ციფრული ეკოსისტემის საფრთხეები

ქეთევან სიჭინავა
საქართველოს საპატრიარქოს წმიდა ანდრია
პირველწოდებულის სახელობის ქართული
უნივერსიტეტის, ეკონომიკისა
და ბიზნესის მართვის სკოლის დოქტორანტი

რეზიუმე

სტატიაში განხილულია ციფრული ეკოსისტემის მნიშვნელობა და ის საფრთხეები, რომლებიც პირდაპირ და ირიბად მოქმედებენ ადამიანთა კეთილდღეობაზე. კიბერსივრცის უსაფრთხოება მნიშვნელოვან სირთულეებს ქმნის ეროვნულ და საერთაშორისო დონეზე. შესაბამისად, სტატიაში აღნიშნულია ციფრული საფრთხეების შემცირების მიზნით, გლობალური და ლოკალური კიბერსაფრთხეების ტაქტიკური მიდგომები.

საკვანძო სიტყვები: ეკოსისტემა, კიბერსივრცე, ციფრული საფრთხეები, კიბერდანაშაული, ციფრული ემოციური ინტელექტი, კიბერშეტევის მსხვერპლი.

ძირითადი ტექსტი

ეკონომიკა სულ უფრო დამოკიდებული ხდება ტექნოლოგიებზე. ინტერნეტ ტექნოლოგიები აფართოებს, როგორც სოციალურ-ეკონომიკურ სარგებელს, ისე საფრთხეებს, იწვევს სოციალურ ცვლილებებს, ზრდის საზოგადოებრივ გაურკვევლობას, წარმოაჩენს სახელმწიფოს კიბერ საფრთხეებსა და მოწყვლად ადგილებს.(1)

კიბერსივრცედ მხოლოდ ინტერნეტი აღარ განიხილება, რადგან ინტერნეტში ჩართულია საყოფაცხოვრებო ნივთები, ტექნიკა, საგნები, აქსესუარები, ნებისმიერი ფიზიკური სივრცე. აღნიშნული მოცემულობა ნიშნავს იმას, რომ კიბერსაფრთხეები პირდაპირ თუ ირიბ გავლენას ახდენს არამხოლოდ ციფრულ სივრცეში, არამედ ფიზიკურ სივრცეში ადამიანთა კეთილდღე-

ობასა და ცხოვრებაზე. (2)

IBM-ის 2016 წლის კვლევის შედეგებით, გამოკვეთილია კიბერიერიშმიტანილი სფეროები, მათ შორის: **ჯანდაცვის სფერო** (ელექტრონული მედიცინის ბარათები შეიცავს ინფორმაციას მოქალაქის პირად მონაცემის, საკრედიტო ბარათის, ელექტრონული ფოსტის, სოციალური უზრუნველყოფის ნომრისა და სხვა იდენტიფიცირების მონაცემებს.); **მრეწველობა** (მანქანათმშენებლობის, ელექტროტექნიკის, ტექსტილის, პარმაცევტული პროდუქციის წარმოება); **საფინანსო მომსახურება** (ბანკები, მობაილ ბანკი, საკრედიტო ბარატი, საინვესტიციო ფონდები); **სახელმწიფო მართველობა** (საჯარო მომსახურეებზე არსებული ინფორმაციის გაჟონვა, შპიონაჟი); **ტრანსპორტირება** (ავიაკომპანიის, ავტობუსის, მეტროს, რკინიგზის, საზღვაო ტრანსპორტის სფეროში არსებული ინფორმაცია). აღნიშნული დარგი ემსახურება მსოფლიო ვაჭრობას, მის გარეშე მსოფლიო ეკონომიკა ადვილად დაიშლება (3).

არსებითია, რომ პოლიტიკურად მოტივირებული კიბერდანაშაულები მიმართულია მასობროვი ქაოსის, მმართველობითი და პოლიტიკური კრიზისის შექმნის, პოლიტიკური ნდობის შემცირების, სახელმწიფო სისტემის მდგრადობის შესუსტებისკენ. თუმცა გამორიცხავს ფინანსურ სარგებელს.

ინტერნეტის უნივერსალურ სივრცეში, ყველა ქვეყნისათვის ერთნაირია კიბერსაფრთხეების ფორმები, თუმცა განსხვავებულია პრევენციის ღონისძიებები და საფრთხეების მასშტაბები.

