

კიბერ დაზღვევის ბაზარი და მისი განვითარების ტენდენციები Cyber Insurance Market and it's Development Tendencies

ილია კოჟორიძე - საქართველოს ტექნიკური უნივერსიტეტის დოქტორანტი
გიორგი ცაავა - საქართველოს ტექნიკური უნივერსიტეტი პროფესორი

Ilia Kozhoridze – PhD Student of Georgian Technical University

Giorgi Tsaava – PhD in Economics, Professor, Georgian Technical University

აბსტრაქტი. ინფორმაციული რევოლუცია შესაძლებლობებთან ერთად გარკვეულ გამოწვევებთან ასოცირდება, რომელთა შორის ყველაზე მნიშვნელოვანია კიბერ რისკები. სტატიაში საუბარია კიბერ რისკების ეფექტიანი მართვის მექანიზმზე - კიბერ დაზღვევაზე, რომელიც ჯერ კიდევ განვითარების პროცესშია და უამრავ პრობლემას აწყდება. მსოფლიო კიბერ დაზღვევის ბაზარზე არ არსებობს უნიფიცირებული წესები და ის მასშტაბები, რომელთა დაფარვაც უნდა მოხდეს კიბერ დაზღვევის პოლისით, არსებობს ასიმეტრიული ინფორმაციის პრობლემა და ფასწარმოქმნის სირთულეები, რომლებიც აქტუარული ინფორმაციის საკითხებს უკავშირდება. სწორედ ამ პრობლემებზეა საუბარი და გამოკვეთილია მათი შემცირების ღონისძიებები. ამ კონტექსტში მნიშვნელოვანი დახმარების გაწევა შეუძლია ინსტიტუციურ თეორიას, რომელიც კიბერ დაზღვევაში მონაწილე სხვადასხვა მხარის ინტერესებს აფასებს და გამოკვეთს შესაძლო გავლენებს მარეგულირებელი, ნორმატიული და კულტურულ-კოგნიტური ინსტიტუტების თვალსაზრისით. სტატიაში ასევე განხილულია საქართველოს სადაზღვევო ბაზარზე არსებული მდგომარეობა კიბერ დაზღვევის პროდუქტების მიმართულებით.

საკვანძო სიტყვები: კიბერ რისკები, კიბერ დაზღვევა, კიბერ უსაფრთხოება, ინსტიტუტები.

Abstract. The Information Revolution is Associated with Opportunities, but also certain challenges in which the most important are cyber risks. This article discusses the mechanism of effective cyber risk management – cyber

insurance, which is still under development and faces many problems. There are no universal rules and scope of cyber insurance policy in the global cyber insurance market. One of the most important problem is asymmetric information and pricing difficulties related to actuarial issues. Institution theory can help us to reduce uncertainties related to the nature of cyber risk by studying different groups interests in cyber insurance. The article also discusses the current situation in the Georgian insurance market in the field of Cyber insurance products.

Keywords: Cyber Risks, Cyber Insurance, Cyber Security, Institutions.

შესავალი. კიბერ დაზღვევა თანდათან გვევლინება როგორც მნიშვნელოვანი ინსტრუმენტი ორგანიზაციებისთვის, იმ დანაკარგებისგან თავის არიდებისთვის, რომელიც დაკავშირებულია კიბერ თავდასხმებთან. მიმდინარე დაკვირვებებმა გამოავლინა ბევრი გართულება და გამოწვევა კიბერ დაზღვევის ბაზარზე. სხვადასხვა მზღვეველების კიბერ დაზღვევა ხშირად მოიცავს განსხვავებულ კომბინაციებს, ეს კი მყიდველებისთვის ართულებს სხვადასხვა პოლისების ღირებულებების შედარებას. ბევრი ბიზნესი ჯერ ვერ მიხვდა კიბერ დაზღვევის მნიშვნელობას. პრობლემების საწყისი არის სტანდარტიზაციის ნაკლებობა და საერთო ლექსიკონის არარსებობა კიბერ დაზღვევაში. დამატებით პრობლემაა ის, რომ ზოგიერთი მზღვეველი აზღვევს მხოლოდ სპეციფიკურ კიბერ რისკებს. მზღვეველებსა და პოლისის მფლობელებში გაურკვევლობა გამოიწვია სიახალემ და გაურკვევლობის განცდამ. მაგალითები გვიჩვენებს, რომ კიბერ დაზღვევასთან დაკავშირებული წესები, ნორმები და სტანდარტები არ არის კარგად განვითარებული. დამატებით არსებობს ბევრი შემთხვევა როცა არის არეულობა და უთანხმოება იმასთან დაკავშირებით რა შემთხვევები უნდა დაფაროს კიბერ დაზღვევის პოლისმა. ინსტიტუციურ თეორიას შეუძლია მნიშვნელოვანი პუნქტები შემოიტანოს ამ პრობლემის მოგვარებაში. განსაკუთრებით აღნიშნული თეორია გვეხმარება გავიგოთ, ავხსნათ

