# ინფორმაციული უსაფრთხოება და კიბერუსაფრთხოების განვითარება

**ოთარ შონია, ლუკა შონია, ლევან ყოლბაია**

საქართველოს ტექნიკური უნივერსიტეტი
o.shonia@gtu.ge, shonia@gtu.ge, levank34@gmail.com

**რეზიუმე**

ნაშრომი განიხილავს ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების განვითარების თანამედროვე ტენდენციებს, გამოწვევებსა და მომავალ პერსპექტივებს. ციფრული ტრანსფორმაციის პირობებში, როდესაც ჩვენი ცხოვრების ყველა ასპექტი გახდა დამოკიდებული ინფორმაციულ ტექნოლოგიებზე, კიბერუსაფრთხოება სცდება ტექნიკური დისციპლინის ჩვეულებრივ ფარგლებს და იქცევა სტრატეგიულ, ეკონომიკურ და სოციალურ მნიშვნელობის საკითხად. სტატიაში გაანალიზებულია ახალი ტექნოლოგიების (ხელოვნური ინტელექტი, ნივთების ინტერნეტი, ბლოკჩეინი) გავლენა უსაფრთხოების ლანდშაფტზე, განხილულია Zero Trust-ის მოდელის მნიშვნელობა, ადამიანური ფაქტორის როლი და კიბერგანათლების გაუმჯობესების აუცილებლობა. ასევე აქცენტი გაკეთებულია საერთაშორისო თანამშრომლობისა და კანონმდებლობითი რეგულირების მნიშვნელობაზე, როგორც კიბერსივრცის ეფექტიანი მართვის აუცილებელ პირობაზე.

**საკვანძო სიტყვები:** ინფორმაციული უსაფრთხოება, კიბერუსაფრთხოება, ციფრული ტექნოლოგიები, ხელოვნური ინტელექტი, ნივთების ინტერნეტი (IoT), Zero Trust, კიბერდაცვა, მონაცემთა დაცვა, GDPR, კიბერგანათლება, საერთაშორისო თანამშრომლობა.

## 1. შესავალი.

თანამედროვე ციფრულ ეპოქაში ინფორმაცია გახდა ყველაზე მნიშვნელოვანი აქტივი და რესურსი, მისი დაცვა კი არანაკლებ მნიშვნელოვანი, ვიდრე ფიზიკური უსაფრთხოება. ციფრული ტექნოლოგიების სწრაფმა განვითარებამ, ინტერნეტის ყოველგვარ პროცესში ინტეგრაციამ და მონაცემთა მოცულობის ექსპონენციალურმა ზრდამ წარმოქმნა ახალი გამოწვევები. კიბერთავდასხმები დღეს აღარ არის მხოლოდ ინდივიდუალური ჰაკერების წყურვილი, ისინი გადაიქცნენ მოწინავე, კოორდინირებულ ოპერაციებად, რომლებსაც ახორციელებენ კიბერდანაშაულის ორგანიზებული ჯგუფები და სახელმწიფოებრივი სტრუქტურები. ამ თავდასხმების მიზანია არა მხოლოდ ფინანსური მოგება, არამედ პოლიტიკური გავლენის მოხდენა, კრიტიკული ინფრასტრუქტურის დაზიანება და საზოგადოებრივი აზრის მანიპულირებაა.

ზემოხსენებულ პირობებში, კიბერუსაფრთხოება უკვე წარმოადგენს სტრატეგიულ, სოციალურ და ეკონომიკურ პრობლემას, რომლის მართვა მოითხოვს კოორდინირებულ მოქმედებას სახელმწიფოს, ბიზნესისა და საზოგადოების თითოეული წევრის მხრიდან. ამ სტატიის მიზანია ყოვლისმომცველი ანალიზის ჩატარება ინფორმაციული უსაფრთხოების მიმდინარე მდგომარეობის, განვითარების ტენდენციებისა და იმ გამოწვევების შესახებ, რომლებიც დაკავშირებულია ახალ ტექნოლოგიებთან, ადამიანურ ფაქტორთან და გლობალურ კიბეროპერაციებთან.

