

**ევროკავშირის კიბერ-უსაფრთხოების სტრატეგია ღია,
უსაფრთხო და დაცული კიბერ-სივრცისათვის**

*შოთა ქვაჩაკიძე,
სტუ-ს დოქტორანტი*

რეზიუმე

უკანასკნელი ორი ათწლეულის მანძილზე, ინტერნეტმა და ზოგადად საინფორმაციო სისტემებმა, ფართოდ მოიცვა საზოგადოების ცხოვრების ყველა სფერო. ჩვენი ყოველდღიური ცხოვრება დამოკიდებულია საინფორმაციო და საკომუნიკაციო ტექნოლოგიების მუშაობაზე. ღია და თავისუფალი კიბერ-სივრცე ხელს უწყობს პოლიტიკურ და სოციალურ ჩართულობას მსოფლიოს მასშტაბით. მან შეამცირა ბარიერები ქვეყნებს, საზოგადოებებსა და მოქალაქეებს შორის, რაც საშუალებას იძლევა მოხდეს ინფორმაციისა და იდეების გაზიარება მთელი მსოფლიოსთვის. იმისათვის, რომ კიბერსივრცე დარჩეს ღია და თავისუფალი, მნიშვნელოვანია, რომ იგივე ნორმები, პრინციპები და ღირებულებები, რომლებიც ძალაშია რეალურ სივრცეში, გადატანილი იქნას ონლაინ რეჟიმშიც. ადამიანის ფუნდამენტური უფლებები, დემოკრატიისა და კანონის უზენაესობა დაცული უნდა იყოს კიბერსივრცეში.

ევროკავშირის მიერ შემოთავაზებულ კიბერ-უსაფრთხოების სტრატეგიაში მისი (ევროკავშირის) ხედვა წარმოდგენილია ხუთი სტრატეგიული პრიორიტეტის სახით: კიბერ მდგრადობის მიღწევა; კიბერდანაშაულის მკვეთრად შემცირება; კიბერუსაფრთხოების პოლიტიკის განვითარება, რომელიც დაკავშირებულია საერთო უსაფრთხოებასა და თავდაცვის პოლიტიკასთან; კიბერუსაფრთხოების ინდუსტრიული და ტექნოლოგიური რესურსების შექმნა; თანმიმდევრული საერთაშორისო კიბერპოლიტიკის შემუშავება (ევროკავშირის სივრცისთვის), რომელიც შესაბამისობაში იქნება ევროკავშირის ძირითად ღირებულებებთან. ევროკავშირის მიერ შემოთავაზებული კიბერ სტრატეგია, ასახავს ევროკავშირის ხედვას და საჭირო ქმედებებს, დაფუძნებულს მოქალაქეთა უფლებებზე და ევროკავშირის ონლაინგარემოს უსაფრთხოებაზე.

საკვანძო სიტყვები: ინფორმაციული უსაფრთხოება, კიბერ უსაფრთხოება, ევროკავშირი, ინტერნეტი, კიბერპოლიტიკა.

**Cybersecurity Strategy of the European Union:
An Open, Safe and Secure Cyberspace**

Shota Qvachakidze, Phd of Gtu

Summary

Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society. Our daily life depend on information and communication technology working seamlessly. An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe. For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace.

In the EU cyber-security strategy, the EU vision presented is in five strategic priorities: Achieving cyber resilience, drastically reducing cybercrime, developing cyberdefence policy and capabilities related to the Common Security and Defence Policy, develop the industrial and technological resources for cybersecurity, establish a coherent international cyberspace policy for the European Union and promote core EU values. In Cyber strategy offered by the EU, is vision of EU and the necessary actions, based on citizens' rights and EU cyberspace.

Keywords: Information security, cybersecurity, European Union, internet, cyberspace.

