

მდგრადი განვითარებისა და ინფორმაციის უსაფრთხოების მნიშვნელობა, როგორც უსაფრთხოების პროდუქტების განვითარების საშუალება

ნინო ბენდიანიშვილი

ეკონომიკის დოქტორი
სტუ-ს პროფესორის ასისტენტი

რეზიუმე

ელექტრონული კომერციის განვითარებასთან ერთად ბიზნესი დამოკიდებული გახდა საინფორმაციო სისტემებზე. ინფორმაციის უსაფრთხოება უფრო და უფრო მნიშვნელოვანია მონაცემთა დაცვისათვის. შესაბამისად, უსაფრთხოების ცვალებადი მოთხოვნები მორგებული უნდა იყოს თანამედროვე გარემოს და მხოლოდ ახალი სტრატეგიებითა და კიბერპოლიტიკით სარგებლობდეს. ელექტრონული კომერციის განვითარების ეტაპზე უნდა მოიაზრებოდეს აპლიკაციებისა და უსაფრთხოების საკითხები.

აღსანიშნავია ინფორმაციის უსაფრთხოების მნიშვნელობა მდგრადი განვითარებისთვის. ციფრული ტრანზაქციები, შეტყობინებების ავთენტიფიკაციის და ინტერნეტ აპლიკაციებში ძლიერი ინფრასტრუქტურის არსებობა შესაძლებელს ხდის არსებობდეს დაცული და სანდო ოპერაციები. შედეგად, უზრუნველყოფილი ხდება ინფორმაციის უსაფრთხოების ჩარჩოს მდგრადობა.

აღსანიშნავია უსაფრთხოების პოლიტიკა იდენტიფიკაციისა და ციფრული პროცესების გენერირების, მართვისა და შენახვის საკითხების განვითარების საქმეში. აუცილებელია კრიპტოგრაფიული უსაფრთხოების პოლიტიკის განხილვა, რომელიც მნიშვნელოვანი სისტემური პროცესია. კრიპტოგრაფია ყველაზე მნიშვნელოვანი ტექნიკაა, რომელიც ციფრულ ინფორმაციას გარდაქმნის ერთი ფორმატიდან მეორეში. იგი ეფუძნება რიცხვით მნიშვნელობას და ცნობილია, როგორც დაშიფვრის პროცესი.

საჭიროა ფრთხილად დაიგეგმოს უსაფრთხო ქსელი კიბერ თავდასხმების რისკების შემცირების უზრუნველსაყოფად. სწორმა ადმინისტრირებამ კი არასასურველი შედეგები მნიშვნელოვნად შეიძლება შეამციროს. ასე, რომ კარგი სისტემის დიზაინით შესაძლებელია უცნობი შეტევებისაგან დაცვა.

საკვანძო სიტყვები: უსაფრთხოების ტექნოლოგია მდგრადი განვითარებისთვის, ინფორმაციის უსაფრთხოების ჩარჩოს მდგრადობა, კრიპტოგრაფიული უსაფრთხოების პოლიტიკა, დაშიფვრის პროცესი.

“THE IMPORTANCE OF SUSTAINABLE DEVELOPMENT AND INFORMATION SECURITY AS A MEANS OF DEVELOPING SECURITY PRODUCTS”

Nino Bendianishvili

Doctor of Economics
Professor's Assistan of GTU

RESUME

With the development of e-commerce, businesses have become dependent on information systems. Information security is more and more important for data protection. Therefore, the changing security requirements must be adapted to the modern environment and only benefit from new strategies and cyber policies. Application and security issues should be considered at the stage of e-commerce development.

It is worth noting the importance of information security for sustainable development. Having a strong infrastructure for digital transactions, message authentication and Internet applications makes it possible to have secure and reliable operations. As a result, the sustainability of the **information security framework** is ensured.

It is worth noting the security policy in the development of issues of identification and digital processes of generation, management and storage. It is necessary to consider **cryptographic security policy**, which is an important systemic process. Cryptography is the most important technique that converts digital information from one format to another. It is based on a numerical value and is known as an **encryption process**.

A secure network needs to be carefully planned to ensure that the risks of cyber attacks are reduced. Correct administration can significantly reduce adverse effects. So, with a good system design, it is possible to protect against unknown attacks.

Keywords: Security Technology for Sustainable Development, Information Security Framework, Cryptographic Security Policy, Encryptionp Process.

თანამედროვე პერიოდში, ორგანიზაციების უმეტესობა დამოკიდებულია ინფორმაციის დამუშავების სისტემებზე, რასაც უზრუნველყოფს ელექტრონული კომერციის განვითარება. აღნიშნულმა დამოკიდებულებამ კომპიუტერული სისტემების დაცვის საჭიროება წარმოქმნა. რაც უზრუნველყოფილია საინფორმაციო სისტემების უსაფრთხოების საშუალებით. დღევანდელი მთავარი სტრატეგიაა მდგრადობის ინტეგრირება ბიზნესის განვითარებაში და ინვესტიციები ამ მიმართულებით. ახალი გაიდლაინები მოითხოვს რეგიონულ დონეზე გაერთიანდეს წინსვლა და შემუშავდეს სტრატეგია ერთიან ინტეგრირებულ რეგიონულ ჩარჩოში. რაც აუცილებელს ხდის საინფორმაციო სისტემების ფართო გამოყენებას. ინფორმაციული ტექნოლოგიების გამოყენებამ გაზარდა მოთხოვნა ორგანიზაციების მხრიდან უფრო დაცული იყოს მათი მონაცემები და ბიზნესი. ასე რომ, ელექტრონული გარემოს უმნიშვნელოვანესი ნაწილი გახდა საინფორმაციო სისტემის უსაფრთხოება. მასში მოიაზრება ელ-განათლება, ელ-მთავრობა, ელ-კომერცია და ა.შ.

