



**ტექნოლოგიური რისკების თანამედროვე
პრობლემები და განვითარების გზები**

DOI:10.36962/ECS105/5-7/2023-89

ჯამბულ ბინაძე

ეკონომიკის აკადემიური დოქტორი,
ასოცირებული პროფესორი,
აკაკი წერეთლის სახელმწიფო უნივერსიტეტი
Jambul.bitsadze@atsu.edu.ge

ნანა ბენიძე

ეკონომიკის აკადემიური დოქტორი,
ასოცირებული პროფესორი,
აკაკი წერეთლის სახელმწიფო უნივერსიტეტი
Nana.benidze1@atsu.edu.ge

რეზიუმე

გადმოცემულია ტექნოლოგიური რისკების როლი საქართველოს ეკონომიკაში და მის განვითარების გზების ძიება. აღნიშნულია ის პრობლემები რომელიც ამ მიმართულებით დგას. დღეს ტექნოლოგიების ეპოქაში, ტექნოლოგიების განვითარების პირდაპირპროპორციულად იზრდება ტექნიკური რისკების ხარისხი, რომელიც მძიმე ტვირთად იქცა მომხმარებლებისათვის.

დღეს თითოეული ჩვენგანი იყენებს პლასტიკურ ბარათებს ან უბრალოდ აქვს ანგარიში რომელიმე სოციალურ ქსელში, ეს ყველაფერი კი ავტომატურად გვაყენებს ტექნოლოგიური რისკის ქვეშ. ამიტომ, ყველაზე ხშირად განხილვადი საკითხი სწორედ ტექნიკური რისკები და მათი მეშვეობით გამოწვეული შესაძლო მძიმე შედეგებია. ასევე საყურადღებოა ელექტრო-

ნული ვაჭრობა და ინტერნეტ ბანკი, როგორც თავდასხმის ობიექტი. ამდენად ვფიქრობთ რომ თემა აქტუალურია.

ნაშრომში საუბარია იმ ცვლილებებზე, რომელიც განხორციელდა ამ რისკების შესარბილებლად. მოცემულია კვლევის შედეგები, რომლის ანალიზი წარმოდგენას იძლევა არსებული ტექნოლოგიური რისკების ხარისხსა და აღმოფხვრის გზებზე.

აღნიშნულია ის პრობლემები, რომელიც ხელს უშლის ტექნოლოგიური რისკების უკეთ განვითარებას ქვეყნის მამულებით:

1. სახელმწიფოს მხრიდან მხარდაჭერის ნაკლოვანება
2. დასაქმებული პერსონალის არაკვალიფიციურობა
3. არასრულფასოვანი კანონმდებლობა კიბერ უსაფრთხოების კუთხით

4. კიბერ რისკების არასრულფასოვანი დაზღვევა
სტატიაში მოცემულია, კვლევის ფარგლებში ჩატარებული გამოკითხვის შედეგები და შესაბამისი სტატისტიკა.

1. სახელმწიფომ მეტი მხარდაჭერა უნდა აღმოუჩინოს ტექნოლოგიური რისკებით დაზარალებულ ადამიანებს...

2. ამ სფეროში დასაქმებული სპეციალისტების გადამზადება უნდა მოხდეს

3. კანონმდებლობა უნდა დაიხვეწოს და შეესაბამებოდეს თანამედროვე სტანდარტებს და გახდეს დაზარალებულზე მორგებული

4. გაუნჯოხდეს კიბერ უსაფრთხოების დაზღვევა
ყოველივე ამის გათვალისწინება ხელს შეუწყობს ტექნოლოგიურ რისკებში არსებულ პრობლემებს ქვეყნის მასშტაბით

სტატიაში მოცემულია ავტორთა მოსაზრებები და რჩევები, რომელიც დანახულია მეცნიერთა თვალთახედვით და მისი პრაქტიკაში განხორციელება დაეხმარება დარგის საქმიანობის ეფექტურად წარმართვაში.

საკვანძო სიტყვები: ტექნოლოგიური რისკები, კიბერ უსაფრთხოება, ეკონომიკა, პლასტიკური ბარათი, სახელმწიფო დაზღვევა.

პირითადი ტექსტი

საქართველოში 2012 წლიდან მოქმედებს კანონი ინფორმაციული უსაფრთხოების შესახებ.¹ კანონში განსაზღვრულია ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები. ყველა ქვეყანა ცდილობს დაიცვას თავიანთი მოსახლეობა კიბერ შეტევებისაგან დამოუკიდებლად, რის გამოც ყველა საჭირო ზომები და ლონისძიებები ხშირ შემთხვევაში არ არის საკმარისი. არსებობს უამრავი სირთულე, როგორც კიბერუსაფრთხოების სირთულეების ჩვენებულ გაგებაში, ისე სახელმწიფო პოლიტიკაში და ტექნიკურ შესაძლებლობებში, რომლებიც საჭიროებს დაუყოვნებლივ გადაჭრას.