და ჩამოვყალიბოთ კიბერ დაზღვევის ინდუსტრიაში მონაწილე სხვადასხვა მხარის ინტერესები და ქმედებები.

ძირითადი ტექსტი. სწრაფი გაციფრულება ქვეყნებს სთავაზობს ახალ შესაძლებლობებს ეკონომიკური განვითარებისთვის, მაგრამ ასევე ახლავს ახალი გამოწვევები კიბერდანაშაულის უკონტროლო ზრდის ფორმით. კიბერ დანაშაულების გაზრდილი რაოდენობა ქვეყნდება ყოველწლიურად, რომელთა შორის არის: იდენტობის მოპარვა, ონლაინ თაღლითობა, სახიფათო პროგრამები და მონაცემების მოპარვა. მთავრობები მნიშვნელოვან როლს თამაშობენ კიბერ საფრთხეების წინააღმდეგ იმ კუთხით, რომ საკვანძო ინდუსტრიის წარმომადგენლებს აძლევენ რეკომენდაციებს უსაფრთხოების სტანდარტებზე. მაგალითად, 2018 წელს ევროკავშირში მიღებული გენერალური მონაცემების დაცვის რეგულაცია აწესებს მითითებებს პერსონალური მონაცემების შეგროვებისა და დამუშავებისთვის ევროკავშირის მასშტაბით.

მიუხედავად იმისა, რომ კერძო და საჯარო სექტორი ყოველწლიურად ზრდის ხარჯებს კიბერუსაფრთხოების პროდუქტებზე, კიბერდანაშაულების შემთხვევები მაინც განაგრძობს ზრდას. კიბერ დაზღვევა ჯერ კიდევ განვითარების პროცესშია, იგი სთავაზობს სადაზღვევო ინდუსტრიას ზრდის შესაძლებლობებს. კიბერ დაზღვევის ბაზრები ძირითადად აწყდებიან პრობლემებს კიბერ რისკების თანდაყოლილი ბუნების გამო. კიბერ დაზღვევის ერთ-ერთი სირთულე დაკავშირებულია სადაზღვევო დაფარვის ბუნდოვანებასთან. გლობალური კიბერ დაზღვევის ბაზარი არის ძალიან რთული, რომელიც მოიცავს მსოფლიოს მასშტაბით ასობით მზღვეველის მიერ 600-ზე მეტი ფორმის კიბერ დაზღვევის პოლისს. არ არის უნიფიცირებული ტერმინები, რომლებიც წარმოქმნის გაურკვევლობებს. კიბერ დაზღვევის დროს ასევე მნიშვნელოვან პრობლემას წარმოადგენს მორალური საფრთხის პრობლემა, როდესაც ფირმები სადაზღვევო პოლისის ყიდვის შემთხვევაში

უფრო ნაკლებ ინვესტიციას განახორციელებენ კიბერუსაფრთხოების გაუმჯობესებაში.

ასევე არსებობს გამოწვევები მონაცემებთან და ფასწარმოქმნასთან დაკავშირებით. ტრადიციულ სადაზღვევო პროდუქტებზე ფასწარმოქმნა ხორციელდება აქტუარული ცხრილების საშუალებით, რომლებიც მიღებულია დიდი მოცულობის ისტორიული მონაცემებიდან. მაგრამ კიბერ დაზღვევის შემთხვევაში არ გვაქვს საკმარისი ინფორმაცია კიბერ დანაკარგების შესახებ. ამ შემთხვევებში სადაზღვევო კომპანიებმა კიბერ დაზღვევის პოლისებზე ფასწარმოქმნა, შესაძლებელია განახორციელონ იმის მიხედვით, თუ რა დანაკარგებია მოსალოდნელი დაზღვეულისთვის, რომელიც თავის მხრივ დამოკიდებულია კიბერუსაფრთხოებაში განხორციელებულ ინვესტიციებზე.²¹