## 2. მეთოდოლოგია.

სტატიის მოსამზადებლად გამოყენებული იქნა სამეცნიერო ლიტერატურის სისტემატიზირებული ანალიზის მეთოდი. შესწავლილი იქნა რეცენზირებული სამეცნიერო სტატიები,

სამეცნიერო-ანალიტიკური ანგარიშები და სტატისტიკური მონაცემები სანდო წყაროებიდან, როგორიცაა კიბერუსაფრთხოების კომპანიების (Symantec, Cisco) კვლევები, საერთაშორისო ორგანიზაციების (ENISA, ITU) ანგარიშები და აკადემიური პუბლიკაციები. ასევე გამოყენებული იქნა შედარებითი ანალიზის მეთოდი, რათა შეფასდეს სხვადასხვა მიდგომების (მაგ., Zero Trust) ეფექტურობა და სინთეზის მეთოდი ახალი ტექნოლოგიების გავლენის განსაზღვრისთვის. კვლევა ეფუძნება თეორიულ ჩარჩოს, რომელიც აერთიანებს ტექნოლოგიურ, ორგანიზაციულ და სოციალურ ასპექტებს.

## 3. მსჯელობა.

### 1. ტექნოლოგიური ევოლუცია და ახალი გამოწვევები

კიბერუსაფრთხოების სისტემები დღეს უკვე შორს არის ინდივიდუალური ანტივირუსებისა და ფაირვოლებისგან. ისინი გადაიქცნენ კომპლექსურ ეკოსისტემად, რომელიც უნდა აკონტროლებდეს მილიარდობით მოწყობილობასა და მომხმარებელს.

- **ხელოვნური ინტელექტი (AI) და მანქანური სწავლა (ML):** AI ორმაგი იარაღია კიბერუსაფრთხოების სფეროში. ერთი მხრივ, ის გამოიყენება თავდასხმების ავტომატიზაციისთვის, რაც საშუალებას აძლევს მოწინააღმდეგეს შექმნას ადაპტირებადი მავნე პროგრამები, რომლებიც თავს არიდებენ ტრადიციულ დაცვას. მეორე მხრივ, AI არის უმნიშვნელოვანესი ინსტრუმენტი თავდაცვისთვის. მანქანური სწავლების ალგორითმებს შეუძლიათ გაანალიზონ უზარმაზარი მოცულობის ქსელის ტრაფიკი რეალურ დროში, ამოიცნონ ანომალიები და შეამცირონ რეაგირების დრო მილიწამებამდე. AI-ზე დაფუძნებული სისტემებს შეუძლიათ პროგნოზირება მოახდინონ მომავალი თავდასხმების ტენდენციების შესახებ, რაც უსაფრთხოების ზომებს პროაქტიულ ხასიათს აძლევს.
- **ნივთების ინტერნეტი (IoT):** IoT-ის ექსპანსიამ – განათლების სისტემებიდან და სმარტფონებიდან მედიცინის მოწყობილობებამდე და სამრეწველო კონტროლერებამდე – რადიკალურად გაზარდა თავდასხმის ზედაპირი. ამ მოწყობილობების უმრავლესობა შექმნილია ფუნქციონალურობისა და ეკონომიკური ეფექტიანობის პრიორიტეტით, და არა უსაფრთხოების მექანიზმების გათვალისწინებით. შედეგად, ისინი ხშირად ხდებიან მარტივი სამიზნეები. დაუცველი IoT მოწყობილობების გამოყენება შესაძლებელია მასშტაბური DDoS თავდასხმების (როგორიც იყო Mirai-ს ბოტნეტი) განსახორციელებლად ან ფიზიკური ინფრასტრუქტურის დასაზიანებლად.
- **ბლოკჩეინი:** მიუხედავად იმისა, რომ ბლოკჩეინი ცნობილია კრიპტოვალუტების კუთხით, მისი პოტენციალი კიბერუსაფრთხოებისთვის ძალზედ მნიშვნელოვანია. მისი დეცენტრალიზებული, უცვლელი და დაშიფრული სისტემა შეიძლება გამოყენებულ იქნას უსაფრთხო სერტიფიკატების მართვისთვის, იდენტობის ვერიფიკაციისთვის და მონაცემთა მთლიანობის უზრუნველსაყოფად. თუმცა, ამავე დროს, სმარტ-კონტრაქტების დაუცველობა ან ბირჟების გაურკვევლობა ქმნის ახალ უსაფრთხოების რისკებს.

