

კიბერუსაფრთხოების როლი ციფრული პროდუქტებისა და სერვისების ინოვაციურ განვითარებაში

DOI:10.36962/ECS106/6-8/2024-23

ნინო ბენდიანიშვილი
პროფესორის ასისტენტი, სტუ
E-mail: bendianishvili.nino@gtu.ge

რეზიუმე

ციფრული ეკონომიკის თანამედროვე გამოწვევებიდან გამომდინარე, მნიშვნელოვანია კიბერუსაფრთხოების საფრთხეების გაანალიზება, რაც მზარდ გავლენას ახდენს ეროვნულ უსაფრთხოებაზე. კიბერუსაფრთხოებასთან დაკავშირებული პრობლემების გადაჭრა განსხვავდება ახალი თაობის საერთაშორისო სავაჭრო შეთანხმებების ტენდენციებისგან, რომლებიც ქმნიან უსაფრთხოების ფართო გამოწვევებს და შექმნილია საერთაშორისო ვაჭრობასა და ეროვნულ უსაფრთხოებას შორის ბალანსის აღსადგენად. თუმცა, ეს ახალი მიდგომები შესაძლოა არ იყოს დაცული პოტენციური ბოროტად გამოყენებისგან. [1]

ციფრული ტექნოლოგიების სწრაფი განვითარება ზრდის თავდასხმების რისკს, რაც ორგანიზაციებს უფრო მგრძნობიარეს ხდის კიბერ საფრთხეების მიმართ. რაც უფრო მეტი მოწყობილობა, სისტემა და ქსელია ურთიერთდაკავშირებული, მით უფრო იზრდება წარმატებული კიბერშეტევების რისკი. რაც შეეხება საქართველოს კიბერუსაფრთხოების პოლიტიკას, უმთავრეს გამოწვევად რჩება შემდეგი: კიბერუსაფრთხოების პროაქტიული სახელმწიფო პოლიტიკის ჩამოყალიბება, სახელმწიფო უწყებებში კიბერცნობიერების ამაღლება, კადრების პრობლემა და კიბერუსაფრთხოების არაპრიორიტეტულობა. [2]

დღევანდელ სწრაფად განვითარებად ციფრულ გარემოში, ორგანიზაციები განიცდიან მნიშვნელოვან ცვლილებას, რომელიც ცნობილია, როგორც ციფრული ტრანსფორმაცია. ტერმინი „ციფრული ტრანსფორმაცია“ აღნიშნავს ციფრული ტექნოლოგიების ინტეგრაციას კორპორატიული ოპერაციების ყველა ასპექტში, რაც ღრმა გავლენას ახდენს კომპანიების ფუნქციონირებასა და ღირებულებაზე. მიუხედავად იმისა, რომ ციფრულ ტრანსფორმაციას უამრავი შესაძლებლობა და სარგებელი მოაქვს, თან სდევს კიბერუსაფრთხოების უამრავი გამოწვევა. დიდია კიბერუსაფრთხოების როლი და მნიშვნელობა უსაფრთხო ციფრული ტრანსფორმაციის უზრუნველსაყოფად.

საკვანძო სიტყვები: კიბერუსაფრთხოების უზრუნველყოფა, ციფრული ტრანსფორმაცია, მონაცემთა კონფიდენციალურობა, კიბერუსაფრთხოების სტრატეგია.

შესავალი

ინფორმაციის გაზიარების გაზრდა, თანამშრომლობის ხელშეწყობა (მათ შორის საერთაშორისო დონეზე) და მიწოდების მხარეზე უსაფრთხოების პრინციპების უზრუნველყოფა, მნიშვნელოვანი გზებია კიბერპოლიტიკის განსახორციელებლად. [3]

სანამ კიბერუსაფრთხოების როლს უფრო ღრმად ჩავუღრმავდებით, მნიშვნელოვანია გვესმოდე, რას გულისხმობს ციფრული ტრანსფორმაცია. ციფრული ტრანსფორმაცია მოიცავს ციფრული ტექნოლოგიების მიღებას, როგორცაა ხელოვნური ინტელექტი, გამოთვლები, დიდი მონაცემების ანალიტიკა და ახალი პროდუქტებისა და სერვისების შეთავაზება მომხმარებლისთვის პირობების გასაუმჯობესებლად. ეს საშუალებას აძლევს ორგანიზაციებს იყვნენ უფრო მოქნილი, ინოვაციური და კონკურენტუნარიანი ციფრულ ეპოქაში.