კიბერ თავდასხმების რისკების შემცირების ერთ-ერთი ინსტრუმენტია კიბერ დაზღვევა: სადაზღვევო პოლისები, რომლებიც ფარავენ დანაკარგებს კიბერ თავდასხმებისგან და მონაცემების მოპარვისგან. კიბერ დაზღვევის პოლისების ფასწარმოქმნის დროს მნიშვნელოვანი პრობლემაა არასასურველი შერჩევის ფენომენი, რომლის დროსაც ფირმები, რომლებსაც უფრო მაღალი კიბერ საფრთხეების რისკები აქვთ, უფრო მეტად იქნებიან მიდრეკილნი კიბერ დაზღვევის პოლისის შეძენისკენ. სადაზღვევო კომპანიები აღნიშნულ პრობლემას უმკლავდებიან უსაფრთხოების აუდიტების ინფორმაციის მოთხოვნით.²²

²¹ Shaun S. Wang, Integrated framework for information security investment and cyber insurance, Pacific-Basin Finance Journal, Volume 57, 2019

²² Scott J. Shackelford, should your firm invest in cyber risk insurance? Business Horizons, Volume 55, Issue 4, 2012, Pages 349-356

კიბერ დაზღვევის ბაზარი თანდათანობით ვითარდება, გამოკითხვებისა და წლიური ანგარიშების მიხედვით ისინი დადებითად ზემოქმედებენ კიბერ უსაფრთხოებაზე, მაგრამ აწყდებიან გარკვეულ პრობლემებსაც. რისკის შეფასების თანამედროვე მდგომარეობები ძირითადად არის ხარისხობრივი და არ უზრუნველყოფს მონეტარულ ინფორმაციას, რომელიც საჭიროა კიბერ დაზღვევაში ანდერრაიტინგის პროცესისთვის. მეცნიერების კვლევები დიდწილად ფოკუსირებულია იმაზე, რომ წახალისონ ორგანიზაციები გაზარდონ კიბერუსაფრთხოების ინვესტიციები იმ შემთხვევაში, როდესაც კიბერ დაზღვევა ხელმისაწვდომია.²³

კიბერ დაზღვევა შესაძლებელია შეთავაზებული იყოს როგორც ცალკე პროდუქტი ან სხვა პროდუქტებზე დანამატი. მაგალითად ამერიკული საერთაშორისო ჯგუფი ყიდის კიბერ დაზღვევის პოლისებს, როგორც დამატებით სერვისს სახლების დაზღვევის დროს. 2019 წელს 46-მა მზღვეველმა გამოიმუშავა 1.1 მლრდ აშშ დოლარის სადაზღვევო პრემია ცალკე გაყიდული კიბერ დაზღვევის პროდუქტებიდან. გლობალური ბაზრის კვლევის კომპანიამ განახორციელა ბაზრის კვლევა, რომლის მიხედვითაც კიბერ დაზღვევის გლობალურმა ბაზარმა 2018 წელს შეადგინა 4.85 მლრდ აშშ დოლარი, რომელიც ნავარაუდევია, რომ 2026 წლისთვის მიაღწევს 28.6 მლრდ აშშ დოლარს.

კიბერ დაზღვევა განსხვავდება სხვა განვითარებული სადაზღვევო პროდუქტებისგან მარეგულირებელი, ინდუსტრიული და საბაზრო ფაქტორების მიხედვით. დღეს კიბერ დაზღვევის ბაზარი არის უფრო მცირე ზომის, ვიდრე ტრადიციული სადაზღვევო პროდუქტებისა. მსოფლიოს მასშტაბით 2015 წელს 50-ზე ნაკლები

²³ Ganbayar Uuganbayar et al. Optimisation of cyber insurance coverage with selection of cost effective security controls., Computers & Security, Volume 101, 2021

კომპანია სთავაზობდა კიბერ დაზღვევას ევროპაში. 2019 წლისთვის აშშ-ში დაახლოებით 200 მზღვეველი სთავაზობდა მომხმარებელს კიბერ დაზღვევას. კიბერ დაზღვევის ბაზარი ვითარდება თანდათანობით. მაგალითად, იზრდება მენეჯმენტის ცნობიერება კიბერ რისკებთან დაკავშირებით. ნაკლებია გაურკვევლობა თუ რა უნდა დაფაროს კიბერ დაზღვევამ.

