Scientific and Practical Cyber Security Journal (SPCSJ) 1(1):52-59
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

2017 CYBER SECURITY CHALLENGES AND GEORGIA

V. Svanadze
Scientific Cyber Security Association

ABSTRACT

The article contains an overview of the report by an American authoritative organization FireEye that reflects challenges of Cybersecurity for 2017 in the European, Middle East and African regions. What is the situation in Cybersecurity for 2017? What types of activities should we expect on the national level? Which areas can become a cyberattack target and what harmful programs can be used? What investments will be implemented for 2017? On these and other questions experts answer that "it is generally difficult to foresee the future, but the cyber security industry has a clear idea that certain types of attacks will continue with the same pace." According to the report of FireEye, at the next year it is expected to increase the cyberattacks in the world's least developed regions, including the European, Middle East and Africa (EMEA). Particularly, politically motivated cybercritical operations that are increasingly attributable to global and regional conflicts.

KEYWORDS: challenges, cyber security

სტატიაში მოცემული არის ამერიკული ავტორიტეტული ორგანიზაცია FireEye - ს სპეციალისტთა ჯგუფის მიერ მომზადებული რეპორტის მიმოხილვა, რომელიც ასახავს ევროპის, ახლო აღმოსავლეთისა და აფრიკის რეგიონებში 2017 წელს კიბერუსაფრთხოების დარგში არსებულ გამოწვევებს. როგორი იქნება კიბერუსაფრთხოების მიმართულებით ვითარება ახალ 2017 წელს? ეროვნულ დონეზე რა ტიპის აქტივობებს უნდა ველოდოთ? რომელი სფეროები შეიძლება გახდეს კიბერთავდასხმის სამიზნე და რა მავნე პროგრამები შეიძლება იყოს გამოყენებული? რა ინვესტიციები განხორციელდება 2017 წელს? ამ და სხვა კითხვებზე ექსპერტები პასუხობენ, რომ „მომავლის განჭვრეტა ზოგადად რთულია, მაგრამ კიბერუსაფრთხოების ინდუსტრიაში ნათელი წარმოდგენა აქვთ, რომ ზოგიერთი განსაზღვრული თავდასხმების ტიპები გაგრძელდება იმავე ტემპებით.“ FireEye - ს მოცემული რეპორტის მიხედვით, მომავალ წელს მოსალოდნელია კიბერთავდასხმების გაზრდა მსოფლიოს ნაკლებად განვითარებულ რეგიონებზე, მათშორის ევროპის, ახლო

აღმოსავლეთისა და აფრიკის რეგიონებში (EMEA). კერძოდ, ძალზედ გაიზრდება პოლიტიკურად მოტივირებული კიბერნეტიკული ოპერაციები, რომლებიც როგორც წესი თან ახლავს გლობალურ და რეგიონალურ კონფლიქტებს.

როგორი იქნება კიბერუსაფრთხოების მიმართულებით ვითარება ახალ 2017 წელს? ეროვნულ დონეზე რა ტიპის აქტივობებს უნდა ველოდოთ? რომელი სფეროები შეიძლება გახდეს კიბერთავდასხმის სამიზნე და რა მავნე პროგრამები შეიძლება იყოს გამოყენებული? რა ინვესტიციები განხორციელდება 2017 წელს? ამ და სხვა კითხვებზე ექსპერტები პასუხობენ, რომ „მომავლის განჭვრეტა ზოგადად რთულია, მაგრამ კიბერუსაფრთხოების ინდუსტრიაში ნათელი წარმოდგენა აქვთ, რომ ზოგიერთი განსაზღვრული თავდასხმების ტიპები გაგრძელდება იმავე ტემპებით.“[1]

