტიკური დოკუმენტების შემუშავების მეშვეობით, შესაბამისი ადრესატების მხარდაჭერას უზრუნველყოფს.

აღნიშნულთან ერთად, საბჭოს აპარატის ფუნქციების კონტექსტში, მნიშვნელოვანია ეროვნულ დონეზე კრიზისული ვითარების მართვის კომპონენტი. საბჭოს აპარატის ერთ-ერთი სტრუქტურული ერთეული, კერძოდ კი, კრიზისული ვითარების მართვის ეროვნული ცენტრი (დეპარტამენტი), ეროვნული სიტუაციური ოთახის ფუნქციონირებას უზრუნველყოფს. აღნიშნული ინფრასტრუქტურა, ეროვნული ინტერესებისთვის საფრთხის შემცველი კრიზისული ვითარების დროს აქტიურდება და მისი მეშვეობით, საქართველოს პრემიერ-მინისტრის მიერ, შესაბამისი ვითარების პოლიტიკურ / სტრატეგიულ დონეზე მართვა ხორციელდება.

ბოლო ათი წლის განმავლობაში საქართველომ მიიღო და განახორციელა კიბერუსაფრთხოების ორი თანმდევი ეროვნული სტრატეგია შესაბამისი სამოქმედო გეგმებით; ჩამოყალიბდა ინფორმაციული და კიბერუსაფრთხოების სამართლებრივი ბაზა – „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი და მისგან გამომდინარე კანონქვემდებარე აქტები; განისაზღვრა კრიტიკული ინფორმაციული სისტემის სუბიექტები და კიბერუსაფრთხოების უზრუნველყოფაზე პასუხისმგებელი სახელმწიფო ორგანოები; საფუძველი ჩაეყარა ქვეყნის შიგნით საჯარო-კერძო პარტნიორობას კიბერუსაფრთხოების ფორუმის სახით; საქართველომ მონაწილეობის მიღება დაიწყო საერთაშორისო და რეგიონულ დონეზე ორმხრივ და მრავალმხრივ ფორმატებში (EU, NATO, OSCE, UN, EaP, CoE, EUROPOL & INTERPOL, CEPOL, ENISA) კიბერუსაფრთხოების საერთაშორისო პროექტებსა და შეხვედრებში; საქართველოს სამთავრობო უწყებების ორგანიზებით განხორციელდა ცნობიერების ამაღლების ფართომასშტაბიანი კამპანიები, რომელთა მიზანია მოსახლეობაში

კიბერჰიგიენის დანერგვა; ასევე, დღემდე აქტიურად მიმდინარეობს სხვადასხვა სამიზნე ჯგუფის სწავლება-გადამზადება ამ მიმართულებით. საქართველოს მთავრობასა და დიდი ბრიტანეთისა და ჩრდილოეთ ირლანდიის გაერთიანებულ სამეფოს შორის, 2018 წლის ნოემბერში გაფორმდა მემორანდუმი კიბერუსაფრთხოების სფეროში გრძელვადიანი და კომპლექსური თანამშრომლობის თაობაზე. ამას გარდა, საქართველოს ეროვნულ და სამთავრობო კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფს (CERT.GOV.GE) გაფორმებული აქვს ცოდნისა და გამოცდილების გაზიარების შესახებ თანამშრომლობითი მემორანდუმები ევროპულ და აღმოსავლეთ პარტნიორობის არაერთი ქვეყნის შესაბამის უწყებებთან (მაგ.: ლიეტუვა, რუმინეთი, მოლდოვა, უკრაინა). საქართველო აქტიურად მონაწილეობს საერთაშორისო კიბერსავარჯიშოებსა და სწავლებებში და შედეგების თვალსაზრისით, მოწინავე ადგილს იკავებს.

ამასთან, სსიპ – საქართველოს ოპერატიულ-ტექნიკურმა სააგენტომ გააფორმა მემორანდუმი მსოფლიოში აღიარებულ კიბერუსაფრთხოებისა და ციფრული ექსპერტიზის საგანმანათლებლო დაწესებულებასთან – ირლანდიის ეროვნული უნივერსიტეტის კიბერუსაფრთხოებისა და კიბერდანაშაულის გამოძიების ცენტრთან, რომელიც მომავალ წლებში სააგენტოს მისცემს საშუალებას, გადაამზადოს საკუთარი თანამშრომლები ევროკავშირის სამართალდამცავი უწყებების მიერ აღიარებული სპეციალიზებული და ელიტური სასწავლო პროგრამების მიხედვით.