Deloitte-ის კვლევის ანგარიშით, ინტერნეტ-გარემოს დინამიური განვითარების პარალელურად მნიშვნელოვანი გამოწვევების წინაშეა სახელმწიფო კიბერდაცვაც. მათ შორის შეიძლება აღინიშნოს: ელექტრონული კომერცია ვითარდება ფიქსირებული ინეტერნეტ და მობილური მოწყობილობების გამოყენებით; საერთო დანაშაულებში, განსაკუთრებული ზრდით ხასიათდება კიბერდანაშაულები; ტერორიზმის მასშტაბები ფართოვდება ტექნოლოგიების საუძველზე, იზრდება ინტერნეტში ჩართული საგნების რაოდენობა, რომელიც ზრდის რო-

გორც კეთილდღეობას, ისე საფრთხეებს; წარმოჩენილია გლობალური ინტერნეტ ბაზრის საინვესტიციო მიმზიდველობით და გლობალური გამოწვევებით (4).

სისტემის უსაფრთხოება ნიშნავს ინფორმაციის და სისტემის დაცვას შემთხვევით ან გამიზნულ არანებადართულ წვდომაზე, არანებადართულ მოდიფიკაციაზე ან ინფორმაციის განადგურებაზე (Layton, 2007). უსაფრთხოება ეხება ინფორმაციის არქიტექტურის დაცვას ქსელის ჩათვლით, მოწყობილობის და პროგრამულ უზრუნველყოფას და თვითონ ინფორმაციის ხელმისაწვდომობას (Basu, 2004). ინფორმაციის უსაფრთხოება, კიბერუსაფრთხობა თუ კომპიუტერული უსაფრთხოება ელექტრონული მთავრობის მნიშვნელოვანი გამოწვევაა. იგი უმნიშვნელოვანესი კომპონენტია მოქალაქესა და სახელმწიფოს შორის ნდობის ზრდისთვის, ეფუძნება დაცვის პოლიტიკასა და სტანდარტებს, აკმაყოფილებს მოქალაქეების მოთხოვნებს, მოიცავს ქსელის უსაფრთხოებასა და დოკუმენტების დაცულობას, მოიცავს ელექტრონული ინფრასტუქტურის დაცვის მხარდაჭერას, უსაფრთხო ტექნოლოგიების გამოყენებას (როგორიცაა: ციფრული ხელმოწერა და ტრანსკრიფცია მომხმარებლის იდენტობის დასაცავად, პაროლი, საკრედიტო ბარათის ნომერი, საბანკო ანგარიშები, და სხვა მსგავსი მონაცემები რომელიც გავრცელებულია ინტერნეტის მეშვეობით და ავტომატურად ინახება), რაც მნიშვნელოვანია ელ-მთავრობის სისტემის მიზნებისთვის (Feng, 2003).

კიბერსივრცის დაცვის საკითხები მნიშვნელოვან სირთულეებს ქმნის ნაციონალური თუ საერთაშორისო დონეზე. შესაბამისად, სახელმწიფოს კიბერთავდაცვის პოლიტიკა საჭიროებს: ტრანსნაციონალურ თანამშრომლობას, იურისდიქციის პრობლემატიკის მოწესრიგებას, ციფრული სივრცის საერთაშორისო სამართლის კონცეფციის თეორიტიზირებას, კიბერთავდასხმის შემთხვევაში კონკრეტული ღონისძიებების გატარებას (5).

ქვეყანაში ციფრული საფრთხეების ეკონომიკური გავლენის შემცირების მიზნით, გლობალური და ლოკალური კიბერსაფრ-