უკანასკნელი ორი ათწლეულის მანძილზე, ინტერნეტმა და ზოგადად საინფორმაციო სისტემებმა, ფართოდ მოიცვა საზოგადოების ცხოვრების ყველა სფერო. ჩვენი ყოველდღიური ცხოვრება, დამოკიდებულია საინფორმაციო და საკომუნიკაციო ტექნოლოგიების მუშაობაზე. ღია და თავისუფალი კიბერ-სივრცე ხელს უწყობს პოლიტიკურ და სოციალურ ჩართულობას მსოფლიოს მასშტაბით; მან შეამცირა ბარიერები ქვეყნებს, საზოგადოებებსა და მოქალაქეებს შორის, რაც საშუალებას იძლევა მოხდეს ინფორმაციისა და იდეების გაზიარება მთელი მსოფლიოსთვის. იმისათვის, რომ კიბერსივრცე დარჩეს ღია და თავისუფალი, მნიშვნელოვანია, რომ იგივე ნორმები, პრინციპები და ღირებულებები, რომლებიც ძალაშია რეალურ სივრცეში, გადატანილი იქნას ონლაინ რეჟიმშიც. ადამიანის ფუნდამენტური უფლებები, დემოკრატიისა და კანონის უზენაესობა დაცული უნდა იყოს კიბერსივრცეში. ჩვენი თავისუფლება

და კეთილდღეობა უფრო და უფრო დამოკიდებულია ინოვაციურ ინტერნეტსივრცეზე, მაგრამ „ონლაინ თავისუფლება“ აგრეთვე მოითხოვს უსაფრთხოებასა და დაცვას. კიბერსივრცე დაცული უნდა იყოს ინციდენტების, მუქარის და უკანონო გამოყენებისაგან. ამ კუთხით, მთავრობას აქვს რამდენიმე ძირითადი ამოცანა: უზრუნველყოფილ იქნას ხელმისაწვდომობა და ღიაობა, დაცული იქნას ადამიანის ფუნდამენტური უფლებები „ონლაინ“ და შენარჩუნებული იყოს საიმედოობა ინტერნეტსივრცეში. თუმცა აღსანიშნავია, რომ კერძო სექტორი ფლობს და ოპერირებს კიბერსივრცის მნიშვნელოვან ნაწილში და ნებისმიერმა ინიციატივამ, რომელიც მიზნად ისახავს ამ სფეროში წარმატებას, მნიშვნელოვანია აღიაროს მისი წამყვანი როლი. საინფორმაციო და საკომუნიკაციო ტექნოლოგიები გახდა ეკონომიკური ზრდის ხერხემალი და წარმოადგენს კრიტიკულ რესურსს, რომელსაც ეყრდნობა ყველა ეკონომიკური სექტორი. ამჟამად ის ეფუძნება კომპლექსურ სისტემას, რომელიც ინარჩუნებს მსოფლიოს ეკონომიკურ განვითარებას ისეთ ძირითად სექტორებში, როგორებიცაა: ფინანსები, ჯანდაცვა, ენერგეტიკა და ტრანსპორტი. [1]