### 2. Zero Trust-ის პარადიგმა: „არ ენდო არავის, ყველა შეამოწმე“

ტრადიციული უსაფრთხოების მოდელები, რომლებიც დაფუძნებული იყო ე.წ. „ციხესიმაგრის“ კონცეფციაზე (დაცული პერიმეტრი, რომლის შიგნითაც ყველა იყო სანდო), აღარ არის ეფექტური მობილური, ღრუბლოვანი და დისტანციური მუშაობის პირობებში. Zero Trust-ის არქიტექტურა პასუხობს ამ გამოწვევებს. მისი ძირითადი პრინციპია:

- **ექსპლიციტური ვერიფიკაცია:** თითოეული მომხმარებელი, მოწყობილობა და აპლიკაცია უნდა იყოს ავტენტიფიცირებული და ავტორიზებული წვდომის მინიჭებამდე, მიუხედავად მათი მდებარეობისა (ქსელის შიგნით თუ გარეთ).
- **მინიმალური პრივილეგიის პრინციპი:** მომხმარებლებს ენიჭებათ მხოლოდ ის წვდომის უფლებები, რომლებიც მათ აბსოლუტურად აუცილებელი აქვთ დავალების შესასრულებლად.
- **დანაყოფების შექმნა (მიკროსეგმენტაცია):** ქსელი იყოფა პატარ-პატარა, იზოლირებულ სეგმენტებად, რათა თავდასხმის შემთხვევაში მისი გავრცელება შეზღუდული იყოს.

Zero Trust-ის ინტეგრაცია საშუალებას აძლევს ორგანიზაციებს მკაცრად აკონტროლონ თავიანთი ინფრასტრუქტურა და მნიშვნელოვანად შეამცირონ მონაცემთა გაჟონვის ან სხვა სახის კიბერთავდასხმების რისკი.

**3. ადამიანური ფაქტორი: ყველაზე სუსტი რგოლი**

ტექნოლოგიური მიღწევების მიუხედავად, ადამიანური ფაქტორი კვლავ რჩება ერთ-ერთ ყველაზე დიდ საფრთხედ. სოციალური ინჟინერიის თავდასხმები, როგორიცაა ფიშინგი, დამოკიდებულია არა სისტემების დაუცველობაზე, არამედ მომხმარებელთა უცოდინარობასა და უყურადღებობაზე. ერთი მომხმარებლის მიერ საეჭვო ბმულზე დაწკაპუნებამ ან პაროლის გაჟონვამ შეიძლება მთელი ორგანიზაციის დაცვის სისტემა გაანადგუროს. აქედან გამომდინარე, კიბერგანათლება ხდება არა მხოლოდ რეკომენდაცია, არამედ სტრატეგიული აუცილებლობა. რეგულარული ტრენინგები, ფიშინგის სიმულაციები და უსაფრთხოების კულტურის ჩამოყალიბება თანამშრომელთა შორის არანაკლებ მნიშვნელოვანია, ვიდრე ტექნიკური ინვესტიციები.

**4. რეგულაციური ჩარჩო და საერთაშორისო თანამშრომლობა**

კიბერსივრცე არ აღიარებს სახელმწიფო საზღვრებს, რაც აქცევს კიბერუსაფრთხოებას გლობალურ პრობლემად. ამ გამოწვევის მოსაგვარებლად აუცილებელია საერთაშორისო თანამშრომლობა და ერთიანი სტანდარტების შემუშავება.

- **GDPR (General Data Protection Regulation):** ევროკავშირის მიერ დანერგილი GDPR იქცა გლობალურ ბენჩმარკად მონაცემთა დაცვის სფეროში. ის ადგენს მკაცრ წესებს პერსონალური მონაცემების შეგროვების, დამუშავების და შენახვისთვის და აწესებს მნიშვნელოვან ჯარიმებს მათი დარღვევისთვის. ეს აიძულებს კომპანიებს სერიოზულად მიუდგნენ ინფორმაციულ უსაფრთხოებას.
- **სახელმწიფოთაშორისი თანამშრომლობა:** მთავრობები სულ უფრო აქტიურად თანამშრომლობენ ერთმანეთთან ინფორმაციის გაცვლის, საერთო საფრთხეების იდენტიფიცირების და კიბერდანაშაულის წინააღმდეგ ბრძოლის მიზნით. შექმნილია რეგიონალური და საერთაშორისო ორგანიზაციები (როგორიცაა ENISA, NATO-ს კიბერგანათლების ცენტრი), რომლებიც ხელს უწყობენ ამ თანამშრომლობას.

**4. შედეგები.**

კვლევისა და ანალიზის შედეგად გამოვლინდა შემდეგი ძირითადი პუნქტები:

1. კიბერუსაფრთხოება გადაიქცა სტრატეგიულ პრიორიტეტად სახელმწიფოს, ბიზნესისა და საზოგადოებისთვის, რომელიც პირდაპირ კავშირშია ეროვნულ უსაფრთხოებასთან და ეკონომიკურ სტაბილურობასთან.