2021 წელს საქართველოს პარლამენტმა მიიღო კანონი კიბერ უსაფრთხოების, 2021-2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის შესახებ, რომლის მთავარი ამოცანებია:

- ეროვნულ დონეზე კიბერინციდენტებისა და კიბერუსაფრთხოების დროული გამოვლენის, რეპორტირებისა და მათთან ეფექტიანი გამკლავების სისტემის შექმნა და განვითარება;

- კიბერდანაშაულის წინააღმდეგ ბრძოლის ეფექტიანი სისტემის განვითარება;

- კიბერშესაძლებლობების განვითარება ძლიერი ადამიანური რესურსითა და სათანადო ტექნიკური უზრუნველყოფის საშუალებით;

აქედან გამომდინარე, ტექნოლოგიური რისკებისგან თავდაცვის საკითხში სახელმწიფოს დიდი როლი აკისრია და იგი თავისი საკანონმდებლო მექანიზმებით არეგულირებს მოსახლეობის მონაცემთა დაცვას.

კიბერსივრცეში, ბოლო დროს განვითარებულმა მოვლენებმა გვაჩვენეს, რომ სულ უფრო გააქტიურდა ჰაკერული დაჯგუფებების თავდასხმა სხვადასხვა ორგანიზაციებზე, სახელმწიფო თუ კერძო სექტორის ვებ-გვერდებზე, რაც პირდაპირ საფრთხეს უქმნის როგორც ცალკეულ ორგანიზაციებსა და

¹ <https://matsne.gov.ge/ka/document/view/1679424?publication=5>

მომხმარებლებს, ისე მთლიანად საერთაშორისო, რეგიონალურ თუ ეროვნულ უსაფრთხოებას. ამ მოცემულობას ართულებს ის გარემოება, რომ დანაშაულებრივ ქმედებებში გამოიყენება უახლესი კომპიუტერული და პროგრამული ტექნოლოგიების მიღწევები.

ელექტრონული ვაჭრობა ბოლო პერიოდში პოპულარული გახდა, თუმცა ის უამრავ რისკთანაა დაკავშირებული. პირველი და უმთავრესი რისკი არის მომხმარებელთა პირადი ინფორმაციის შესაძლო გაჟონვა. ონლაინ ვაჭრობის დროს გვინევს სხვადასხვა ვალუტასთან შეხება, რაც ზრდის სავალუტო რისკსაც, ვინაიდან ვალუტის კურსი ცვალებადია. რაც შეეხება, ელექტრონულ სავაჭრო ვებ-გვერდს, აქვს მოუწესრიგებელი ინტერფეისი, რაც იწვევს შეკვეთების დაზიანებას, მიწოდების გადადებას ან სულაც შეკვეთის სხვა პირისთვის გადაცემას. ხშირია რისკი ელექტრონული ვაჭრობისას, ჰაკერებს აქვთ წვდომა პირად მონაცემებზე და ხსნიან თანხების ანგარიშებიდან სხვადასხვა გზით.¹

ინტერნეტ ბანკინგში უამრავი ტექნოლოგიური რისკია. ეს ოპერაციული რისკები შეგვიძლია დავყოთ სამ ნაწილად.

1. არასწორი ტრანზაქციური პროცესი;

2. მონაცემთა ერთობლიობისა და კონფიდენციალურობის დარღვევა;

3. საბანკო სისტემაზე არაავტორიზებული წვდომა².

სარეკლამო კამპანიებმა ახალი პროდუქტის ბაზარზე გატანისას საინფორმაციო და კიბერუსაფრთხოების რისკი შეიძლება გაზარდოს, რამაც, უდიდესი რისკის ქვეშ დააყენოს საბანკო სისტემა.

საჭიროა ყურადღება გამახვილდეს ტექნოლოგიური რისკების დაზღვევაზე, როგორც ამ რისკების მართვის მექანიზმზე. ამისათვის აუცილებელია შიქმნას შესაბამისი სისტემები და სერვისები, რათა ყველა მონაცემი იყოს დაცული და არ შეექმნას საფრთხე ბიზნესსა და მომხმარებლებს.

1 <https://www.sana-commerce.com/blog/solve-ecommerce-business-risks/>

2 https://www.investopedia.com/terms/o/operational_risk.asp

ტექნოლოგიური რისკების დაზღვევის მექანიზმებიდან აღსანიშნავია:

1. მონაცემთა დაშიფრვა და რეზერვების შექმნა;
2. პროგრამული სერვისების განახლება;
3. ძლიერი პაროლების გამოყენება;
4. სისტემების ჩამკეტი სერვისი.