უკანასკნელი წლის ევროპაროგნოზმა აჩვენა, რომ ევროპელების თითქმის მესამედი არ არის დარწმუნებული ინტერნეტბანკით განხორციელებული ოპერაციებისა და ონლაინშესყიდვების უსაფრთხოებაში. აბსოლუტურმა უმრავლესობამ ასევე განაცხადა, რომ ისინი ერიდებიან პირადი ინფორმაციის ინტერნეტში განთავსებას უსაფრთხოების პრობლემების გამო. ევროკავშირის მასშტაბით, ინტერნეტის ყოველი 10 მომხმარებელიდან ერთი უკვე გახდა თაღლითობის მსხვერპლი. უკანასკნელმა წლებმა აჩვენა, რომ ერთის მხრივ ციფრულ სამყაროს მოაქვს უზარმაზარი სარგებელი და ამასთან იგი არის საკმაოდ დაუცველი. ინციდენტები, იქნება ეს განზრახ თუ შემთხვევით, იზრდება საგანგაშო ტემპით და შეიძლება შეაფერხოს მოსახლეობისთვის ისეთი არსებითი მომსახურებების მიწოდება, როგორებიცაა: წყალმომარაგება, ჯანდაცვა, ელექტროენერგიის ან მობილური კომუნიკაციით მომსახურება. საფრთხეებს შეიძლება ჰქონდეთ განსხვავებული წარმოშობა - მათ შორის: სისხლის სამართლის, პოლიტიკურად მოტივირებული. ასევე გასათვალისწინებელია ბუნებრივი კატასტროფები და შემთხვევითი შეცდომები. ევროკავშირის ეკონომიკა უკვე დაზარალდა კერძო სექტორის თუ ფიზიკური პირების წინააღმდეგ მიმართული მოქმედებებისაგან. კიბერ-კრიმინალები იყენებენ სულ უფრო და უფრო დახვეწილ მეთოდებს საინფორმაციო სისტემებში შესაღწევად და მონაცემების მოსაპარად. ეკონომიკური ჯაშუშობის ზრდა კიბერსივრცეში ახალი კატეგორიის საფრთხეებს უქმნის ევროკავშირის წევრი სახელმწიფოების მთავრობებსა და კომპანიებს. ეს ფაქტორი ხსნის, თუ რატომ დაიწყეს მსოფლიოს მასშტაბით მთავრობებმა კიბერუსაფრთხოების სტრატეგიის განვითარება და მიიჩნიეს კიბერსივრცე, როგორც მეტად მნიშვნელო-

ვანი საერთაშორისო საკითხი.

კიბერ უსაფრთხოების პრინციპები:[2]

უსაზღვრო და მრავალფუნქციური ინტერნეტი, დღესდღეობით გახდა ერთ-ერთი ყველაზე ძლიერი ინსტრუმენტი გლობალური პროგრესისათვის. ის ძირითადი კანონები და ნორმები, რომლებიც გამოიყენება რეალური ცხოვრების სხვადასხვა სფეროში, ასევე ვრცელდება კიბერსივრცეშიც. ფუნდამენტური უფლებების დაცვა, გამოხატვის თავისუფლება, პირადი მონაცემების კონფიდენციალურობა კიბერსივრცეში მხოლოდ მაშინ შეიძლება იყოს ეფექტური, როდესაც ის ეფუძნება ევროკავშირის ძირითად ღირებულებებს, ევროკავშირის ქარტიის ფუნდამენტურ უფლებებსა და თავისუფლებებს. ნებისმიერი ინფორმაციის გაცვლა, რომელიც ეხება პირად მონაცემებს, შესაბამისობაში უნდა მოდიოდეს ევროკავშირის შესაბამის კანონთან მონაცემთა დაცვის შესახებ და მოიცავდეს სრულყოფილ ანგარიშს ამ სფეროში ადამიანის უფლებების შესახებ. იმის გათვალისწინებით, თუ რამდენად „ციფრულ“ სამყაროში უწევთ დღევანდელ დღეს მოქალაქეებს ცხოვრება, ციფრულ სერვისებზე ხელმისაწვდომობის შეზღუდვა, წარმოადგენს მნიშვნელოვან პრობლემას მოქალაქეებისთვის. ყველას უნდა ჰქონდეს ინტერნეტთან წვდომა და შეეძლოს ინფორმაციული ნაკადების შეუფერხებლად მიღება. ინტერნეტით სარგებლობა გარანტიას უნდა იძლეოდეს მისით (ინტერნეტით) მოსარგებლე თითოეული მოქალაქის უსაფრთხოებისათვის. ქვეყანაში დემოკრატიული და ეფექტური ხელისუფლების პირობებში, ციფრული სამყარო არ კონტროლდება მხოლოდ ერთი პირის მიერ. დღესდღეობით, არსებობს რამდენიმე დაინტერესებული მხარე, რომელთაგან ბევრია კომერციული და არასამთავრობო ორგანიზაციები. ისინი ჩართულნი არიან ინტერნეტრესურსების მართვის, სტანდარტების შემუშავების და ინტერნეტის სამომავლო განვითარების საქმეში. არსებობს საერთო პასუხისმგებლობა, რათა უზრუნველყოფილ იქნას საინფორმაციო უსაფრთხოება სხვადასხვა სფეროში, რადგან საინფორმაციო და საკომუნიკაციო ტექნოლოგიებზე ადამიანის უფრო და უფრო მზარდი დამოკიდებულების პირობებში, გაზრდილია ხარვეზებიც, რომლებიც უნდა იქნას სათანადოდ განსაზღვრული, ზედმინწევნიტ გაანალიზებული, შემცირებული და გამოსწორებული. ყველა შესაბამისმა პირმა, იქნება ის საჯარო ხელისუფლების წევრი, წარმომადგენელი კერძო სექტორიდან, თუ უბრალოდ მოქალაქე, უნდა გაიაზროს ეს საერთო პასუხისმგებლობა, მიიღოს ზომები, რათა დაიცვას საკუთარი თავი და საჭიროების შემთხვევაში ჩაერთოს კოორდინირებულ მოქმედებებში საერთო კიბერუსაფრთხოების გაძლიერებისათვის. ევროკავშირის ხედვა წარმოდგენილია ხუთი სტრატეგიული პრიორიტეტის სახით:

კიბერ მდგრადობის მიღწევა;

კიბერდანაშაულის მკვეთრად შემცირება;

კიბერუსაფრთხოების პოლიტიკის განვითარება, რომელიც დაკავშირებულია საერთო უსა-

ფრთხილებასა და თავდაცვის პოლიტიკასთან

კიბერუსაფრთხოების ინდუსტრიული და ტექნოლოგიური რესურსების შექმნა;

თანმიმდევრული საერთაშორისო კიბერპოლიტიკის შემუშავება (ევროკავშირის სივრცისთვის), რომელიც შესაბამისობაში იქნება ევროკავშირის ძირითად ღირებულებებთან.

კიბერ მდგრადობის მიღწევა: იმისათვის, რომ ხელი შეუწყოს ევროკავშირის კიბერ მდგრადობას, მნიშვნელოვანია, რომ სახელმწიფო ორგანოებმა და კერძო სექტორმა განავითარონ ერთმანეთთან ეფექტური თანამშრომლობა. დადებით შედეგებზე საქმიანობის დაფუძნება, შესაძლებელს გახდის, რომ სამომავლოდ შემცირებული იქნას კიბერ რისკები და საფრთხეები. ეს გააუმჯობესებს ევროკავშირის შიდა უსაფრთხოებას. აღსანიშნავია, რომ კერძო აქტორებისთვის ჯერ კიდევ არ არსებობს ეფექტური ნახალისების მექანიზმები, რათა მათ უსაფრთხოების სისტემებში მეტი ინვესტირება მოახდინონ. ევროკავშირის მიერ შემოთავაზებული კანონმდებლობა, მიზნად ისახავს ძირითადი სფეროების მოთამაშეებისათვის (კერძოდ, ტრანსპორტი, ენერგეტიკა, საბანკო, საფონდო ბირჟები, ინტერნეტგაყიდვების მომსახურება, ასევე, საჯარო ადმინისტრაციები) მათ წინაშე მდგარი კიბერრისკების შეფასებას და საიმედო და სტაბილური ქსელებისა და საინფორმაციო სისტემების მეშვეობით შესაბამისი რისკების მართვის უზრუნველყოფას. კიბერკულტურის გაძლიერება გააძლიერებს ბიზნესის შესაძლებლობებსა და კონკურენტუნარიანობას კერძო სექტორში.

