

ინფორმაციული უსაფრთხოების გამოწვევები თანამედროვე ეკონომიკაში

თეა ბიძინაშვილი¹

ნინო ვერულავა²

<https://doi.org/10.61446/pa.3.2025.10281>

აბსტრაქტი

თანამედროვე ეკონომიკა სწრაფი ციფრული ტრანსფორმაციის პერიოდში ვითარდება, რაც ახალ შესაძლებლობებთან ერთად ზრდის სხვადასხვა რისკებსაც. ინფორმაციული უსაფრთხოება სულ უფრო აქტუალური საკითხი ხდება, რადგან ეკონომიკური სისტემები მეტად დამოკიდებულები არიან ტექნოლოგიურ ინფრასტრუქტურაზე და ინფორმაციული რესურსების დაცვა უმნიშვნელოვანესი პრიორიტეტია. კიბერშეტევები, მონაცემთა გაჟონვები, ფიშინგი და სხვა კიბერდანაშაულები ქმნიან მნიშვნელოვან საფრთხეებს ბიზნესებისთვის, ფინანსურ ინსტიტუტებსა და სახელმწიფო ორგანიზაციებისთვის.

ინფორმაციული უსაფრთხოების დარღვევა არა მხოლოდ კომპანიის ფინანსურ ზარალს იწვევს, არამედ ზიანს აყენებს მის რეპუტაციას და მომხმარებელთა ნდობას, რაც საბოლოოდ აისახება მთელ ეკონომიკურ სისტემაზე. შედეგად, საკითხი გადადის ტექნიკურ დონეზე და დგება, როგორც სტრატეგიულად და პოლიტიკურად მნიშვნელოვან პრობლემად. ბიზნესები და სახელმწიფო უწყებები აწყდებიან აუცილებლობას, ინტეგრირდნენ მოწინავე ტექნოლოგიებთან, როგორცაა ხელოვნური ინტელექტი, მანქანური სწავლება, ბლოკჩეინი და ავტომატიზაცია, რაც მათ საშუალებას აძლევს ეფექტურად დაუპირისპირდნენ თანამედროვე კიბერშეტევებს.

ნაშრომი მიზნად ისახავს გაანალიზოს თანამედროვე ეკონომიკაში ინფორმაციული უსაფრთხოების გამოწვევები, მათ შორის კიბერშეტევების ეკონომიკური ზიანი, ინოვაციური ტექნოლოგიების გამოყენების შესაძლებლობები და შესაბამისი პოლიტიკების მნიშვნელობა. განსაკუთრებული ყურადღება ეთმობა საქართველოს კონტექსტს, სადაც ციფრული ეკონომიკა სწრაფად ვითარდება, თუმცა გამოწვევებიც თანმხლებია, რაც მოითხოვს სისტემურ მიდგომებს როგორც სახელმწიფო, ისე კერძო სექტორის მხრიდან.

აღსანიშნავია, რომ ინფორმაციული უსაფრთხოება არის განუყოფელი კომპონენტი ქვეყნის ეკონომიკური განვითარებისა და გლობალურ ბაზრებზე კონკურენტუნარიანობის შესანარჩუნებლად. შესაბამისად, მოთხოვნილია ეფექტიანი სამართლებრივი ბაზის ჩამოყალიბება, ეროვნული უსაფრთხოების სტრატეგიების განახლება და აქტიური თანამშრომლობა საერთაშორისო პარტნიორებთან.

ამ გზით, სტატია ემსახურება არა მხოლოდ გამოწვევების იდენტიფიკაციას, არამედ წინადადებებს, რომლებიც უზრუნველყოფს მდგრადი და უსაფრთხო ეკონომიკური გარემოს შექმნას ციფრულ ეპოქაში.

საკვანძო სიტყვები: ინფორმაციული უსაფრთხოება, კიბერშეტევები, ციფრული ეკონომიკა, ხელოვნური ინტელექტი, ბლოკჩეინი, ეკონომიკური, ზიანისაქართველოს ეკონომიკა, კიბერდაცვა, ციფრული ტრანსფორმაცია, სახელმწიფო პოლიტიკა.