არსებობს კიბერუსაფრთხოების გაზრდილი რისკები ციფრულ ტრანსფორმაციაში: კიბერკ-

რიმინალები მუდმივად ეძებენ მოწყვლადობას ექსპლუატაციისთვის და ციფრული ტრანსფორმაცია მათ ახალ შესაძლებლობებს აძლევს. მონაცემთა დარღვევა, გამოსასყიდი პროგრამული თავდასხმები და ინსაიდერული საფრთხეები არის კიბერუსაფრთხოების რისკი, რომელსაც აწყდებიან ორგანიზაციები ციფრული ტრანსფორმაციის დროს.

ძირითადი ტექსტი

კიბერუსაფრთხოების სექტორში ამჟამად ყველაზე დიდი გამოწვევა არის კიბერუსაფრთხოების პოლიტიკის სტანდარტებსა და გაიდლაინებში ინტეგრირება. ასევე საჯარო და კერძო თანამშრომლობის მოდელი, რაც გულისხმობს კიბერუსაფრთხოების პროფესიონალების ნაკლებობას საჯარო სექტორში და კიბერუსაფრთხოების სტრატეგია, რაც ფოკუსირებულია კიბერდანაშაულებზე. [4]

კიბერუსაფრთხოების უზრუნველყოფა, როგორც ციფრული ტრანსფორმაციის საფუძველი, გულისხმობს შემდეგს: უსაფრთხო ციფრული ტრანსფორმაცია მოითხოვს პროაქტიულ და ყოველისმომცველ კიბერუსაფრთხოების სტრატეგიას. ციფრული ტრანსფორმაციის ყოველი ნაბიჯი უნდა იყოს გამყარებული ძლიერი კიბერუსაფრთხოების ზომებით, რათა უზრუნველყოფილი იყოს სენსიტიური მონაცემებისა და კრიტიკული სისტემების მთლიანობა, კონფიდენციალობა და ხელმისაწვდომობა.

ორგანიზაციებმა პროდუქტებისა და სერვისების წარმოებისას პრიორიტეტი უნდა მიანიჭონ კიბერუსაფრთხოების შემდეგ მიდგომებს: 1) რისკის შეფასება და მართვა - ორგანიზაციებმა უნდა ჩაატარონ რისკების რეგულარული შეფასება, რათა გამოავლინონ ციფრული ტრანსფორმაციის ინიციატივებთან დაკავშირებული პოტენციური საფრთხე და რისკები. 2) უსაფრთხო დიზაინის მიდგომა - უსაფრთხოება თავიდანვე უნდა იყოს ჩართული ციფრული ტექნოლოგიების, სისტემებისა და აპლიკაციების დიზაინში. 3) ძლიერი ავტორიზაცია და წვდომის კონტროლი - მრავალეტაპიანი ავთენტიფიკაცია, ასევე მკაცრი კონტროლი გადამწყვეტია მონაცემების დასაცავად და არავტორიზებული წვდომის შეზღუდვისთვის. 4) ძლიერი ქსელის უსაფრთხოება - როდესაც ორგანიზაციები აფართოებენ თავიანთ ციფრულ ინფრასტრუქტურას, მათი ქსელების დაცვა უმნიშვნელოვანესია. 5) მონაცემთა დაცვა და კონფიდენციალურობა - დაშიფვრის, მონაცემთა კლასიფიკაციისა და კონფიდენციალურობის დაცვის ტექნიკა უნდა იყოს გამოყენებული სენსიტიური მონაცემების დასაცავად. მონაცემთა დაცვის შესაბამისი რეგულაციების გაზიარება, როგორიცაა მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR - General Data Protection Regulation), აუცილებელია. 6) უწყვეტი მონიტორინგი და საფრთხის დაზვერვა - ორგანიზაციებმა უნდა შექმნან უსაფრთხოების ოპერაციების ცენტრი (SOC - Security Operations Center) და განახორციელონ რეალურ დროში მონიტორინგი, საფრთხეების დაზვერვა და ინციდენტებზე რეაგირება. ეს კიბერუსაფრთხოების პროაქტიული გამოვლენის საშუალებას იძლევა.

რაც შეეხება კიბერუსაფრთხოების სფეროში თანამშრომლობასა და პარტნიორობას, ამ სფეროს დიდი მნიშვნელობა ენიჭება. კიბერუსაფრთხოება მხოლოდ ორგანიზაციებს არ შეუძლიათ. გარე პარტნიორებთან თანამშრომლობა, როგორიცაა კიბერუსაფრთხოების სერვისის პროვაიდერები, ინდუსტრიული ასოციაციები და სამთავრობო უწყებები, აძლიერებს ორგანიზაციის უნარს დაიცვას კიბერუსაფრთხოების საფრთხეების დაზვერვის, საუკეთესო პრაქტიკისა და სტანდარტების გაზიარება აძლიერებს კოლექტიური კიბერუსაფრთხოების მდგრადობას ციფრული ტრანსფორმაციის დროს.