მნიშვნელოვანია, აღინიშნოს, რომ საქართველოს ევროპული და ევროატლანტიკური კურსის ერთ-ერთ მდგრად ქვაკუთხედს საქართველოს NATO-სთან თანამშრომლობა წარმოადგენს. შესაბამისად, საქართველოს თავდაცვის სამინისტროს სსიპ კიბერუსაფრთხოების ბიურო თანამშრომლობის აქტიურ ფაზაშია NATO-ს წევრ სახელმწიფოებთან და მონაწილეობს როგორც ინდივიდუალურად, ისე NATO-ს ეგიდით გამართულ სხვადასხვა სახის პროექტებსა და სტრატეგიულ თუ ტექნიკურ სწავლებებში. გარდა ზემოთქმულისა, ბიურომ თანამშრომლობა გააძლიერა EU CSDP პლატფორმის ფარგლებშიც, რაც ეხმიანება ორგანიზაციის საერთაშორისოდ განსაზღვრულ სტრატეგიულ მიზნებს და ჯამში, საქართველოს თავდაცვის სფეროს კიბერუსაფრთხოების შესაძლებლობების განვითარებით ხელს უწყობს ეროვნული უსაფრთხოების განმტკიცებას. საქართველოს მთავრობა აქტიურად ზრუნავს კიბერუსაფრთხოების სფეროში საჯარო სექტორში დასაქმებულ პროფესიონალთა კვალიფიკაციის ამაღლებაზე. შედეგად, თანამშრომელთა კვალიფიკაციის დონე მაღალია და დასაქმებულთაგან არაერთი ფლობს საერთაშორისოდ აღიარებულ და მაღალი რეპუტაციის მქონე სერტიფიკატებს (SANS, ISACA, ISO).

ეროვნული უსაფრთხოების საბჭოს აპარატს, კიბერუსაფრთხოების სფეროს განვითარებაში საკუთარი წვლილი შეაქვს. საბჭოს აპარატის ორგანიზებითა და საქართველოს მთავრობის მხარდაჭერით, 2020 წლის სექტემბერში, „საქართველოს კიბერუსაფრთხოების ფორუმი“ იქნა ინიცირებული. ფორუმი მაღალი დონის ღონისძიებას წარმოადგენს და ის ყოველწლიურად ჩატარდება. აღნიშნულმა ღონისძიებამ, კიბერსივრცეში ქვეყნის (და შავი ზღვის რეგიონის) წინაშე არსებულ გამოწვევებსა და შესაძლებლობებთან დაკავშირებით, იდეების გაზიარებისთვის პლატფორმის ფუნქცია უნდა შეასრულოს. აქედან გამომდინარე, ის,

ერთი მხრივ, საქართველოს ეროვნული კიბერუსაფრთხოების არქიტექტურის განმტკიცებას ემსახურება, მეორე მხრივ კი, შავი ზღვის რეგიონში ქვეყნის შესაბამის „სექტორულ პოზიციონირებას“ ამყარებს.

ეროვნული უსაფრთხოების საბჭოს აპარატს, კიბერუსაფრთხოების სფეროში სტრატეგიული და ტექნიკური სავარჯიშოების ორგანიზების / კოორდინაციის კუთხით, მნიშვნელოვანი გამოცდილება დაუგროვდა. 2020 წ., ეროვნული უსაფრთხოების საბჭოს აპარატის კოორდინაციით, ევროსაბჭოსა და ევროკავშირის მხარდაჭერით, “CyberEast”-ისა და “CyberSecurity EAST”-ის პროექტების ფარგლებში, არჩევნების (კიბერ) უსაფრთხოების თემატიკაზე ტექნიკური და სტრატეგიული სავარჯიშოები ჩატარდა. საბჭოს აპარატის მიერ, იგეგმება თანამშრომლობის აღნიშნული მიმართულების გაღრმავება და საარჩევნო კონტექსტს მიღმა, შესაბამის სფეროში სავარჯიშოების კომპონენტის გააქტიურება.

ამასთან, ეროვნული უსაფრთხოების საბჭოს აპარატი, ცალკეულ, მნიშვნელოვან საკითხებზე საუკეთესო საერთაშორისო პრაქტიკის ქართული მხარისთვის გაზიარებას უზრუნველყოფს (აღსანიშნავია, მაგ. საბჭოს აპარატისა და NATO-საქართველოს პროფესიული განვითარების პროგრამის (PDP) ერთობლივი პროექტის ფარგლებში, ესტონურ მხარესთან თანამშრომლობით ორგანიზებული დისტანციური სემინარი კიბერუსაფრთხოების სფეროში საჯარო და კერძო სექტორებს შორის თანამშრომლობის (PPP) აქტუალურ საკითხებზე).