¹საქართველოს ტექნიკური უნივერსიტეტის ასოცირებული პროფესორი, სსიპ დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემიის სამეცნიერო-კვლევითი ცენტრის რედაქტორი, ბიზნესის ადმინისტრირების აკადემიური დოქტორი

²საქართველოს ტექნიკური უნივერსიტეტის ასისტენტ პროფესორი, ინფორმატიკის ინჟინერიის აკადემიური დოქტორი

Information Security Challenges in the Modern Economy

Tea Bidzinashvili³

Nino Verulava⁴

Abstract

The modern economy is evolving rapidly amid digital transformation, bringing new opportunities along with increasing risks. Information security has become an increasingly critical issue, as economic systems heavily depend on technological infrastructure, making the protection of information resources a top priority. Cyberattacks, data breaches, phishing, and other cybercrimes pose significant threats to businesses, financial institutions, and government organizations.

A breach of information security causes not only financial losses for companies but also damages their reputation and customer trust, ultimately impacting the entire economic system. Consequently, the issue transcends the technical level and becomes a strategic and politically important problem. Businesses and government agencies face the necessity to integrate advanced technologies such as artificial intelligence, machine learning, blockchain, and automation to effectively combat modern cyber threats.

This article aims to analyze the challenges of information security in the modern economy, including the economic damage caused by cyberattacks, opportunities for using innovative technologies, and the importance of relevant policies. Special attention is given to the context of Georgia, where the digital economy is rapidly developing but accompanied by challenges that require a systemic approach from both the public and private sectors.

It is noteworthy that information security is an integral component of a country's economic development and maintaining competitiveness in global markets. Therefore, effective legal frameworks, updates of national security strategies, and active cooperation with international partners are required.

In this way, the article serves not only to identify challenges but also to propose solutions that ensure a sustainable and secure economic environment in the digital age.

Keywords: Information Security, Cyberattacks, Digital Economy, Artificial Intelligence, Blockchain, Economic Damage, Georgian Economy, Cyber Defense, Digital Transformation, Government Policy.

³ Chief Editor of Scientific Research Center of LEPL-David Agmashenebeli National Defense Academy of Georgia Invited Associate Professor of Georgian Technical University, Academic Doctor of Business Technology

⁴ Assistant Professor of Technical University of Georgia, Academic Doctor of Informatics Engineering

შესავალი

ციფრული ტექნოლოგიების განვითარების შედეგად, თანამედროვე ეკონომიკა სწრაფი და სისტემური ტრანსფორმაციის პროცესშია. ბიზნესები, ფინანსური ინსტიტუტები და სახელმწიფო უწყებები სულ უფრო მეტად ხდებიან დამოკიდებული ინფორმაციული ტექნოლოგიების ინფრასტრუქტურაზე და მონაცემთა მართვაზე. ამასთან, ინფორმაციული უსაფრთხოების საკითხები ცენტრალურ მნიშვნელობას იძენს, რადგან ნებისმიერი დაუცველობა ან კიბერშეტევა შეიძლება გამოიწვიოს მნიშვნელოვანი ეკონომიკური ზარალი, ბიზნესის რეპუტაციის დეფექტი და მომხმარებელთა ნდობის დაკარგვა.

კიბერკრიმინალები მუდმივად აუმჯობესებენ თავიანთი ტექნიკებს, რაც ქმნის გამოწვევებს, როგორც ტექნიკურ, ასევე ორგანიზაციულ დონეებზე. შესაბამისად, თანამედროვე ეკონომიკის სტაბილურობა და განვითარება დამოკიდებულია არა მხოლოდ ინოვაციებზე, არამედ უსაფრთხოების სისტემების ეფექტურობაზე და სახელმწიფოს პოლიტიკაზე ინფორმაციული უსაფრთხოების დაცვის კუთხით.

ამ შესავლის მიზანია აღძრას საკითხის მნიშვნელობა და დაანახოს, რომ ინფორმაციული უსაფრთხოება არ არის მხოლოდ ტექნიკური პრობლემა, არამედ ეკონომიკური და სტრატეგიული კომპონენტი, რომელიც განსაზღვრავს ქვეყნის კონკურენტუნარიანობასა და მდგრადობას გლობალურ ციფრულ ეკონომიკაში.

სტატია მოიცავს ინფორმაციული უსაფრთხოების ძირითად გამოწვევებს, კიბერშეტევების ეკონომიკურ შედეგებს და საქართველოსთვის არსებულ სპეციფიკურ გამოწვევებს, აგრეთვე განიხილავს ინოვაციურ მიდგომებს და სახელმწიფო პოლიტიკის მნიშვნელობას ამ სფეროში.