ამერიკული ავტორიტეტული ორგანიზაცია FireEye - ს სპეციალისტთა ჯგუფის მიერ მომზადდა რეპორტი ევროპის, ახლო აღმოსავლეთისა და აფრიკის რეგიონებში 2017 წელს კიბერუსაფრთხოების დარგში გამოწვევების შესახებ. რეპორტში ასევე გაკვრით არის საუბარი შეერთებული შტატების კიბერუსაფრთხოების პოლიტიკის მომავალზე ახალი პრეზიდენტის ადმინისტრაციის ლეგიტიმაციის შემდეგ. ამ ბოლო საკითხზე ნაკლებად გვექნება ქვევით საუბარი, მხოლოდ აქვე ავღნიშნავ, რომ ახლადარჩეული პრეზიდენტის დონალდ ტრამპის ინაუგურაციამდე თითქმის ერთი თვით ადრე, ბარაქ ობამამ 2017 წლის თავდაცვის კანონპროექტში ერთ - ერთ პრიორიტეტად შეიტანა საკითხი ეროვნული უსაფრთხოების სააგენტოდან[2] კიბერომის სარდლობის გამოყოფის[3] შესახებ. ფუნქციების მიხედვით, ეროვნული უსაფრთხოების სააგენტო (NSA) პასუხისმგებელი იქნება მთავრობის საიდუმლო დოკუმენტების დაცვაზე, ხოლო კიბერომის სარდლობა (USCYBERCOM) როგორც ქვეყნის კიბერსივრცის დაცვაზე, ასევე მოწინააღმდეგის ქსელის განადგურებაზე იზრუნებს. თუმცა ამ თემაზე ჯერჯერობით უცნობია თავად დონალ ტრამპის პოზიცია. მაგრამ ობამას ადმინისტრაციამ უკვე მიიღო გარკვეული ზომები და ქვეყნიდან გააძევა 35 რუსი დიპლომატი, რომლებიც დაკავშირებულნი იყვნენ საპრეზიდენტო არჩევნების პერიოდში შეერთებული შტატების ქსელზე, კერძოდ დემოკრატიული პარტიის ოფისებზე კიბერთავდასხმებთან[4].

---

[1] ამერიკული ავტორიტეტული ორგანიზაცია FireEye - ს 2016 წლის დეკემბრის რეპორტი - *Kevin Mandia, Grady Summers,* Special Report/Questions and Answers: The 2017 Security Landscape - EMEA, *December, 2016, FireEye;*

[2] National Security Agency (NSA);

[3] The United States Cyber Command (USCYBERCOM);

[4] გერმანიის დაზვერვის (Bundesnachrichtendienst/BND) პრეზიდენტის ბრუნო კალის განცხადებით, 2017 წელს მოსალოდნელია გერმანიაში არჩევნების პერიოდში რუსეთიდან წამოსული კიბერთავდასხმების

ასევე გამოქვეყნდა იმ რუსული ორგანიზაციებისა და პირთა სია, რომლებიც იყვნენ შემსრულებლები.

ეს არის ნიშანდობლივი ფაქტი, რადგან კიბერუსაფრთხოების სფეროში გაჩნდა ახალი პრეცედენტი და შესაბამისად რეაგირების ახალი ტიპი, რაც უკავშირდება დიპლომატიურ დემარშებს. მანამდე, 2015 წელს იყო დაახლოებით მსგავსი სიტუაცია, როცა შეერთებული შტატების ადმინისტრაციამ გაანალიზა რა ჩინეთის მხრიდან წამოსული კიბერშეტევების რაოდენობის მასშტაბურობა, რეაგირების ერთერთ საშუალებად განიხილებოდა დიპლომატიური გზა, მათშორის ჩინეთის ხელისუფლებისთვის საპროტესტო ნოტის გაგზავნა.