თხეები საჭიროებს ტაქტიკურ მიდგომებს. ასეთი მიდგომებიდან შეიძლება აღვნიშნოთ საერთაშორისო ორგანიზაცია The World Economic Forum-ის მიერ წარმოდგენილი 8 მიმართულება; **ციფრული იდენტიფიცირება**: ციფრული თანამშრომლობა, ციფრული მოქალაქეობრიობა, ციფრული მეწარმეობა; **ციფრული უფლებების დაცვა**: სიტყვის თავისუფლება, ინტელექტუალური საკუთრების დაცვა, პირადი ცხოვრების ხელშეუხებლობა; **ციფრული წიგნიერება:** კომპიუტერული უნარ-ჩვევები და აზროვნება, კონტენტის შექმნა, კრიტიკული აზროვნება; **ციფრული კომუნიკაცია:** ონლაინ თანამშრომლობა, ონლაინ კომუნიკაცია, ციფრული „ნაკვალევი“; **ციფრული უსაფრთხოება:** უსაფრთხოების კოდების დაცვა, ინტერნეტ უსაფრთხოება, მობილური უსაფრთხოება; **ციფრული დაცვა:** კონტენტის რისკი, სამომხმარებლო რისკი; **ციფრული მოხმარება**: კომპიუტერთან მუშაობის დრო, საზოგადოებების ჩართულობა, ციფრული კეთილდღეობა და ჯანმრთელობა; **ციფრული ემოციური ინტელექტი:** სოციალურ და ემოციური ცნობიერების ამაღლება, ემოციების რეგულირება / მართვა, ემპატია(6).

კონფიდენციალურობა და უსაფრთხოება არის კრიტიკული გამოწვევა ელ-მთავრობის იმპლემენტაციის დროს მოქალაქესთან მიმართებაში (OECD, 2003). კონფიდენციალურობა ეხება შესაბამის დაცვის დონეს ინდივიდის ინფორმაციასთან დაკავშირებით(Basu, 2004). სახელმწიფოს აქვს ვალდებულება რომ უზრუნველყოს მოქალაქეების უფლება პირადი ინპორმაციასთან დაკავშირებით, მხოლოდ ლეგიტიმური გამოყენებისთვის გროვდება და იმართება პერსონალური მონაცემები (Sharma & Gupta, 2003). საიტის გატეხვაზე ღელვა, ინფორმაციის გაზიარება, პირადი ინფორმაციის გამომჟღავნება უნივერსალურად ხშირია. ასევე შიშობენ რომ ელ-მთავრობა თვითონაც გამოიყენებს პირად იმფორმაციას მოქალაქეების დაკვირვების მიზნით და შეიჭრან მათ პირადში. Seifert (2003)-ის მიხედვით ელ-მთავრობას უნდა მოეთხოვებოდეს ინდივიდის პირადი სივრცის დაცვა. ტექნიკური და საკანონმდებლო პოლიტიკის გამოყენება შეიძლება გახდეს საჭირო ამ საკითხთან დაკავშირებით.

უფრო მეტიც, საჭიროა პასუხი გაეცეს ეფექტურად პირად საკითხებს იმისათვის რომ მოქალაქის თავდაჯერებულობა გაიზარდოს სახელმწიფო სერვისების გამოყენებისას. მოქალაქის დარწმუნება იმაში რომ სახელმწიფო კეთილსინდისიერად იყენებს მის პირად მონაცემებს და არის ფრთხილი მათი გამოყენებისას არის ძალიან მნიშვნელოვანი ელ-მთავრობის აპლიკაციებისთვის. Basu-მ (2004) აღნიშნა რომ განვითარებად ქვეყნებში ადამიანები იმდენად შეშფოთებულები არიან ამ საკითხით, რომ ისინი უარს ამბობენ ელ-მთავრობის შესაძლებლობებზე. წესდებამ უნდა დააკონკრეტოს რომ მოქალაქეების უფლება პირად ინფორმაციაზე და მანდატი ამ ინფორმაციის გამოყენებაზე იქნება მხოლოდ ლეგიტიმური მიზნებისთვის (Teeter & Hart, 2003).

უსაფრთხოება მნიშვნელოვანია როგორც საჯარო, ასევე კერძო სექტორის საქმიანობისათვის. იგი გამოიყენება ელექტრონული მმართველობის ან ელექტრონული საქმისწარმოების მიზნებისათვის. ასევე, ამ პროცესებთან დაკავშირებული რისკების შესამცირებლად ან თავიდან ასაცილებლად.