ინსტიტუციურ თეორიას შეუძლია მნიშვნელოვანი პუნქტები შემოიტანოს კიბერ დაზღვევის ბაზარზე არსებული პრობლემის მოგვარებაში. განსაკუთრებით აღნიშნული თეორია გვეხმარება გავიგოთ, ავხსნათ და ჩამოვაყალიბოთ კიბერ დაზღვევის ინდუსტრიაში მონაწილე სხვადასხვა მხარის ინტერესები და ქმედებები. ინსტიტუტები არის მაკრო დონის თამაშის წესები, რომელიც მოიცავს ფორმალურ ინსტიტუტებს, როგორიცაა წესები, კანონები, კონსტიტუცია და არაფორმალური ინსტიტუტები, როგორიცაა სოციალური ნორმები, კონვენციები და თვითშემზღუდველი წესები. სკოტი მიუთითებს სამ ინსტიტუციურ სვეტს: მარეგულირებელი, ნორმატიული და კულტურულ-კოგნიტური. განვიხილოთ სკოტის 3 ინსტიტუციური სვეტი კიბერ დაზღვევის მაგალითზე.

კიბერ დაზღვევის კონტექსტში მარეგულირებელი ინსტიტუტები მოიცავს კანონებს და წესებს, რომლებიც გავლენას ახდენენ მათზე. მაგალითად კიბერ დაზღვევის სწრაფი ზრდა ევროპულ ბაზარზე შეიძლება დავუკავშიროთ ევროკავშირის გენერალური მონაცემების დაცვის აქტის თანმხლებ რისკებს. შესაძლებელია მთავრობამ სავალდებულო გახადოს ყველა მზღვეველისთვის, რომ მომხმარებლებს შესთავაზონ კიბერ დაზღვევა. გაზრდილ კონკურენციას ექნება დადებითი გავლენა კიბერ დაზღვევის ხელმისაწვდომობაზე. სამთავრობო პოლიტიკას ასევე შეუძლია გაზარდოს კიბერ დაზღვევის სექტორისთვის საჭირო სამუშაო ძალა, მონაცემები და საკვანძო კომპონენტები.

ნორმატიული ინსტიტუტები დაკავშირებულია მორალურ და სოციალურ კონვენციებთან. ძირითადი პრობლემები ნორმატიული ინსტიტუტების შემთხვევაში ასოცირებულია პროფესიულ და სოციალურ ვალდებულებებთან. ნორმატიული ინსტიტუტები ასევე მოიცავს სავაჭრო თუ პროფესიულ ასოციაციებს, ინდუსტრიულ ჯგუფებსა და არამომგებიან ორგანიზაციებს. მათ შეუძლიათ გამოიყენონ სოციალური სავალდებულო მოთხოვნები რათა წახალისონ გარკვეული ქცევები. კიბერ დაზღვევის ინდუსტრიაში არაფორმალურ წესებს შეუძლიათ შექმნან გარკვეული ვალდებულება კანონის გარეშე. ამასთანავე სავაჭრო და პროფესიული ასოციაციები შეიძლება ჩართული იყვნენ ცნობიერების ამაღლების აქტივობებში თუ ლობისტურ კამპანიებში.

კულტურულ-კოგნიტური ინსტიტუტების თვალსაზრისით კიბერ დაზღვევის კონტექსტში ყველაზე რელევანტური საკითხია ორგანიზაციული გადაწყვეტილებების მიმღებთა წარმოდგენები კიბერ დაზღვევაზე.²⁴

2021 წლის თებერვლის მდგომარეობით საქართველოში რეგისტრირებულია 18 სადაზღვევო კომპანია, რომლებიც ფლობენ ორივე - სიცოცხლის და არასიცოცხლის დაზღვევის ლიცენზიას.²⁵ აქედან 3 კომპანია მომხმარებელს სთავაზობს კიბერ დაზღვევას. აღნიშნული კომპანიებია: ალდაგი, არდი დაზღვევა და უნისონი. სადაზღვევო კომპანიები ალდაგი და არდი ოფიციალურ ვებგვერდზე არ უთითებენ კიბერ დაზღვევის პროდუქტის მახასიათებლებს, ალდაგი კიბერ დაზღვევის პროდუქტს სთავაზობს კორპორატიულ კლიენტებს, ხოლო არდი დაზღვევა ფინანსურ