დასკვნა

ტექნოლოგიები განაგრძობენ განვითარებას და ახალი ციფრული ტრანსფორმაციის ინიციატივების გაჩენას. კომპანიები უნდა იყვნენ მოქნილნი თავიანთი კიბერუსაფრთხოების სტრატეგიების მართვაში. ხელოვნურ ინტელექტს და ავტომატიზაციას შეუძლია გადამწყვეტი როლი შეასრულოს კიბერუსაფრთხოების გაძლიერებაში. თანამშრომლების უწყვეტი ტრენინგი და

ცნობიერების ამაღლების პროგრამები უზრუნველყოფს, რომ ორგანიზაციები ფხიზლად იყვნენ განვითარებადი კიბერ საფრთხეების წინააღმდეგ.

დასკვნის სახით უნდა ითქვას, რომ ციფრული ტრანსფორმაცია უზარმაზარ შესაძლებლობებს სთავაზობს ორგანიზაციებს გააუმჯობესონ სამუშაოს ეფექტურობა, გააძლიერონ მომხმარებელთა გამოცდილება და მოიპოვონ კონკურენტული უპირატესობა. თუმცა, კიბერუსაფრთხოების ადეკვატური ზომების გარეშე, ამ მიღწევებს მნიშვნელოვანი რისკები მოჰყვება. ორგანიზაციებმა უნდა აღიარონ კრიტიკული როლი, რომელსაც კიბერუსაფრთხოება ასრულებს მათი ციფრული ტრანსფორმაციის ინიციატივების დაცვაში. კიბერუსაფრთხოებისადმი პროაქტიული და ყოვლისმომცველი მიდგომით, კომპანიებს შეუძლიათ ჩამოაყალიბონ ნდობა, დაიცვან კონფიდენციალური მონაცემები და უზრუნველყონ უსაფრთხო და წარმატებული ციფრული გარემო.

გამოყენებული ლიტერატურა:

- 1) „Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions“, Published online by Cambridge University Press: 08 May 2023, p.6;
- 2) ჯღარკავა ი., „საქართველოს კიბერუსაფრთხოების პოლიტიკა, გამოწვევები და შესაძლებლობები“, თბ. 2021, გვ. 30;
- 3) „Enhancing the Digital Security of Products“, Published on February 09, 2021, In series:OECD Digital Economy Papers, p.88;
- 4) „ინტერსექტორული თანამშრომლობის შესაძლებლობების მხარდაჭერა კვლევასა და ინდუსტრიას შორის“, თბ. 2022, TWINNING, გვ.19.

REFERENCES:

- 1) „Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions“, Published online by Cambridge University Press: 08 May 2023, p.6;
- 2) Jgharkava I., “Georgia’s Cyber Security Policy, Challenges and Opportunities”, Georgia 2021, p. 30;
- 3) „Enhancing the Digital Security of Products“, Published on February 09, 2021, In series: OECD Digital Economy Papers, p.88;
- 4) “Supporting Opportunities for Intersectoral Cooperation in Research and Between the Industry”, Georgia 2022, TWINNING, p.19.

THE ROLE OF CYBER SECURITY IN THE INNOVATIVE DEVELOPMENT OF DIGITAL PRODUCTS AND SERVICES

Nino Bendianishvili

Professor's Assistant, GTU

E-mail: bendianishvili.nino@gtu.ge

RESUME

Given the modern challenges of the digital economy, it is important to analyze cyber security threats, which increasingly affect national security. Addressing cyber security concerns is different from the trends in the new generation of international trade agreements, which create broad security exceptions and are designed to restore balance between international trade and national security. However, these new approaches may not be immune to potential abuse. [1]

The rapid development of digital technologies increases the risk of attacks, making organizations more susceptible to cyber threats. The more devices, systems and networks are interconnected, the greater the risk of successful cyber attacks. As for Georgia's cyber security policy, the following remain the main challenges: establishing a proactive state cyber security policy, raising cyber awareness in state agencies, staffing problems, and non-priority of cyber security. [2]

In today's rapidly evolving digital environment, organizations are undergoing a major change known as digital transformation. The term "digital transformation" refers to the integration of digital technologies into all aspects of corporate operations, which has a profound impact on the performance and value of companies. While digital transformation brings many opportunities and benefits, it also brings many cybersecurity challenges. The role and importance of cyber security in ensuring a secure digital transformation is huge.

Keywords: Ensuring Cyber Security, Digital Transformation, Data Privacy, Cyber Security Strategy.