ციფრული ტექნოლოგიების ინტეგრაცია ეკონომიკაში შექმნა ახალი შესაძლებლობები და გამოწვევები. ერთის მხრივ, მას სთავაზობს ეფექტურობას, სწრაფ გადაწყვეტილებებს და გლობალურ ბაზრებთან წვდომას. მეორეს მხრივ კი, ზრდის საფრთხეებს ინფორმაციული უსაფრთხოების თვალსაზრისით. ბოლო წლებში კიბერშეტევების რაოდენობა მნიშვნელოვნად გაიზარდა და მათი მიზნები სულ უფრო რთულდება, რაც საფრთხეს უქმნის არა მხოლოდ ინდივიდუალურ კომპანიებს, არამედ ქვეყნის მთელ ეკონომიკურ სისტემას.

ეკონომიკური ზარალი, გამოწვეული კიბერშეტევებით, მოიცავს როგორც პირდაპირ ფინანსურ დანაკარგებს, ისე სერვისების შეწყვეტას, მონაცემთა დაკარგვას, ინოვაციების შეფერხებას და მომხმარებელთა ნდობის შემცირებას. ამ საკითხის გლობალური მნიშვნელობა აისახა მრავალი ქვეყნის სახელმწიფო სტრატეგიებში, სადაც საინფორმაციო უსაფრთხოების გაძლიერება წარმოადგენს პრიორიტეტს.

საქართველოც, როგორც სწრაფად მზარდი ციფრული ეკონომიკის მქონე ქვეყანა, მნიშვნელოვან გამოწვევებს აწყდება ამ სფეროში. ციფრული ინფრასტრუქტურის გაფართოებასთან ერთად, აუცილებელია განახლდეს დაცვის მექანიზმები და შექმნას კოორდინირებული მიდგომები კერძო და საჯარო სექტორებს შორის.

ამ პროცესში, თანამედროვე ტექნოლოგიები, როგორიცაა ხელოვნური ინტელექტი და ბლოკჩეინი, იძლევიან ახალ შესაძლებლობებს ინფორმაციული უსაფრთხოების გაძლიერებისთვის, თუმცა მათი ეფექტური გამოყენება მოითხოვს კარგად ჩამოყალიბებულ პოლიტიკასა და საკანონმდებლო ბაზას.

სტატია მიზნად ისახავს ამ თემების კომპლექსურად განხილვას და შესთავაზოს რეკომენდაციები, რომლებიც დაეხმარება საქართველოსა და სხვა ქვეყნების ეკონომიკას გაუმჯობესოს თანამედროვე ციფრულ გამოწვევებს.

ძირითადი ნაწილი **თანამედროვე ეკონომიკის ციფრულ ტრანსფორმაციაში ინფორმაციული** **უსაფრთხოების როლი**

ციფრული ეკონომიკის განვითარება განპირობებულია სწრაფი ტექნოლოგიური ინოვაციებით, როგორიცაა ინტერნეტის მასიური გავრცელება, ღრუბლოვანი პლატფორმები, დიდი მონაცემები (Big Data), ხელოვნური ინტელექტი და ინტერნეტი ნივთების (IoT) ზრდა. ამ პროცესმა შეცვალა ბიზნეს-მოდელები, ოპერაციები და მომხმარებელთა მომსახურება.⁵

თუმცა, ტექნოლოგიური ტრანსფორმაცია თან ახლავს ახალ გამოწვევებს — ციფრული ინფრასტრუქტურა ხდება მოწყვლადი კიბერთავდასხმების მიმართ, რაც ქმნის სისტემურ რისკებს ეკონომიკისთვის. განსაკუთრებით მნიშვნელოვანია

⁵ R. Anderson, & Moore, T. *Information Security Economics – and Beyond*. Foundations and Trends® in Privacy and Security, 4(2-3), (2020). 149-219.

ფინანსური სექტორი, ენერგეტიკა, ლოგისტიკა და ჯანდაცვა, რომელთა შეფერხება შეიძლება გამოიწვიოს არა მხოლოდ ფინანსური დანაკარგი, არამედ სოციალურ და უსაფრთხოების კრიზისებამდეც კი მისვლა.