კიბერდანაშაული საქართველოში ყოველდღიურად მატულობს, სამინისტროს მიერ დაფიქსირებული კიბერდანაშაულების რიცხვმა 2014 წელთან შედარებით, 2015 წლის იანვარ - აგვისტოს მდგომარეობით 11,11% - ით მოიმატა. რაც შეეხება კიბერდანაშაულის გახსნას, 2014 წელს გახსნის მაჩვენებელმა შეადგინა 59,26%, როცა 2015 წლის იანვარ - აგვისტოს მდგომარეობით ის შეადგენს 34,44%. სტატისტიკური მონაცემებით, საქართველოში 2008 – 2014 წლებში განხორციელებული კიბერშეტევების დიდი რაოდენობა მოდიოდა რუსეთზე (FirEye, 2014), რომლის დროსაც სისტემატურად ხორციელდებოდა კიბერშეტევა შინაგან და საგარეო საქმეთა სამინისტროების, ასევე კავკასიის თემაზე მომუშავე ზოგიერთი არასამთავრობო ორგანიზაციის ვებ - გვერდებზე (7).

2008 წელს საქართველო-რუსეთის ომის დროს, საქართველო გახდა კიბერ შეტევების მსხვერპლი, რომელთა მოსაგერიებლად საქართველო მოუმზადებელი იყო. 2012 წელს აღმოჩ-

ნდა, რომ სამთავრობო უწყებების კომპიუტერებიდან ინფომაციას რამდენიმე წლის განმავლობაში ინფორმაციას იპარავდა Georbot მავნე პროგრამა. 2015 წელს კი ცნობილი გახდა, რომ ისევ სამთავრობო ორგანიზაციების ქსელებიდან ინფორმაციას იპარავდა APT28. სამივე შემთხვევაში შეტევები ირიბად რუსულ კიბერ დანაშაულებრივ ჯგუფებს უკავშირდება(8).

2015 წელს რუსეთის აქტიურობა საქართველოს კიბერ სივრცეში ნაკლებად შეინიშნებოდა, მათი მხრიდან შემოღწევა ოფიციალურად არ დაფიქსირებულა. თუმცა 2016 წლის 21 – 25 მაისს ქართულ საფინანსო ორგანიზაციებზე განხორციელდა მასიური DDoS შეტევა. სულ შეტევაში მონაწილეობდა 300 000-მდე უნიკალური IP მისამართი 160-ზე მეტი ქვეყნიდან. შეტევის მასშტაბიდან, მომზადების ხარისხიდან და რეგიონისადმი გეოპოლიტიკური ინტერესიდან გამომდინარე, უნდა ვივარაუდოთ, რომ აღნიშნული შეტევის უკან რუსეთთან დაკავშირებული ჰაკერული ჯგუფი იდგა. იმის გათვალისწინებით, რომ ასეთ მასშტაბური შეტევა არ იყო ორიენტირებული ფინანსურ ზარალზე, დიდი ალბათობით, იგი მიზნად ისახავდა ყურადღების გადატანას სხვა, შესაძლოა უფრო მეტად ზიანის მომტანი შეტევისაგან. 2015 წელს საქართველოს კიბერსივრცეში არასანქცირებული შეტევებიდან შეიძლება გამოიყოს შემდეგი ინციდენტები(9):

19 იანვარს მოხდა კიბერ თავდასხმა დიასპორის საკითხებში სახელმწიფო მინისტრის აპარატის ვებ-გვერდზე;

2 თებერვალს მოხდა მასობრივი კიბერშეტევა ელექტრონულ ფოსტებზე. კერძოდ, ინტერნეტში გავრცელდა ახალი კომპიუტერული ვირუსი, რომელიც სხვადასხვა ენებზე აგზავნის ელექტრონულ წერილებს, მათ შორის ქართულ ენაზეც. ვირუსი მსხვერპლს 96 საათს აძლევს, რათა გადარიცხოს კონკრეტული თანხა, წინააღმდეგ შემთხვევაში ფაილები სამუდამოდ განადგურდება;

5 თებერვალს განხორციელდა კიბერ შეტევა საქართველოს საგარეო საქმეთა სამინისტროს ოფიციალურ ვებ-გვერდზე;

წლის პირველ ნახევარში განხორციელდა რამდენიმე კიბერ

შეტევა საქართველოს სოფლის მეურნეობის ვებ - გვერდზე.