მნიშვნელოვანია, არსებობდეს მონაცემთა რეზერვები, რათა მათი ნაშლის შემთხვევაში შესაძლებელი იყოს მათი დაბრუნება, აგრეთვე, საჭიროა ყველა პროგრამაში შეიქმნას სისტემების ჩამკეტი სერვისი, რათა საფრთხის შემთხვევაში პროგრამამ ავტომატურად დახუროს მონაცემთა ბაზები. ბიზნესისთვის ყველაზე დიდ საფრთხეს წარმოადგენს ფულის გათეთრება, რის რისკსაც სწორედ ტექნიკური გაუმართაობა ქმნის.¹

თანამედროვე ეპოქაში გაზრდილია ტექნოლოგიების მოხმარების მოცულობა და ხანგრძლივობა, ყველა ბიზნეს-კომპანიის პირადი ინფორმაცია ელექტრონულ სისტემებში ინახება. შესაბამისად, ჰაკერები შეძლებენ მათზე წვდომას, ამით მთელ კომპანიას გაანადგურებენ. ამ საფრთხის წინაშე ყველა საეჭრო დაწესებულება დგას.

ტექნოლოგიური რისკები უმეტესად გამოწვეულია შემდეგი მიზეზებით:

1. მაღალკვალიფიციური სპეციალისტების ნაკლებობა;
2. მცირე ბიუჯეტი უსაფრთხოების სისტემებისთვის;
3. უკონტროლო წვდომა სხვადასხვა სერვისებზე;
4. სოციალურ მედიაში ინფორმაციის გაჟონვა.

ტექნიკური რისკების სამართავად აუცილებელია კონკრეტული გეგმის არსებობა. ყველაზე მოსახერხებელი და ეფექტურია Agile სქემა, რომელიც რისკების შემცირებისკენაა მიმართული და მისი საფეხურებია:

1. ბრენსტორმინგი - საბაზისო რისკის ზედამხედველობა;
2. აღმოჩენა - ზომიერი რისკის ზედამხედველობა დოკუმენტირებული მოსაზრებებით;

¹ <https://rmi.com.sg/2021/06/16/key-types-of-business-risk/>

3. გადანყვეტა - რისკის წინასწარი შეფასება საბაზისო რისკების სანინაალმდეგოდ

4. მუდმივი რისკის შეფასება სრული ზედამხედველობით¹.

აქედან გამომდინარე, ტექნოლოგიური რისკების განსაზღვრისათვის გუნდის წევრებს არ სჭირდებათ, იყვნენ ექსპერტები ტექნოლოგიურ სფეროში, მათ სჭირდებათ, გაიაზრონ ტექნოლოგიური ლანდშაფტი იმდენად, რომ შეძლონ მისი მართვა.

ჩატარდა კვლევა და კვლევაში მონაწილეობა მიიღო 130-მა რესპოდენტმა, რომელთაგან 67,5% მდებრობითია, ხოლო 32,5% მამრობითი. ასაკობრივი სტრუქტურის მიხედვით რესპოდენტები ასე განაწილდა: 20-25 წლის-57,5%, 26-35 წლის-7%, 36-40 წლის-6,5%, 41-55 წლის-15%. 56-60 წლის-10%. 60 და ზევით-4%. სოციალური სტატუსის მიხედვით: სტუდენტი-52,5%. მოსამსახურე-25%. საჯარო მოხელე-12,5%. უმუშავერი-7,5%. სხვა-2,5%. რესპოდენტთა 45% აცხადებს რომ ეს სახელმწიფოს მხრიდან მხარდაჭერა ნაკლებია. 37,5%-პერსონალის არაკვალიფიციურობა. 7,5%-საკანონმდებლო ბაზა. 5%-არასრულფასოვანი დაზღვევა. სხვა-5%.

კითხვაზე-თუ რა არის მნიშვნელოვანი ტექნოლოგიური რისკებთან საბრძოლველად, ყველა რესპოდენტი ერთხმად აცხადებს, რომ კიბერდანაშაულის წინააღმდეგ ბრძოლის ეფექტიანი სისტემის შემუშავება. რაც შეეხება პროფესიულ კადრებს -70%, აცხადებს რომ ნაწილობრივ არის დაკომპლექტებული. შესაბამემა თუ არა ტექნოლოგიური დაზღვევა საერთაშორისო სტანდარტებს-65,5% აცხადებს რომ ნაწილობრივ შეესაბამება. 22,3% არ ფლობს ინფორმაციას. 12,2%-სრულად აკმაყოფილებს.