მაგალითად, 2021 წელს, აშშ-ში რეკორდულად გაიზარდა Ransomware ტიპის შეტევები, რამაც საშუალო ბიზნესს მნიშვნელოვნად შეუქმნა ფინანსური პრობლემები და ზოგიერთმა კომპანიამ კარი დახურა. ამ ტიპის თავდასხმები ხაზს უსვამს ციფრული ეკონომიკის მოწყვლადობას და საჭიროებს სისტემურ დაცვის მექანიზმებს.⁶

საქართველოში ციფრული ტრანსფორმაცია სწრაფად მიმდინარეობს, თუმცა ინფრასტრუქტურა და კიბერუსაფრთხოების პრაქტიკა ჯერ კიდევ ვითარდება. სახელმწიფოსთვის მნიშვნელოვანია ეროვნული სტრატეგიების შემუშავება და ინვესტიციების ზრდა, რათა დაცული იყოს როგორც საჯარო, ისე კერძო სექტორის მონაცემები და სისტემები.

კიბერშეტევების ტიპები და მათი ეკონომიკური გავლენა ფიშინგი (Phishing)

ფიშინგი წარმოადგენს ერთ-ერთ ყველაზე გავრცელებულ კიბერშეტევას, რომლის დროსაც თავდამსხმელები „მატყუარა“ ელ. ფოსტით ან სხვა დისტანციური საშუალებით მოიპარავენ მომხმარებლის პირად მონაცემებს — საბანკო ანგარიშის, საკრედიტო ბარათის, პაროლის და სხვა მნიშვნელოვან მონაცემებს. 2023 წელს, გლობალურად ფიშინგის შეტევების რაოდენობა გაიზარდა 40%-ით, რაც ქმნის მნიშვნელოვან საფრთხეს როგორც კომპანიებისთვის, ასევე პირადი მომხმარებლებისთვის.

Ransomware (გამტაცებელი პროგრამები)

Ransomware-ი „დაბლოკავს“ კომპანიის მონაცემებს და ითხოვს გამოსასყიდს მათ გასათავისუფლებლად. 2022 წლის მონაცემებით, ასეთი ტიპის შეტევებმა მიაყენა ზარალი მსოფლიო ბიზნესს 20 მილიარდ აშშ დოლარზე მეტი. მაგალითად, Colonial Pipeline თავდასხმა შეაჩერა აშშ-ს დასავლეთ სანაპიროს საწვავის მიწოდება

⁶ N. Kshetri, *Cybersecurity in Developing Economies: Challenges and Opportunities*. Journal of Information Technology, 36(1), 45-59. (2021).

რამდენიმე დღით, რაც გამოიწვია ფართო ეკონომიკური და სოციალური პრობლემები.

DDoS (Distributed Denial of Service)

ეს არის სერვერების გადატვირთვის მეთოდი, რაც იწვევს სერვისის ხელმისაწვდომობის შეზღუდვას მომხმარებლისთვის. DDoS შეტევები ხშირად გამოიყენება როგორც პოლიტიკური ან ფინანსური შანტაჟის საშუალება და ზოგჯერ თანახლავს სხვა სახის კიბერშეტევებს.

სოციალური ინჟინერია

ადამიანის ფსიქოლოგიის გამოყენებით, თავდამსხმელები იკვლევენ და აშინებენ თანამშრომლებს, რათა მათგან მიიღონ სენსიტიური ინფორმაცია. ეს არის მნიშვნელოვანი საფრთხე იმ კომპანიებისთვის, რომლებმაც არ გაზარდეს თანამშრომლების განათლებისა და კიბერუსაფრთხოების კულტურის დონე.

3. ინფორმაციული უსაფრთხოების გამოწვევები და რისკები თანამედროვე ბიზნესში

თანამედროვე ბიზნესი დგას წინაშე მრავალი გამოწვევის:

- ❖ **ადამიანური ფაქტორი** — კომპანიის თანამშრომლების არასწორი მოქმედება, არასაკმარისი კიბერუსაფრთხოების განათლება, პაროლის უსაფრთხოების შეცდომები და დაბალი ინფორმაციის დაცვა. 60%-ზე მეტი კიბერშეტევა სწორედ ადამიანის შეცდომით იწყება.
- ❖ **მოხმარებული ტექნოლოგიების მოძველება** — ძველი სისტემები არ ემორჩილებიან თანამედროვე უსაფრთხოების სტანდარტებს და ხდებიან მოწყვლადი.
- ❖ **მცირე ბიზნესის დაზარალების მაღალი რისკი** — მცირე და საშუალო კომპანიებს ხშირად არ აქვთ რესურსი, ინვესტიცია მოახდინონ კიბერუსაფრთხოებაში, რაც მათ ხშირად ჰქმნის ადვილ სამიზნედ.
- ❖ **მონაცემთა გაზრდილი მოცულობა** — გროვდება დიდი რაოდენობით მონაცემები, რაც რთულს ხდის მათი ეფექტიან დაცვას და კონტროლს.