კვლევები ადასტურებს, რომ გლობალურ და ლოკალურ სივრცეში, კიბერთავდასხმებთან და კიბერტერორიზმთან ბრძოლის აღიარებული მეთოდებია: პროგრამების, პოლიტიკისა და პროცედურების შემუშავება; ბიზნეს უწყვეტობისა და საზოგადოების უსაფრთხოებისათვის, სამივე სექტორის კოორდინირებული კიბერაქტივობა; სამართლებრივი პასუხისმგებლობის გამკაცრება; კადრების მომზადება; ტექნიკური უსაფრთხოების შეფასება და მონიტორინგი (10).

ინფორმაციული ტექნოლოგიების გამოყენებით მართვის სრულყოფისათვის, რომელიც საშუალებას იძლევა ავიცილოთ უამრავი გაუთვალისწინებელი ხარჯები და მივიღოთ მაქსიმალური სარგებელი, აუცილებელია: ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება, დანერგვა და პერიოდულად გაუმჯობესება(11).

ინფორმაციული და კიბერ უსაფრთხოების სფეროში გასათვალისწინებელია საერთაშორისო დონეზე არსებული მთავარ სუბიექტის ევროკავშირის კომისიის პროექტები და სტრატეგიები, სამეცნიერო კვლევითი პროექტები და სამართლებრივ-ნორმატიული ბაზა. მათ შორის შეიძლება აღინიშნოს: ევროკავშირის კომისიის დაკვეთით, ელექტრონული კავშირის ინფრასტრუქტურის შეღწევადობისა და საიმედოობის პრობლემების კვლევების ჩატარება (ARECI); პროექტი „კრიტიკული ინფრასტრუქტურის საფრთხეების შეტყობინების ინფორმაციული ქსელი“ (CIWIN); ქსელური და ინფორმაციული უსაფრთხოების ევროპული სააგენტოს (ENISA) პროექტი ელექტრონული ქსელების უსაფრთხოების მაღალი დონის მიღწევა; ტელემეტრიის ტრანსევროპული სამთავრობოთაშორისო სამსახური (TESTA) (ეს არის სამთავრობო თაშორისო კავშირის ქსელი, რომელიც მოქმედებს მხოლოდ ევროკავშირის ფარგლებში. ის არ არის ჩართული ინტერნეტ - სივრცეში და სხვადასხვა უწყების თანამდებობის პირებს ერთმანეთთან ურთიერთობისას, ინფორმაციის დაზიანებისა და გადინების თავიდან აცილების საშუალებას აძლევს); ინფორმაციული საზოგადოების ტექნოლოგიე-

ბი (პროექტები FP6 და FP7); უსაფრთხოების პრობლემების ევროპული სამეცნიერო - კვლევითი პროგრამა (ESRP); კრიტიკული ინფორმაციული ინფრასტრუქტურის პრობლემების სამეცნიერო - კვლევითი საკოორდინაციო პროექტი (CI2RCO); ინფრასტრუქტურისა და პროექტირების არქიტექტურა; მონაცემთა დაცვის დირექტივა (1995 წელი); ელექტრონული ხელმოწერის დირექტივა (1999 წელი); ელექტრონულ კავშირების სფეროში კონფიდენციალობის დაცვის დირექტივა (2002 წელი); ჩარჩო დირექტივა (2002 წელი); ინფორმაციულ სისტემებზე შეტევის საბჭოს ჩარჩო გადაწყვეტილება (2005 წელი); მონაცემთა შენახვის დირექტივა (2006 წელი)(12).