კვლევაში მნიშვნელოვანია რესპოდენტთა ხედვები ტექნოლოგიური რისკების აღმოფხვრასთან დაკავშირებით:

1. სახელმწიფომ მეტი მხარდაჭერა უნდა აღმოუჩინოს ტექნოლოგიური რისკებით დაზარალებულ ადამიანებს.

2. ამ სფეროში დასაქმებული სპეციალისტების გადამზადება

1 <https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cyber-security-and-technology-risk-in-virtual-banking>

უნდა მოხდეს კვალიფიციური სექტორის მიერ;

3. კანონმდებლობა უნდა დაიხვეწოს და შეესაბამებოდეს თანამედროვე სტანდარტებს და გახდეს დაზარალებულზე მორგებული;

4. უნდა მოხდეს, სადაზღვევო კომპანიების მხრიდან, სადაზღვევო პაკეტების გაუმჯობესება.

დასკვნა

უნდა აღინიშნოს, რომ ჩვენ სრულიად ვიზიარებთ კვლევაში მონაწილე რესპოდენტების მოსაზრებებს და ვიძლევიტ გარკვეულ რეკომენდაციებს, რომელთა გათვალისწინება დაეხმარება დარგის სპეციალისტებსა და ხელმძღვანელობას დროულად გადაჭრან ზემოთ ჩამოთვლილი პრობლემები. ეს რეკომენდაციებია:

1. აუცილებელია, სახელმწიფომ მეტი მხარდჭერა აღმოუჩინოს ტექნოლოგიური რისკებით დაზარალებულ ადამიანებს.

2. სასწრაფოდ უნდა გადამზადდნენ ამ სფეროში დასაქმებული პირები. გადამზადება უნდა მოხდეს კვალიფიციური სექტორის მიერ;

3. აუცილებელია კანონმდებლობა დაიხვეწოს, შეესაბამებოდეს თანამედროვე სტანდარტებს და გახდეს დაზარალებულზე მორგებული;

4. სადაზღვევო კომპანიების მხრიდან, უნდა მოხდეს სადაზღვევო პაკეტების გაუმჯობესება.

REFERENCES

1. <https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-and-technology-risk-in-virtual-banking>

2. <https://www.sana-commerce.com/blog/solve-ecommerce-business-risks/>

3. https://www.investopedia.com/terms/o/operational_risk.asp

4. <https://rmi.com.sg/2021/06/16/key-types-of-business-risk/>

5. <https://www2.deloitte.com/us/en/pages/center-for-board-effectiveness/articles/information-technology-risks-financial-services.html?fbclid=IwAR1raMx98DZA9oLIHklFiGycV7ZL3DgkGPzIDfFEK4SL9EfoQ0j5VnJKIYk>

6. https://gipa.ge/uploads/files/Cyber_Protection.pdf

CONTEMPORARY PROBLEMS OF TECHNOLOGICAL RISKS AND THE WAYS OF DEVELOPMENT

Jambul Bitsadze

Academic Doctor of Economics,
Associate Professor at Akaki
Tsereteli State University
Jambul.bitsadze@atsu.edu.ge

Nana Benidze

Academic Doctor of Economics,
Associate Professor at Akaki
Tsereteli State University
Nana.benidze1@atsu.edu.ge

RESUME

The article “Contemporary problems of technological risks and ways of development ” describes the role of technical risks in the economy of Georgia and the search for ways of its development.

The problems that stand in this direction are mentioned. Today, in the era of technologies, the degree of technical risks increases in direct proportion of the development of technologies, which has become a heavy burden for users.

Today, each of us uses plastic cards or simply has an account in some social network, and all this automatically puts us at technological risk. Therefore, the most frequently discussed issue is precisely the technical risks and possible serve consequences caused by them.

Electronic commerce and internet banking are also noteworthy as the object of attack. Thus, we think that the topic is relevant.

The paper discusses the changes that have been made to mitigate these risks. The results of the research are given, the analysis of which gives an idea of the quality of the existing technological risks and ways of elimination.

The problems that prevent the better development of technological risks throughout the country are mentioned:

1. Lack of support from the government.
2. Unqualified staff.
3. Inadequate legislation in terms of cyber security.
4. Inadequate insurance of cyber risks.

The article presents the results of survey conducted within the framework of the study and relevant statistics.

1. The government should find more support for people affected by technological risks.
2. Specialists employed in the field should be retrained.
3. Legislation should be refined and become victim-friendly.
4. Improve cyber security insurance.

Taking all this into account will help' to solve the problems in technological risks throughout the country.

The article contains the opinions and advice of the authors, seen from the point of view of scientists and its implementation in practice will help to effectively conduct the activities of the field.

Keywords: Technological risks. Cyber security. Economy. Plastic cards. Government. Insurance.