FireEye - ს მოცემული რეპორტის მიხედვით, მომავალ წელს მოსალოდნელია კიბერთავდასხმების გაზრდა მსოფლიოს ნაკლებად განვითარებულ რეგიონებზე, მათშორის ევროპის, ახლო აღმოსავლეთისა და აფრიკის რეგიონებში (EMEA). კერძოდ, ძალზედ გაიზრდება პოლიტიკურად მოტივირებული კიბერნეტიკული ოპერაციები, რომლებიც როგორც წესი თან ახლავს გლობალურ და რეგიონალურ კონფლიქტებს. ჩვენ ასევე მომავალ წელს კიბერ დამნაშავეობის აგრესიული და ძალზედ დინამიური განვითარების მოწმენი გავხდებით, რომელსაც ექნება თავისი მოტივირებული ინტერესები და მიზნები ფინანსური სექტორის მიმართ. ეს ნიშნავს, რომ მომავალ 2017 წელს კიბერ თაღლითები/გამომძალველები, ასევე ინფორმაციების, პერსონალური მონაცემებისა და ანგარიშების მოპარვა, ისევ რჩება დიდ პრობლემად და მწვავე გამოწვევად EMEA – ს რეგიონის უმეტესი ორგანიზაციებისთვის და მთავრობებისთვის. გარდა ამისა, მომავალ წელს კიდევ უფრო გაიზრდება საკრედიტო და სადებეტო ბარათებთან, ასევე ATM ტერმინალებთან დაკავშირებული მაქინაციები, უკანონო საბანკო გადარიცხვები და ასე შემდეგ. მსგავსი სახის საფრთხეები განსაკუთრებით ემუქრება ნაკლებად განვითარებულ ქვეყნებს, სადაც ვერ ხორციელდება საბანკო პროგრამების განახლება, მუშაობს მოძველებული ოპერაციული სისტემები, ვიდეო კონტროლი (CCTV[5] კამერები) და ფიზიკური დაცვა ვერ პასუხობს თანამედროვე სტანდარტებს, და ქსელში არსებობს უამრავი მოწყვლადი ადგილები. ეს კი კიბერდამნაშავეებისთვის, რომლებიც მუდმივად იყენებენ მოწინავე ტექნოლოგიებს, წარმოადგენს შესანიშნავ და იოლ სამიზნეს. ყოველივეს აგრეთვე ემატება ის გარემოებაც, რომ EMEA რეგიონი წარმოადგენს ბიზნესმენთათვის მიმზიდველ ადგილს ახალი ბიზნეს წამოწყებებისთვის, განსაკუთრებით ეს ეხება „თავისუფალ ეკონომიკურ ზონებს (თეზ)“, სულ უფრო მზარდი ხდება კონკურენტული გარემო როგორც რეგიონალურ, ისე გლობალურ დონეზე. ამ შემთხვევაში, და კომპანიების ეფექტურობის ზრდაში დიდ როლს თამაშობს ახალი თანამედროვე ტექნოლოგიები, რაც კიდევ უფრო მეტად ზრდის

მკვეთრი ზრდა http://www.ibtimes.co.uk/russian-hackers-may-disrupt-germanys-2017-election-warns-spy-chief-1594221

[5] Closed - circuit television (CCTV)

კიბერთავდასხმის რისკებს. ამიტომ კერძო სექტორის წარმომადგენლებმა, შეიძლება მთავრობებთან ერთადაც, იზრუნონ აგრეთვე თავიანთი ქსელის დაცვაზე, შესაბამისი დაცვითი ტექნოლოგიების შეძენასა და მონტაჟზე. ამის პარალელურად, EMEA რეგიონისთვის კიდევ ერთი დიდი პრობლემა 2017 წელს იქნება შესაბამისი კვალიფიკაციის მქონე კადრების სიმცირე. ამიტომ მათზე ისევე როგორც 2016 წელს, მომავალ წელსაც იქნება დიდი მოთხოვნილება როგორც სამთავრობო, ისე კერძო სექტორში. თუმცა უნდა აღინიშნოს, რომ ამ შემთხვევაში სამთავრობო სექტორს არ შეუძლია შესთავაზოს სპეციალისტებს ისეთი ფინანსური ანაზღაურება და ლგოტები, როგორც ამას აკეთებს კერძო სექტორი. ამიტომ შედარებით მაღალკვალიფიციური კადრები უფრო მუშაობენ კერძო კომპანიებსა და ორგანიზაციებში, რაც წარმოადგენს გარკვეულ სირთულეებს სახელმწიფო სექტორისთვის, რადგან თუ სახელმწიფოს არ შეუძლია მოიძიოს და დაასაქმოს კვალიფიციური პერსონალი, რათა მაქსიმალურად იქნას დაცული ინფორმაციული უსაფრთხოება და კრიტიკული ინფორმაციული სისტემა, მაშინ ის დროთა განმავლობაში დაკარგავს კონტროლს ციფრულ მონაცემებზე. გარდა ამისა, სახელმწიფოს პასუხისმგებლობა და ვალდებულებაა ინციდენტის მოგერიება, გამოძიება და საპასუხო რეაგირება, კიბერდარტყმის ჩათვლით. რაც შესაბამისი სპეციალისტების არ არსებობის შემთხვევაში რთულად განხორციელებადი პროცესია.