საქართველოს მიერ კიბერუსაფრთხოების უზრუნველყოფისკენ ბოლო ათწლეულში გადადგმული ნაბიჯები, განხორციელებული რეფორმები და მიმდინარე პროცესები პოზიტიურად არის შეფასებული საერთაშორისო ასპარეზზე. აღმოსავლეთ პარტნიორობისა და პოსტსაბჭოთა ქვეყნებს შორის კიბერუსაფრთხოების განვითარების თვალსაზრისით, საქართველო მოწინავე პოზიციაზეა. ის ითვლება სამხრეთ კავკასიისა და შავი ზღვის აუზის ქვეყნებს შორის რეგიონის ლიდერ ქვეყნად, წინ უსწრებს აღმოსავლეთ და ცენტრალური ევროპის არაერთ სახელმწიფოს, რისი დასტურიცაა საერთაშორისო სატელეკომუნიკაციო გაერთიანების (ITU) კიბერუსაფრთხოების გლობალური ინდექსის (GCI – Global Cybersecurity Index) მაჩვენებლები. სამართლებრივი, ტექნიკური და ადამიანური რესურსების შესაძლებლობების, თანამშრომლობითი ფორმატებისა და ორგანიზაციული კომპონენტების შეფასებით, 2018 წლის შედეგებით, საქართველო მსოფლიოში – მე-18, ხოლო ევროპაში მე-9 ადგილზე იყო. აღსანიშნავია ისიც, რომ 2017 წელს საქართველო 0.81 ქულით ევროპაში საფრანგეთთან ერთად იყოფდა მე-2, ხოლო მსოფლიოში იკავებდა მე-8 ადგილს. კიბერუსაფრთხოების სფეროში საქართველოს შესაძლებლობები, ასევე, შეფასდა ოქსფორდის უნივერსიტეტის კიბერუსაფრთხოების გლობალური ცენტრის მიერ.

1.5. საფრთხეები

კიბერსაფრთხეების „ტრადიციულ“ ფორმებთან ერთად, შესაბამის სივრცეში საქართველოს მოწყვლადობას, აღნიშნული საფრთხეების თანამედროვე გამოვლინებები განაპირობებს. ახალი კორონავირუსის (COVID-19) პანდემიით გამოწვეულ, დისტანციური მუშაობის უზრუნველყოფის მიზნით ელ. სერვისებზე მზარდ დამოკიდებულებას, შესაბამისი ქსელების / სისტემების უსაფრთხოების კუთხით დამატებითი გამოწვევები მოაქვს.

კიბერსივრცის უსაფრთხოებაზე საკუთარი გავლენა აქვს ხელოვნური ინტელექტის განვითარებას. ამასთან, ყოველდღიურ ცხოვრებაზე, 5-G და ბლოკჩეინ ტექნოლოგიები უშუალო და სულ უფრო მზარდ ზეგავლენას ახდენს. შესაბამისად, კიბერუსაფრთხოების სფეროში, მათთან დაკავშირებული სირთულეების გათვალისწინებაც ხდება საჭირო. აღნიშნული ტექნოლოგიები, ინფორმაციის მიღების, ცოდნის გენერირებისა და მონაცემთა გაცვლის ახალ შესაძლებლობებს ქმნიან, თუმცა, შესაბამისი სისტემების „ახალი ფორმით“ მოწყვლადობასაც განაპირობებენ.

შესაბამის ინფრასტრუქტურაზე/ტექნოლოგიებზე მზარდი დამოკიდებულება, შესაძლებლობებთან ერთად, საფრთხის აქტორების მხრიდან აღნიშნული ინოვაციების ბოროტად გამოყენების რისკებსაც ზრდის. ახალი ტექნოლოგიების განვითარება იწვევს კიბერთავდასხმების მეთოდებისა და საშუალებების დივერსიფიცირებასა და შემდგომ დახვეწას. აღნიშნული სიტუაცია კიბერუსაფრთხოების უზრუნველყოფის კონტექსტში გარკვეული მიდგომების ცვლილებას / ადაპტაციას განაპირობებს და საერთაშორისო თანამეგობრობის მხრიდან სათანადო რეაგირებას მოითხოვს.

მიუხედავად გარკვეული აღმავლობისა, მომდევნო ნაწილში აღწერილ საფრთხეებსა და რისკებთან გამკლავების მიზნით საქართველოს ჯერ კიდევ დიდი ძალისხმევა დასჭირდება კიბერუსაფრთხოების ეროვნულ-სტრატეგიულ დონეზე განვითარების თვალსაზრისით. თუკი წინა წლებში შეიქმნა მყარი საფუძველი კიბერუსაფრთხოებისთვის, დღეს და სამომავლოდ კრიტიკულია ამ ხელშემწყობი ჩარჩოების მდგრადი განვითარება, არსებული პროგრესის შენარჩუნება და მასზე დაშენებით კიბერუსაფრთხოების ეროვნული შესაძლებლობებისა და საქართველოს კიბერუსაფრთხოების პოლიტიკის სტრატეგიული მიმართულებების გაძლიერება.