²⁴ Kshetri, Nir. “The Evolution of Cyber-Insurance Industry and Market: An Institutional Analysis.” Telecommunications Policy, vol. 44, no. 8, 2020

²⁵ <http://insurance.gov.ge/ka/page/insurers>. უკანასკნელად გადამოწმდა 09.03.2021

ორგანიზაციებს. დამატებითი ინფორმაციის მისაღებად უნდა დაუკავშირდნენ მათ. სადაზღვევო კომპანია უნისონს კი ოფიციალურ საიტზე მითითებული აქვს კიბერ დაზღვევის სფეროები, რომლებიც მოიცავს: პერსონალური და კონფიდენციალური ინფორმაციის პასუხისმგებლობას, კიბერ შეტევის შედეგად დამდგარ რეპუტაციულ ზიანს, კიბერ შეტევის შედეგად გამოწვეულ იურიდიულ ხარჯებს და ქსელის მუშაობის უწყვეტობას.²⁶

დასკვნა. ბოლო წლების განმავლობაში მნიშვნელოვნად გაიზარდა კიბერ შეტევებთან დაკავშირებული რისკები და დანაკარგები, რაც ინფორმაციული რევოლუციის ერთ-ერთი თანმდევი პროცესია. იმისათვის, რომ მოხდეს კიბერ საფრთხეების შემცირება, აუცილებელია ჩამოყალიბდეს ეფექტიანი თანაფარდობა კიბერუსაფრთხოების უზრუნველყოფისთვის საჭირო ინვესტიციებსა და კიბერ დაზღვევას შორის. ჯერჯერობით კიბერ დაზღვევის ბაზარი იმყოფება განვითარების ეტაპზე, რომელიც აწყდება უამრავ პრობლემას, ეს კი კიბერ რისკების ბუნებასთანაა დაკავშირებული. ამ მთავარი პრობლემებია საერთო შეთანხმების არარსებობა სადაზღვევო დაფარვის მასშტაბებზე, უნიფიცირებული წესების არარსებობა, მორალური საფრთხის და არარასსურველი შერჩევის პრობლემა და ფასდადების საკითხები, მაშინ როდესაც არ არსებობს შესაფერისი ინფორმაცია კიბერ ზარალების ოდენობის შესახებ. საქართველოში მოქმედი სადაზღვევო კომპანიებიდან მხოლოდ 3 კომპანია სთავაზობს კიბერ დაზღვევის პროდუქტებს, მაგრამ როგორც სადაზღვევო ბაზრის სტატისტიკური მონაცემები გვიჩვენებს, ჯერჯერობით არ არის მოზიდული პრემია დაზღვევის ამ სახეობაში.

²⁶ <https://unison.ge/b2b/insurance/cyber>. უკანასკნელად გადამოწმდა 09.03.2021

გამოყენებული ლიტერატურა:

1. Ganbayar Uuganbayar et al. Optimisation of cyber insurance coverage with selection of cost effective security controls., Computers & Security, Volume 101, 2021;
2. Kshetri, Nir. “The Evolution of Cyber-Insurance Industry and Market: An Institutional Analysis.” Telecommunications Policy, vol. 44, no. 8, 2020;
3. Scott J. Shackelford, should your firm invest in cyber risk insurance? Business Horizons, Volume 55, Issue 4, 2012, Pages 349-356;
4. Shaun S. Wang, Integrated framework for information security investment and cyber insurance, Pacific-Basin Finance Journal, Volume 57, 2019;
5. <https://aldagi.ge/ka/korporatiuli-dazgveva?category=98>. უკანასკნელად გადამოწმდა 09.03.2021;
6. <https://www.gpih.ge/gpih/org/businessclass.php>. უკანასკნელად გადამოწმდა 09.03.2021;
7. <http://insurance.gov.ge/ka/page/insurers>. უკანასკნელად გადამოწმდა 09.03.2021;
8. <https://unison.ge/b2b/insurance/cyber>. უკანასკნელად გადამოწმდა 09.03.2021.