FireEye - ს იმავე რეპორტში საუბარია ასევე 2017 წელს კიბერუსაფრთხოების დარგის ინვესტირებაზე, რასაც რეპორტის ავტორები საინტერესო კუთხით უდგებიან და ხსნიან არსებულ პრობლემას. კერძოდ, ბოლო წლების განმავლობაში EMEA რეგიონში როგორც სამთავრობო, ისე კერძო სექტორის ორგანიზაციები საკმაოდ დიდ ფინანსურ საშუალებებს ხარჯავდნენ ახალი ტექნოლოგიების შეძენაში, სადაც შედიოდა პროგრამული უზრუნველყოფა, კომპიუტერული ტექნიკა და სერვერული სისტემები, რომლებიც ერთმანეთთან თავსებადობაში არ მოდიოდა და შესაბამისად ან ცუდად მუშაობდა, ან საერთოდ არ ფუნქციონირებდა, რის გამოც გაწეული ფინანსური ხარჯი არ იძლეოდა შესაბამის შედეგს და ტყუილად იხარჯებოდა მომსახურე პერსონალის ძალისხმევა და შესაძლებლობები. ეს კი იყო არასწორად წარმოებული მენეჯმენტის, საკითხისადმი არაკვალიფიციური და არაპროფესიონალური დამოკიდებულება. არსებობს დიდი ალბათობა, რომ ეს პროცესი 2017 წელსაც გაგრძელდება, რაც თავის მხრივ უკვე რისკის შემცველია.

ამ მიმართულებით FireEye - ს სპეციალისტები აღნიშნავენ, რომ აუცილებელია მოხდეს ორგანიზაციის კიბერთავდასხმებისგან დაცვის ერთმანეთთან ავთენტური სისტემების სწორი შერჩევა პროგრამულ და ტექნიკურ დონეზე, აგრეთვე შესაბამისი კვალიფიკაციის კადრების მოძიება. ამიტომ კომპანიებმა უნდა დაიწყონ ტექნოლოგიების კონსოლიდაციისა და გამარტივების პროცესი, რაც უკვე არის მსხვილ ბანკებში, სადაც ფინანსური საშუალებების პარალელურად, უნდა ხდებოდეს ათასობით

კლიენტის მონაცემებისა და ანგარიშების დაცვა, მათი კონფიდენციალობის უზრუნველყოფა.