2. ახალმა ტექნოლოგიებმა (AI, IoT, ბლოკჩეინი) შექმნეს როგორც ახალი შესაძლებლობები დამცველებისთვის, ასევე ახალი, უფრო დახვეწილი საფრთხეები თავდამსხმელებისთვის.
3. Zero Trust-ის არქიტექტურა წარმოადგენს ეფექტურ პასუხს თანამედროვე, ჰიბრიდული გარემოს გამოწვევებზე, რომელიც ცვლის ტრადიციულ პერიმეტრზე დაფუძნებულ მიდგომებს.
4. ადამიანური ფაქტორი კვლავ რჩება კრიტიკულად მნიშვნელოვან ასპექტად, ხოლო კიბერგანათლების დონის ამაღლება აუცილებელი პირობაა უსაფრთხოების საერთო დონის გასაზრდელად.
5. ეფექტიანი კიბერუსაფრთხოების უზრუნველსაყოფად აუცილებელია გლობალური თანამშრომლობა, ერთიანი სტანდარტების დანერგვა და კანონმდებლობის განვითარება.

## 5. დასკვნა.

ინფორმაციული უსაფრთხოება და კიბერუსაფრთხოების განვითარება არის მუდმივი და დინამიური პროცესი, რომელიც მოითხოვს მრავალფაქტორიან მიდგომას. ტექნოლოგიური ინოვაციები, როგორიცაა ხელოვნური ინტელექტი და Zero Trust-ის მოდელი, გვაძლევს მძლავრ ინსტრუმენტებს ახალი კიბერსაფრთხეების გასამკლავებლად. თუმცა, ტექნოლოგია აღნიშნული პრობლემების მხოლოდ ერთი ნაწილია.

რეალური წინსვლა შეუძლებელია ადამიანის ცნობიერების ამაღლების, უწყვეტი განათლებისა და უსაფრთხოების კულტურის ჩამოყალიბების გარეშე. პარალელურად, კიბერსივრცის გლობალური ბუნება მოითხოვს საერთაშორისო თანამშრომლობის გაძლიერებას და კანონმდებლობის ადაპტაციას ახალ რეალობასთან.

მომავალში, ციფრული უსაფრთხოება კვლავ დარჩება გლობალური ყურადღების ცენტრში. როგორც ჩვენი ციფრული ინფრასტრუქტურა განვითარდება, დაცვაც უნდა იყოს არა მხოლოდ რეაქტიული, არამედ პროაქტიული, ადაპტირებადი და ყოველთვის ერთი ნაბიჯით წინ. მხოლოდ ტექნოლოგიის, განათლებისა და კოოპერაციის სინერგიას შეუძლია უზრუნველყოს უსაფრთხო და მდგრადი ციფრული მომავალი.

## გამოყენებული ლიტერატურა:


1. საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ - https://matsne.gov.ge/document/view/1679424?publication=8
2. კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების 2025-2030 წლების სტრატეგია - https://dga.gov.ge/files/mUMPR8s3w59z.pdf
3. European Union Agency for Cybersecurity (ENISA). (2023). ENISA Threat Landscape 2023.
4. National Institute of Standards and Technology (NIST). (2020). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.
5. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207.
6. Cisco. (2023). Cisco Annual Internet Report (2018–2023).
7. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR).

# Development of Information Security and Cybersecurity

Otar Shonia, Luka Shonia, Levan Kolbaia

Georgian Technical University
o.shonia@gtu.ge, shonia@gtu.ge, levank34@gmail.com

**Abstract**

The paper discusses current trends, challenges and future prospects in the development of information security and cybersecurity. In the context of digital transformation, when all aspects of our lives have become dependent on information technologies, cybersecurity goes beyond the usual scope of a technical discipline and becomes an issue of strategic, economic and social importance. The article analyzes the impact of new technologies (Artificial Intelligence, Internet of Things, Blockchain) on the security landscape, discusses the importance of the Zero Trust model, the role of the human factor and the need to improve cyber education. Emphasis is also placed on the importance of international cooperation and legislative regulation as a necessary condition for effective management of cyberspace.

**Keywords:** Information Security, Cybersecurity, Digital Technologies, Artificial Intelligence, Internet of Things (IoT), Zero Trust, Cyber Defense, Data Protection, GDPR, Cyber Education, International Cooperation.