კიბერდანაშაულის მკვეთრად შემცირება: რაც მეტად „ციფრულ“ სამყაროში ვცხოვრობთ, მით მეტი შესაძლებლობები არსებობს კიბერ კრიმინალებისთვისაც. კიბერდანაშაული დანაშაულის ერთ-ერთი ყველაზე სწრაფად მზარდი ფორმაა და ყოველდღიურად მსოფლიოში მილიონზე მეტი ადამიანი ხდება მისი მსხვერპლი. კიბერდანაშაულის ქსელები ხდება სულ უფრო და უფრო დახვეწილი და ჩვენც შესაბამისი საოპერაციო ინსტრუმენტები და შესაძლებლობები უნდა გავაჩინდეს მათთან გასამკლავებლად. კიბერდანაშაული მაღალმომგებიან და დაბალი რისკის საქმიანობებებს მიეკუთვნება და კიბერდამნაშავეები ხშირად ახერხებენ ანონიმური დომენების გამოყენებას. კიბერდანაშაულმა არ იცის საზღვრები და შესაბამისად მთავრობებმა გლობალურად და ერთმანეთთან თანამშრომლობით უნდა ებრძოლონ მის მზარდ საფრთხეს. ევროკავშირსა და მის წევრ სახელმწიფოებს უნდა გააჩნდეთ ძლიერი და ეფექტური კანონმდებლობა კიბერდანაშაულის დასაძლევად. ევროპის საბჭოს კონვენცია კიბერდანაშაულის შესახებ (აგრეთვე ცნობილი როგორც ბუდაპეშტის კონვენცია) არის სავალდებულო საერთაშორისო ხელშეკრულება, რომელიც უზრუნველყოფს ეროვნული კანონმდებლობის ეფექტურობას. ამჟამად, ევროკავშირის წევრ ყველა სახელმწიფოს არ აქვს ოპერატიული შესაძლებლობები, იმისათვის, რათა ეფექტურად უპასუხოს კიბერდანაშაულს.

ყველა წევრ ქვეყანას სჭირდება კიბერ დანაშაულის წინააღმდეგ ბრძოლის ეფექტური ეროვნული ერთეული.

კიბერუსაფრთხოების პოლიტიკის განვითარება, რომელიც დაკავშირებულია საერთო უსაფრთხოებასა და თავდაცვის პოლიტიკასთან: კიბერუსაფრთხოება აგრეთვე ჩართულია თავდაცვის განზომილებაში. იმისათვის რომ გაიზარდოს წევრი ქვეყნების საკომუნიკაციო და საინფორმაციო სისტემების გამძლეობა, კიბერუსაფრთხოების განვითარება კონცენტრირებული უნდა იყოს კიბერ საფრთხეების გამოვლენაზე და ეფექტურ რეაგირებაზე. იმის გათვალისწინებით, რომ საფრთხეები მრავალმხრივია, სამოქალაქო და სამხედრო საზოგადოებებს შორის აუცილებელია მეტი ეფექტური კომუნიკაცია (სინერგია). ეს ძალისხმევა უნდა იყოს მიმართული კვლევებისა და განვითარებისაკენ, აგრეთვე, ევროკავშირში მთავრობებსა და კერძო სექტორს შორის უფრო მჭიდრო თანამშრომლობისაკენ. გაორების თავიდან აცილების მიზნით, ევროკავშირი შეისწავლის შესაძლებლობებს საიმისოდ, თუ როგორ მიმართონ ევროკავშირმა და „ნატომ“ ერთობლივი ძალისხმევა იმ საინფორმაციო ინფრასტრუქტურების გაუმჯობესებისაკენ, რომლებზედაც დამოკიდებულია ორივე ორგანიზაცია.