მოცემული რეპორტის მიხედვით, რუსეთის აგრესია 2016 წელს კიბერთავდასხმების მიმართულებით ძალიან გაიზარდა, რაც გაგრძელდება ახალ 2017 წელსაც. ამის ნათელი მაგალითია კიბერთავდასხმები შეერთებული შტატების დემოკრატიული პარტიის ოფისებსა და სხვა ორგანიზაციებზე, რომლებიც დაკავშირებულნი იყვნენ საპრეზიდენტო არჩევნებთან. რუსეთს გააჩნია კარგად დაფინანსებული კიბერ შესაძლებლობები და ოპერატიული უსაფრთხოება[6] თავიანთი დანაშაულებრივი კვალის წასაშლელად. გარდა ამისა, სახელმწიფოსა და კერძო ჰაკერულ ჯგუფებს შორის არსებული რთული და ძნელად აღსაქმელი ურთიერთობა, კიდევ უფრო ართულებს შეტევების მიკუთვნებას რუსეთზე და ჰაკერების მოქმედების გაგებასა და გამოვლენას. EMEA რეგიონის გარდა, შეერთებული შტატები, იაპონია, ავსტრალია და სამხრეთ კორეა წარმოადგენენ კიბერ ჯაშუშური თავდასხმების ობიექტებს ჩინეთიდან. ეს პროცესი გაგრძელდება და სავარაუდოდ გაიზრდება 2017 წელსაც. ჩინეთის გარდა, კიბერ ჯაშუშური თავდასხმების გაზრდა არის მოსალოდნელი ასევე ირანიდან, ჩრდილოეთ კორეიდან და რუსეთიდან. ეს ქვეყნები, და ტერორისტული ორგანიზაციები უკვე რამოდენიმე წელია იყენებენ უცხოელი ექსპერტების რჩევებსა და ინსტრუმენტებს, რათა გაზარდონ თავიანთი კიბერ ჯაშუშური ოპერაციების შესაძლებლობები. ეს პროცესი თავის გაგრძელებას ჰპოვებს ასევე 2017 წელსაც. აქვე აღსანიშნავია ის გარემოებაც, რომ ლათინური ამერიკისა და აზიის ქვეყნები გახდა კიბერდამნაშავეთა განვითარების ადგილი.

გარდა ამისა, რეპორტი ამახვილებს ყურადღებას საინტერესო სიახლეზე და გვაფრთხილებს, რომ კიბერ ჯაშუშობის, პერსონალური მონაცემებისა და საფინანსო სექტორებზე შეტევების პარალელურად, ახალ 2017 წელს გაიზრდება ასევე კიბერთავდასხმები რელიგიურ ორგანიზაციებზე როგორც საერთაშორისო და რეგიონალარ დონეზე, ისე ქვეყნების შიგნით. ამ მიმართულებით, მოიაზრება რუსეთი, რომელიც ქვეყნის შიგნით თავის კიბერშესაძლებლობებს გამოიყენებს ისეთ სხვადასხვა რელიგიურ ჯგუფებზე, როგორებიც არის მაგალითად, მორმონები და იეღოვას მოწმეები. ამ მხრივ გამონაკლისი არც ჩინეთი და არც ინდოეთი არ იქნება. 2017 წლის ახალ გამოწვევებს ასევე ემატება მიზნობრივი შეტევები კიბერ ფიზიკურ სისტემებზე - კრიტიკული ინფრასტრუქტურის სისტემები, განსაკუთრებით ელექტრო სისტემები[7], და

[6] აქ საუბარია რუსეთის სპეციალური სამსახურების მხრიდან ჩატარებული საიდუმლო ღონისძიების დამკვეთების, შემსრულებლების, ძალებისა და საშუალებების დაფარვაზე, რაც შეადგენს ჩვეულებრივი ოპერატიული საქმიანობის ნაწილს;

[7] 2015 წლის 23 დეკემბერი უკრაინის ელექტროსისტემებზე განხორციელებული კიბერშეტევა და ერთი წლის შემდეგ, 2016 წლის 30 დეკემბერს შეერთებულ შტატებში მომხდარი კიბერშეტევა იგივე ელექტროსისტემებზე;

სამომხმარებლო, საყოფაცხოვრებო ტექნიკა[8]. მსგავსი შეტევები გახდება საშუალება ზიანი მიაყენოს და გამოიწვიოს შიში, რაც ემსახურება პოლიტიკური იძულებისა და მიზნების მიღწევას, სხვა სიტყვებით რომ ვთქვათ გახადოს მასზე დამოკიდებული და აქციოს ე. წ. „პოლიტიკურ მძევლად“. აქვე დავამატებდი, რომ გაგრძელდება და უფრო გაიზრდება შეტევები ინდუსტრიული კონტროლის სისტემებზე[9].