❖ კერძოდ, საქართველო დიდ გამოწვევებს აწყდება კიბერუსაფრთხოების კვალიფიციური კადრების ნაკლებობის გამო, რაც აფერხებს დაცვის ხარისხის გაუმჯობესებას.⁷

4. საქართველოს გამოცდილება და გამოწვევები

საქართველოში ციფრული ეკონომიკა აქტიურად ვითარდება, თუმცა გამოწვევები მრავალი მიმართულებითაა:

- ❖ **ინფრასტრუქტურის მოწყვლადობა** — სახელმწიფო და კერძო სექტორი ხშირად იყენებს მოძველებულ სისტემებს, რაც ზრდის კიბერშეტევების რისკს.
- ❖ **რეგულაციებისა და სტანდარტების დანერგვის აუცილებლობა** — ჯერ კიდევ ვერ არის საკმარისად განვითარებული სამართლებრივი ბაზა, რომელიც მკაცრად და კონკრეტულად განსაზღვრავს კიბერუსაფრთხოების მოთხოვნებს.
- ❖ **კადრების მომზადება** — პროფესიონალების დეფიციტი სერიოზულ დაბრკოლებას ქმნის.
- ❖ **სახელმწიფო და კერძო სექტორის თანამშრომლობა** — პოზიტიური ტენდენციაა, მაგრამ საჭიროა მეტი კოორდინაცია და ინფორმაციის გაცვლა.
- ❖ **საერთაშორისო პარტნიორებთან თანამშრომლობით და სწავლებებით**, საქართველო პროგრესს აღწევს, თუმცა საჭიროა პროცესების სისტემატიზაცია და სტრატეგიული ინვესტიციები.⁸

5. ინოვაციური ტექნოლოგიები და მომავალი პერსპექტივები

- ❖ **ხელოვნური ინტელექტი (AI)** — ხელს უწყობს კიბერშეტევების ადრეულ აღმოჩენასა და რეალურ დროში რეაგირებას, რაც მნიშვნელოვნად ამცირებს ზარალის რისკს.
- ❖ **ბლოკჩეინი** — უზრუნველყოფს ინფორმაციის ავთენტიკურობას, გამჭვირვალობას და ინვულნერობას, რაც ხელს უშლის მონაცემთა მანიპულაციას და თაღლითობას.

⁷ N.Kshetri, *Cybersecurity in Developing Economies: Challenges and Opportunities*. Journal of Information Technology, 36(1), 45-59, (2021).

⁸ National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from, (NIST). (2024). <https://www.nist.gov/cyberframework> გადამოწმებულია 29.05.2025

- ❖ ავტომატიზაცია და მანქანური სწავლება — ეხმარება ანომალიების სწრაფ გამოვლენასა და თავდასხმების ავტომატურ ჩახშობაში.
 - ❖ ინტერნეტი ნივთების (IoT) უსაფრთხოების გაძლიერება — ზრდის მოწყობილობების დაცვას, რომლებსაც დიდი როლი აქვთ ციფრულ ეკონომიკაში.
 - ❖ 6. პოლიტიკა და სტრატეგიული რეკომენდაციები
 - ❖ კანონმდებლობის გამკაცრება — აუცილებელია ისეთი საკანონმდებლო ჩარჩო, რომელიც დაიცავს როგორც მომხმარებელს, ისე ბიზნესს.
 - ❖ სახელმწიფო-კერძო სექტორის პარტნიორობა — საჭიროა უფრო ღრმა თანამშრომლობა ინფორმაციის გაცვლისა და კიბერუსაფრთხოების ღონისძიებების ერთობლივი განხორციელებისთვის.
- განათლების და კადრების მომზადების პროგრამები — სტაბილური საფონდო ბაზის შესაქმნელად.
- ❖ საერთაშორისო თანამშრომლობა — გამოცდილი პარტნიორების ჩართვა და საუკეთესო პრაქტიკების იმპორტი.⁹

დასკვნა

ინფორმაციული უსაფრთხოება თანამედროვე ეკონომიკის განუყოფელ ნაწილად იქცა და მისი მნიშვნელობა წლიდან წლამდე იზრდება. ციფრულმა ტრანსფორმაციამ ახალი შესაძლებლობები გაუხსნა ბიზნესს და საზოგადოების ყველა სექტორს, თუმცა თან ახლავს საფრთხეები, რომლებიც არ შეიძლება იგნორირდეს. კიბერშეტევების, მონაცემთა უკანონო გამოყენების და ტექნოლოგიური ინფრასტრუქტურის მოწყვლადობის ზრდა პირდაპირ აღემატება ეკონომიკის მდგრადობას და სერიოზულ რისკებს უქმნის როგორც ეროვნულ, ისე გლობალურ მასშტაბებს.