კომპიუტერულ ინციდენტებზე დახმარების ეროვნული და სამთავრობო ჯგუფის (CERT.GOV.GE) მიერ ინციდენტების აღმოჩენისა და მათზე რეაგირების სხვადასხვა ტექნოლოგიური საშუალების გამოყენებით (ქსელისა და IP მონიტორინგის სისტემა, პორტალები, სენსორები და ა.შ.) მიღებული სტატისტიკა ცხადყოფს, რომ 2014 წლიდან 2019 წლამდე დარეგისტრირებული ინციდენტების რაოდენობა, სულ მცირე, ორჯერ გაიზარდა. ამასთან, იმატა დაინფიცირებული IP მისამართების რიცხვმა და პორტალებთან დაკავშირებულმა უსაფრთხოების მოვლენებმა.

დასკვნა

- არ გასცეთ არანაირი პაროლი, მათ შორის არც ძალიან ახლობელ ადამიანებთან;
- პაროლი უნდა იყოს რაც შეიძლება საიმედო, რთული (სიმბოლოები, რიცხვები, პატარა და დიდი ასოები);
- არ შეხვიდეთ არასაიმედო საჭვო გვერდებზე;
- არ გახსნათ ვითომდა ბანკი თუ გთავაზობთ რაიმეს, თუნდაც მესიჯის სახით, თუ არ დარწმუნდებით, რომ ინფორმაცია ჭეშმარიტია;
- არ გასცეთ პირადი ინფორმაცია;
- ნებისმიერ საიტზე რეგისტრაციის გავლის დროს, კარგად დაუკვირდით მისამართს და არასოდეს არ შეიტანოთ კონფიდენციალური ინფორმაცია;

• რეგისტრაციის დროს, დააფიქსირეთ შეტყობინების მიღება მობილურ მოწყობილობაზე;

• სისტემისა და ანტივირუსის ხშირი განახლება.

გამოყენებული ლიტერატურა

1. დ.გულუა, კიბერუსაფრთხოება, ბიზნესისა და ტექნოლოგიების უნივერსიტეტი, 2020წ.;
2. ა.დანელიანი, კიბერუსაფრთხოების უზრუნველყოფა ეროვნულ და რეგიონულ დონეზე, საქართველოს, სომხეთისა და აზერბაიჯანის მაგალითზე, სამაგისტრო ნაშრომი, 2019წ;
3. საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ. (n.d.). სსიპ "საქართველოს საკანონმდებლო მაცნე". https://matsne.gov.ge/ka/document/view/5263611?publication=0

Information security and cyber security

Gulnara Kotrikadze

Associate Professor, Georgian Technical University, Faculty of Informatics and Management Systems

Abstract

In the era of digital transformation, the dependence on information technology services and products has increased significantly. Accordingly, the challenges in information security and cyber security have increased.

Social distancing, while playing an important role in containing the spread of COVID-19, increases the risk of infected workstations, unauthorized access, data leakage, malicious code execution, and all the types of risks that come with working in a vulnerable environment.

Computer security, cyber security or information security - protection of computer systems and control points of networks from its interference, unauthorized use or damage to hardware, software and electronic data, as well as from destruction and violation of the services they provide to users.

This area is becoming more and more important for computer systems, the Internet and wireless networks such as Bluetooth and Wi-Fi. Because of its complexity, in terms of politics and technology, cyber security is also one of the main challenges in modern life.

Cyber security is one of the most important fields in today's world. This branch is connected with such demanding professions and specialties as: security analyst, security engineer, security architect, security administrator, security specialist, consultant, etc.

Types of Malware -

• Malware (Malware);

• computer virus;

• mobile media means;

• Trojan (Trojan Horse);

• rootkit;

• Backdoor (Backdoor);

• Worm (Computer worm);

• Keylogger (Keylogger).

In 2003, the computer virus Slammer penetrated the management system of the electric distribution network and slowed down its operation, which also caused the speed of management to slow down. As a result, even a small incident like a tree falling on a power line can set off a serious chain reaction. In particular, in the US state of Ohio, the voltage began to change, and the equipment, which was installed to prevent the cascade effect, failed to isolate the high voltage area in time. As a result, 8 US states, 2 Canadian provinces (a total of 50 million people) were left without electricity and services dependent on it.

This example shows what can result from a little carelessness, ignoring security issues, in the digital information space.

Today, cyber security is at risk like never before.

Keywords: *cyber security, information security, risks, unauthorized use, hacking.*