საყურადღებოა ასევე ის გარემობაც, რომ ახალ 2017 წელს კიბერდამნაშავეები, უსაფრთხოების ტექნოლოგიების სფეროს ახალი მიღწევების გათვალისწინებით, გააგრძელებენ მავნე პროგრამების შექმნას, რომელიც მიმართული იქნება უფრო ეფექტური მოქმედებისკენ და ვირტუალურ სივრცეში უკეთესად შეეძლებათ შენიღბვა. 2016 წელს კიბერდამნაშავეების მიერ გამოყენებული სკრიპტები, მათ მიერ ასევე წარმატებით იქნება გამოყენებული ახალ 2017 წელს.

ბოლოს რეპორტის ავტორები იძლევიან რამოდენიმე მარტივად შესასრულებელ რჩევებს. კერძოდ, მომხმარებლებმა უნდა შეინარჩუნონ სიფხიზლე, მათ ევალებათ შეასრულონ უსაფრთხოების ჰიგიენის ნორმები, უნდა ჰქონდეთ ორ საფეხურიანი აუთენტიფიკაცია ყველა თავის სისტემებსა და ანგარიშებზე, იყენებდნენ პაროლის მართვისა და შეტევის შემთხვევაში მონაცემების ავტომატური კოპირების პროგრამებს. თავის მხრივ ორგანიზაციების ქსელური სისტემები უნდა იყოს მზად შეტევის მოგერიებასა და თავიდან აცილებაზე. აქ დიდ როლს თამაშობს თითოეული თანამშრომლის ცნობიერება კიბერშეტევების შესახებ, და ამ მიზნით, მათთვის მუდმივად სასწავლო კურსებისა და ინსტრუქტაჟის ჩატარება მოსალოდნელი საფრთხეების თაობაზე.

ზემოაღნიშნულის გათვალისწინებით, შეიძლება ითქვას, რომ 2017 წელს არათუ გაგრძელდება კიბესივრცეში უკანონო აქტივობები, არამედ მოხდება მათი ზრდა შემდეგი მიმართულებებით:

1) მოსალოდნელია კიბერთავდასხმების გაზრდა მსოფლიოს ნაკლებად განვითარებულ რეგიონებზე;
2) გლობალური და რეგიონალური კონფლიქტების თანმხლები პოლიტიკურად მოტივირებული კიბერნეტიკული ოპერაციების მკვეთრი ზრდა, მათშორის საარჩევნო პროცესებში ჩარევა;
3) საპასუხო რეაგირებაში დამკვიდრებას დაიწყებს დიპლომატიური დემარშები;
4) კიბერ დამნაშავეობის აგრესიული და ძალზედ დინამიური განვითარების პროცესი, რომელსაც ექნება თავისი მოტივირებული ინტერესები და მიზნები ფინანსური სექტორის მიმართ;

[8] სხვანაირად მას უწოდებენ Internet of Things (IoT);
[9] The Industrial Control Systems (ICS).

5) კიბერ თაღლითების/გამომძალველების მხრიდან ინფორმაციების, პერსონალური მონაცემებისა და ანგარიშების მოპარვა. საკრედიტო და სადებეტო ბარათებთან, ასევე ATM ტერმინალებთან დაკავშირებული მაქინაციებისა და უკანონო საბანკო გადარიცხვების მკვეთრი ზრდა;
6) კვალიფიციური სპეციალისტების ნაკლებობა;
7) კონკურენტული ბიზნეს გარემოს გათვალისწინებით, კერძო სექტორზე კიბერშეტევების მატება;
8) არასწორი ფინანსური ხარჯი, რაც უკავშირდება პროგრამული უზრუნველყოფის, კომპიუტერული ტექნიკისა და სერვერული სისტემების შეძენას, მათ არათავსებად მუშაობასა და არაავთენტურობას;
9) კიბერ ჯაშუშობის ზრდა;
10) კიბერთავდასხმების რაოდენობის გაზრდა რელიგიურ ორგანიზაციებზე;
11) კიბერდამნაშავეების მხრიდან, უსაფრთხოების ტექნოლოგიების სფეროს ახალი მიღწევების გათვალისწინებით, მავნე პროგრამების შექმნის პროცესის გაგრძელება.