უსაფრთხოების ზრდის მიზნით საჭიროა ხალხის განათლება, პირადი პაროლების გამოყენება, საზოგადოების მიერ თავდაცვის უზრუნველყოფა. Cohen & Emicke (2002) აღნიშნავს, რომ სანამ უსაფრთხოება იქნება ელ-მთავრობისთვის დაბრკოლება, არ ექნება დიდი გავლენა მის პროგრესზე, რადგან საზოგადოება ისწავლის იმუშაოს და მიიღოს პერიოდულიად შეცდომები. ასევე ახსენეს სამი მნიშვნელოვანი ასპექტი, რომელსაც აქვს გავლენა უსაფრთხოების დაცვაზე. პირველი მოიცავს მუდმივ გამოსწორებას და განახლებას, რათა ეცადოს სისტემა კრიმინალებზე წინ იყოს. მეორე არის ის რომ, უსაფრთხოება იყოს ხილული და შეუღწეველი კრიმინალებისთვის. ბოლოს კი, უნდა შევეგუოთ იმ აზრს, რომ არც ერთი უსაფრთხოების სისტემა არ არის სრულყოფილი და ყველა შეიძლება იყოს დაძლეული. თუმცა, სახელმწიფო ორგანიზაციები, რომლების პასუხისმგებელნი არიან პირადი ინფორმაციის შეგროვებაზე, შენახვაზე და დისტრიბუციაზე, უნდა გაითვალისწინონ მეთოდები პირადი ინფორმაციის უსაფრთხოებისთვის როგორც შეგროვებული ინფორმაციისთვის, ასევე მათი საიტებისთვისაც. შესაბამისად, ჯგუფი უსაფრთხოების პროფესიონალების უნდა იყოს მზად რათა უპასუხოს მყისიერად საფრთხეებს და დაზიანებებს. ასევე ხელისუფლებისთვის და ინფრასტრუქტურის შიფრირებული სისტება ქონა უნდა იყოს უპირველესი პრიორიტეტი (Feng, 2003).

დასკვნა

ამრიგად, ინტერნეტ-ტექნოლოგიების გამოყენება ზრდის როგორც საზოგადოების სოციალურ და ეკონომიკურ სარგებელს, ასევე იმ საფრთხეებსაც, რომელიც უარყოფითად მოქმედებს ადამიანთა კეთილდღეობაზე. ინფორმაციული და კიბერ უსაფრთხოების სფეროში გასათვალისწინებელია საერთაშორისო დონეზე არსებული ევროკავშირის კომისიის პროექტები და სტრატეგიები, სამეცნიერო კვლევითი პროექტები და სამართლებრივ-ნორმატიული ბაზა. უსაფრთხოების ზრდის მიზნით საჭიროა ხალხის განათლების ამაღლება, პირადი პაროლების გამოყენება, საზოგადოების მიერ თავდაცვის უზრუნველყოფა.

გამოყენებული ლიტერატურა

1. აბულაძე რ. ციფრული საფრთხეების ეკონომიკური გავლენა. მეოთხე საერთაშორისო ეკონომიკური კონფერენცია - IEC 2016 ,,ეროვნული ეკონომიკის განვითარების მოდელები: გუშინ, დღეს, ხვალ“ ბიზნეს-ინჟინერინგის ფაკულტეტი, საინჟინრო-ეკონომიკის დეპარტამენტი, ეკონომიკური განვითარების და მისი სამართლებრივი უზრუნველყოფის სამეცნიერო-კვლევითი ცენტრი. ყოველკვარტალური რეფერირებადი და რეცენზირებადი სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“. № 3 . 14-15 ოქტომბერი, 2016. თბილისი, საქართველო. გვ.58-62;

2. https://www.weforum.org/agenda/2015/09/video-how-should-we-govern-cyberspace/?utm_content=buffer6e063&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer;

3. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment-=SEW03133USEN.PDF;

4. Deloitte. Cyber opportunity analysis report 2016 Positioned to lead. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/IE_ERS_CyberAnalysisReport.pdf;

5. აბულაძე რ. ციფრული საფრთხეების ეკონომიკური გავლენა. მეოთხე საერთაშორისო ეკონომიკური კონფერენცია - IEC 2016 ,,ეროვნული ეკონომიკის განვითარების მოდელები: გუშინ, დღეს, ხვალ“ ბიზნეს-ინჟინერინგის ფაკულტეტი, საინჟინრო--ეკონომიკის დეპარტამენტი, ეკონომიკური განვითარების და მისი სამართლებრივი უზრუნველყოფის სამეცნიერო-კვლევითი ცენტრი. ყოველკვარტალური რეფერირებადი და რეცენზირებადი სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“. № 3 . 14-15 ოქტომბერი, 2016. თბილისი, საქართველო. გვ.58-62;

6. https://www.weforum.org/agenda/2016/06/8-digital-skills-we-must-teach-our-children?utm_content=bufferd8a7f&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer;