საქართველოს მაგალითი კარგად წარმოაჩენს ამ რეალობას — სწრაფი ციფრული განვითარება არ თანაბრად მოაქვს უსაფრთხოების გაუმჯობესებას. ქვეყანას სჭირდება როგორც სამართლებრივი ჩარჩოს გამკაცრება, ისე ძლიერი პროფესიონალური

⁹Gartner. *Top Security and Risk Trends for 2024*. Retrieved from, (2023). <https://www.gartner.com/en/documents/3999707> გადმოწმებულია 29.05.2025

კადრების მომზადება და შესაბამისი ტექნოლოგიური ინფრასტრუქტურის განახლება. მხოლოდ ამ შემთხვევაში იქნება შესაძლებელი ეკონომიკის ეფექტური დაცვა და ინვესტიციების ჩადება ინოვაციებში და განვითარებაში.

მნიშვნელოვანია, რომ ინფორმაციული უსაფრთხოების პოლიტიკა და პრაქტიკა იყოს სისტემური, მრავალსხოვანი და ინკლუზიური — სახელმწიფოს, კერძო სექტორის და სამოქალაქო საზოგადოების თანამშრომლობით. თანამედროვე ეკონომიკაში უსაფრთხოება მოითხოვს არა მხოლოდ ტექნიკურ გადაწყვეტილებებს, არამედ კვალიფიციური ადამიანური რესურსების, ჯანსაღი ბიზნეს კულტურის და ერთიანი სტრატეგიის განვითარებას.

შემდგომი განვითარებისთვის აუცილებელია ხელოვნური ინტელექტის, მანქანური სწავლების და ბლოკჩეინის ტექნოლოგიების ინტეგრაცია, რომლებიც მნიშვნელოვან როლს შეასრულებენ კიბერდამუქებების აღმოჩენაში და პრევენციაში. ამავე დროს, აუცილებელია რეგულაციების შესაბამისი ადაპტაცია, რათა დაცულ იქნას მონაცემები და პირადი ინფორმაციის კონფიდენციალურობა.

საბოლოოდ, ინფორმაციული უსაფრთხოება თანამედროვე ეკონომიკის სტაბილურობისა და განვითარების ერთ-ერთი მთავარი საყრდენია, რომელიც მუდმივ მონიტორინგსა და ინვესტიციებს საჭიროებს. საქართველოსთვის ეს არის გამოწვევა და შესაძლებლობა ერთდროულად — თუ ქვეყანა მოახდენს წარმატებულ გარდაქმნას კიბერუსაფრთხოების სფეროში, ის შეძლებს არა მხოლოდ ადგილობრივ ბაზარზე კონკურენციას, არამედ საერთაშორისო არენაზეც წარმატებით წარდგეს.

ბიბლიოგრაფია

- Anderson, R., & Moore, T. (2020). *Information Security Economics – and Beyond*. Foundations and Trends® in Privacy and Security, 4(2-3), 149-219.
- Symantec Corporation. (2023). *Internet Security Threat Report*. Retrieved from <https://www.symantec.com/security-center/threat-report>
- Verizon. (2023). *Data Breach Investigations Report*. Retrieved from <https://www.verizon.com/business/resources/reports/dbir/>
- European Union Agency for Cybersecurity (ENISA). (2022). *Cybersecurity Challenges in the Digital Economy*. Retrieved from <https://surl.li/vcjeyv> .გადამოწმებულია 29.05.2025
- საქართველოს ინოვაციების და ტექნოლოგიების სააგენტო. (2024). *ციფრული ეკონომიკა და კიბერუსაფრთხოება საქართველოში*. თბილისი.

Kshetri, N. (2021). *Cybersecurity in Developing Economies: Challenges and Opportunities*. Journal of Information Technology, 36(1), 45-59.

National Institute of Standards and Technology (NIST). (2024). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from <https://surl.lt/wgrtno> გადამოწმებულია 29.05.2025

Gartner. (2023). *Top Security and Risk Trends for 2024*. Retrieved from <https://surl.li/zmrryi> გადამოწმებულია 29.05.2025