მიმოვიხილეთ რა ზემოაღნიშნული, უნდა აღინიშნოს, რომ ყველა ის საფრთხე, რომელიც ასახულია FireEye - ს რეპორტში, გასათვალისწინებელია ასევე საქართველოს კიბერსივრცის რეალიებისთვის. გამომდინარე, რომ საქართველო წარმოადგენს ნაკლებად განვითარებულ ქვეყანას, საჭირო ფინანსური საშუალებების გამო არ ხდება უსაფრთხოების პროგრამული უზრუნველყოფის განახლება და არ არსებობს შესაბამისი კვალიფიციური სპეციალისტები, ასევე რეგიონში იკვეთება მსოფლიოს დიდი ქვეყნებისა და ალიანსების გეოპოლიტიკური ინტერესები, მათშორის ენერგეტიკული, რეგიონში არის სამი კონფლიქტური ადგილი, ქვეყანა და მისი კრიტიკული ინფრასტრუქტურა სრულიად შესაძლებელია გახდეს კიბერდამნაშავეების სამიზნე. აქვე ასევე გასათვალისწინებელია ის გარემოებაც, რომ საქართველო ახლო მომავალში შესაძლოა გახდეს ევროკავშირის და ჩრდილოეთ ალიანსის წევრი ქვეყანა, რომელსაც უკვე დასჭირდება ყველა იმ საერთაშორისო სტანდარტების დაკმაყოფილება, რითაც სარგებლობენ მოცემული გაერთიანებების წევრი ქვეყნები. საქართველოს ეს მისწრაფება და დასავლეთზე ორიენტირებული საგარეო კურსი, კიდევ უფრო ზრდის რისკებს დასავლეთის იდეოლოგიურად მოწინააღმდეგე ქვეყნებისა და ტერორისტული ორგანიზაციების მხრიდან ქვეყანაზე და მის კრიტიკულ ინფრასტრუქტურაზე, ასევე დასავლეთის ქვეყნების დიპლომატიურ მისიებსა და კომპანიებზე, საერთაშორისო ენერგოპროექტებზე განხორციელდეს კიბერშეტევები, რომელსაც ექნება როგორც ჯაშუშური, ისე ტექნიკური ზიანის მომტანი ხასიათი. აქვე ასევე გასათვალისწინებელია იმ მსხვილი კომპანიებისა და პროექტების ინფომაციული და ქსელური უსაფრთხოება,

რომლებზეც დამოკიდებულია არამარტო ქვეყნის ეკონომიკა, არამედ ასევე რეგიონში არსებული ქვეყნებიც[10].

გამოყენებული წყაროები

1) *Kevin Mandia, Grady Summers*, Special Report/Questions and Answers: The 2017 Security Landscape - EMEA, *December, 2016, FireEye*;
2) http://edition.cnn.com/2016/12/29/politics/russia-sanctions-announced-by-white-house/index.html;
3) *Vladimer Svanadze, Andria Gotsiridze*, Cyber Defence: Main Players of Cyberspace. Police, Strategy and new Challenges of Cybersecurity, *January, 2016*;
4) https://cdn.ampproject.org/c/s/www.washingtonpost.com/amphtml/world/national-security/obama-moves-to-split-cyberwarfare-command-from-the-nsa/2016/12/23/a7707fc4-c95b-11e6-8bee-54e800ef2a63_story.html.

[10] მაგალითისთვის, ბათუმისა და ფოთის პორტები, ხოლო მომავალში ანაკლიის პორტიც.