7. Internet Development Initiative - IDI 1 ახალი გამოწვევა საქართველოს ინტერნეტ სივრცისთვის. http://indein.net/wp-content/uploads/2015/09/New-Challenges-for-Georgian-Cyber-Space.pdf;

8. კავკასუს ონლაინის გაყიდვასათან დაკავშირებული საფრთხეები. 8 იანვარი. 2016. https://www.cyberhouse.ge/%E1%83%99%E1%83%90%E1%83%95%E1%83%99%E1%83%90%E1%83%A1%E1%83%A3%E1%83%A1%E1%83%98%E1%83%A1-%E1%83%92%E1%83%90%E1%83%A7%E1%83%98%E1%83%93%E1%83%95%E1%83%90/N.WNN1DdKGPIU;

9. Internet Development Initiative - IDI 1 ახალი გამოწვევა საქართველოს ინტერნეტ სივრცისთვის. http://indein.net/wp-content/uploads/2015/09/New-Challenges-for-Georgian-Cyber-Space.pdf;

10. http://www.emrisk.com/knowledge-center/newsletters/cyber-terrorism-emerging-threat;

11. სიჭინავა დ., გოგნაძე თ. ინფორმაციული უსაფრთხოება საგანმანათლებლო დაწესებულებებში. მესამე საერთაშორისო ეკონომიკური კონფერენცია _ IEC-2015` ეროვნული ეკონომიკის განვითარების მოდელები: გუშინ, დღეს და ხვალ. ბიზნეს-ინჟინერინგი - ყოველკვარტალური სამეცნიერო ჟურნალი. N4. 2015;

12. სვანიძე ვ. კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები (კრებული) . საერთაშორისო და რეგიონალური დონის ღონისძიებები მიმართული კიბერსივრცის დაცვაზე . დეკემბერი, 2014 წელი. https://gipa.ge/uploads/files/Cyber_Protection.pdf

REFERENCES:

1. Abuladze R. Economic Impact of Digital Threats. Tbilisi, 2016. (in Georgian language)

2. https://www.weforum.org/agenda/2015/09/video-how-should-we-govern-cyberspace/?utm_content=buffer6e063&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer;

3. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF;

4. Deloitte. Cyber opportunity analysis reports , 2016. Positioned to lead. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/IE_ERS_CyberAnalysisReport.pdf;

5. Abuladze R. Economic Impact of Digital Threats. Tbilisi, 2016. (in Georgian language)

6. https://www.weforum.org/agenda/2016/06/8-digital-skills-we-must-teach-our-children?utm_content=bufferd8a7f&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer;

7. Internet Development Initiative - IDI 1. http://indein.net/wp-content/uploads/2015/09/New-Challenges-for-Georgian-Cyber-Space.pdf;

8. Caucasus Online, Sale Threats , 2016. (in Georgian language) https://www.cyberhouse.ge/%E1%83%99%E1%83%90%E1%83%95%E1%83%99%E1%83%90%E1%83%A1%E1%83%A3%E1%83%A1%E1%83%98%E1%83%A1-%E1%83%92%E1%83%90%E1%83%A7%E1%83%98%E1%83%93%E1%83%95%E1%83%90/N.WNN1DdKGPIU;

9. Internet Development Initiative - IDI 1 http://indein.net/wp-

content/uploads/2015/09/New-Challenges-for-Georgian-Cyber-Space.pdf;

10. http://www.emrisk.com/knowledge-center/newsletters/cyber-terrorism-emerging-threat;

11. Sichinava D. , Gognadze T. Information security in educational institutions . IEC-2015`(in Georgian language)

12. Svanidze V. Cyberspace and cyber security challenges. 2014. (in Georgian language) https://gipa.ge/uploads/files/Cyber_Protection.pdf.

THREATS OF DIGITAL ECOSYSTEM

Ketevan Sichinava
PhD Student
St. Andrew the First-Called
Georgian University of the Patriarchate of Georgia

RESUME

The article discusses the significance of the digital ecosystem and the threats that directly and indirectly affect human wellbeing. Cyberspace security raises the significant challenges on national and international level. Therefore, in view of reducing the digital threats, the article highlights the tactical approaches to both, global and local cyber threats.

Key words: Ecosystem, Cyber Space, Digital Threats, Cyber Crime, Digital Emotional Intellect, Cyber attack victims.