კიბერუსაფრთხოების ინდუსტრიული და ტექნოლოგიური რესურსების შექმნა: ევროპას გააჩნია შესანიშნავი შესაძლებლობები კვლევებისა და განვითარებისათვის. მნიშვნელოვანია იმის უზრუნველყოფა, რომ აპარატურული და პროგრამული კომპონენტების წარმოება მოხდეს ევროკავშირის ფარგლებში და ინფრასტრუქტურული მოწყობილობებიც იყოს უფრო საიმედო რათა გარანტირებული იქნას პირადი მონაცემების დაცვა. მაღალი დონის უსაფრთხოება მიიღწევა მხოლოდ იმ შემთხვევაში, თუ მთლიანი ჯაჭვი (მაგალითად: პროგრამული ალგორითმების მწარმოებლები, პროგრამული უზრუნველყოფის დეველოპერები, მომსახურების პროვაიდერები) მიიჩნევს უსაფრთხოებას როგორც პრიორიტეტს. კერძო სექტორი საჭიროებს ნახალისებას, რათა განავითაროს მაღალი დონის კიბერუსაფრთხოება, მაგალითად, სათანადო კიბერუსაფრთხოების მაჩვენებელი ეტიკეტების არსებობა შესაძლებლობას მისცემს კომპანიებს რომ წარმოაჩინონ ეს ფაქტორი და ამით მიიღონ კონკურენტული უპირატესობა. მთავარი აქცენტი მიმართული უნდა იყოს საიმისოდ, რომ წახალისდეს რისკის მენეჯმენტი და შემუშავდეს უსაფრთხოების სტანდარტები და გადანეცხეტილებები. ასევე შესაძლოა შეიქმნას ევროკავშირის მასშტაბით ნებაყოფლობითი სერთიფიცირების სქემები.

თანმიმდევრული საერთაშორისო კიბერპოლიტიკის შემუშავება (ევროკავშირის სივრცისთვის), რომელიც შესაბამისობაში იქნება ევროკავშირის ძირითად ღირებულებებთან: ღია, თავისუფალი და უსაფრთხო კიბერსივრცის შენარჩუნება გლობალური გამოწვევაა, რომელშიც ევროკავშირი უნდა ჩაერთოს შესაბამის საერთაშორისო პარტნიორობთან, ორგანიზაციებთან, კერძო სექტორთან და სამო-

ქალაქო საზოგადოებასთან ერთად. საერთაშორისო კიბერსივრცის პოლიტიკაში ევროკავშირის მიზანია, ხელი შეუწყოს ინტერნეტის ღიაობასა და თავისუფლებას. მიმართოს ძალისხმევა კიბერსივრცეში ქცევის ნორმების განსავითარებლად და არსებული საერთაშორისო კანონების შესასრულებლად. ევროკავშირი აგრეთვე აქტიურად მონაწილეობს საერთაშორისო ძალისხმევაში კიბერუსაფრთხოების მისაღწევად. ინტერნეტის ხელმისაწვდომობის გაზრდის პირობებში მნიშვნელოვანია მსოფლიოში დემოკრატიული რეფორმების განხორციელება და მათი პოპულარიზაცია. გაზრდილ გლობალურ კომუნიკაციებს არ უნდა ახლდეს ცენზურა. ევროკავშირი ხელს უწყობს კორპორატიული სოციალური პასუხისმგებლობის დანერგვას და საერთაშორისო ინიციატივების ნახალისებას რათა გაუმჯობესდეს გლობალური კოორდინაცია ამ სფეროში.

ამრიგად, ევროკავშირის მიერ შემოთავაზებული კიბერ სტრატეგია, ასახავს ევროკავშირის ხედვას და საჭირო ქმედებებს, დაფუძნებულს მოქალაქეთა უფლებებზე და ევროკავშირის ონლაინგარემოს უსაფრთხოებაზე. ეს ხედვა შეიძლება გაანალიზდეს მხოლოდ მრავალი მხარის მჭიდრო თანამშრომლობის შედეგად.

გამოყენებული ლიტერატურა:

- 1) “Joint Communication to the european Parliament, the council, european economic and social committee and the committee of the regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”. Brussels, 7.2.2013.
- 2) Kim Andreasson - “Cybersecurity: Public Sector Threats and Responses”. USA. New York. 2011.