უსაფრთხოების მოთხოვნები აუცილებელია ინფორმაციული უსაფრთხოების საქმეში. შემუშავებული უნდა იყოს უსაფრთხოების დონე საინფორმაციო სისტემისათვის. ინფორმაციის უსაფრთხოების მნიშვნელობა დიდია მდგრადი განვითარების საკითხში. მთავარი მიდგომა კი არის უსაფრთხოების მოთხოვნების ხაზგასმა ისე და ისე ისეთი სისტემებისადმი, როგორიცაა: ელ-კომერცია, ელ-მმართველობა და ელ-ბანკინგი.

მამასადამე, საინფორმაციო ტექნოლოგიები ცხოვრების დონეს აუმჯობესებს. ხდება ინფორმაციის გაზიარება და ძლიერდება სოციალური ურთიერთობები, რაც ეხმარება ორგანიზაციებს ელექტრონულ გარემოში კონკურენტუნარიანად ჩამოყალიბებაში. მნიშვნელოვანია უსაფრთხო საინფორმაციო სისტემის საჭიროების განსაზღვრა. საინფორმაციო სისტემების მთავარ საკითხს წარმოადგენს საიმედოობა და უსაფრთხოება. ორგანიზაციებს ესაჭიროებათ უსაფრთხოება დოკუმენტების გადაცემის დროს, რაც დამოკიდებულია საინფორმაციო სისტემების ნდობაზე. ბიზნეს ორგანიზაციებს უსაფრთხო ჩარჩო სჭირდებათ თავიანთი ინვესტიციების გასაზრდელად. ასე, რომ ყველა ორგანიზაციის განვითარება ინფორმაციულ უსაფრთხოებაზეა დამოკიდებული.

ორგანიზაციებს შორის ურთიერთდამოკიდებულების პროცესს მოჰყვება მათი საერთო ორგანიზაციათაშორისი ქსელების შექმნა. ამ მიმართულებით კიბერუსაფრთხოება და მდგრადი განვითარება ერთ-ერთ ყველაზე მნიშვნელოვან საკითხად იქცა. გარემოსდაცვითი საქონელი და მომსახურება არის ეკონომიკის ერთ-ერთი ყველაზე სწრაფად განვითარებადი სექტორი. ის სწორედ ქსელის ერთეუ-

ლებს შორის მზარდი ურთიერთობებით იკვებება.

კომპიუტერულ ტექნოლოგიებსა და კიბერუსაფრთხოებას მდგრადი განვითარების კონცეფციის განხორციელებაში შეუძლია წვლილი შეიტანოს. გარემოსდაცვითი ტექნოლოგიების განვითარება, ასევე კიბერუსაფრთხოება არის ერთ-ერთი მთავარი მიზანი ევროკავშირის ქვეყნებს შორის მდგრადი წარმოებისა და შიდა უსაფრთხოების კონცეფციების რეალიზაციისა.[1]

ბიზნესისათვის საინფორმაციო სისტემის უსაფრთხოება არ გულისხმობს მხოლოდ იმას, რომ მათ საშუალება ჰქონდეთ მხოლოდ ახალი ბაზრის შესაძლებლობებით სარგებლობისა, არამედ უზრუნველყოფილი უნდა იყოს მათი აქტივების დაცვაც. მათ ნდობა უნდა ჰქონდეთ ელექტრონულ სამყაროში, რომ გააგრძელონ თავიანთი სპეციფიკური საქმიანობა მთელ მსოფლიოში.

უსაფრთხოების ტექნოლოგიას უაღრესად დიდი როლი აქვს მდგრადი განვითარებისათვის. ტერმინი უსაფრთხოება სწორად უნდა იქნას გაგებული ინტერნეტზე დაფუძნებული სისტემების საკითხში. ნებისმიერ აპლიკაციას აუცილებელია ჰქონდეს უსაფრთხოების პოლიტიკა. ასევე შესაბამისი უსაფრთხოების მექანიზმები. მნიშვნელოვანია მისი გამოყენებისთვის საჭირო ტერიტორია, აგრეთვე მონიტორინგისა და აუდიტის მექანიზმები, რაც უზრუნველყოფს სისტემის უსაფრთხო ფუნქციონირების შემომწმებას. წვდომის კონტროლის მექანიზმები უზრუნველყოფენ მომხმარებელთა დაცულობას. ხდება წვდომა საინფორმაციო რესურსებზე და ბიზნეს ტრანზაქციები ინარჩუნებს კონფიდენციალურობას.

კიბერშეტევების შემცირების ერთ-ერთი მნიშვნელოვანი ხერხია ფრთხილად დაგეგმვა უსაფრთხო ქსელისა და მისი ადმინისტრირება. კიბერუსაფრთხოების ზუსტი განმარტება სადავოა. მაგრამ მდგრადი განვითარების მიზნებისათვის მოიაზრება, როგორც მრავალმხრივი საფრთხის ლანდშაფტის წინააღმდეგ ბრძოლა. იგულისხმება კონფიდენციალურობა, მთლიანობა, ავთენტურობა და ციფრული ინფორმაციის ხელმისაწვდომობა. ასევე ძირითადი ინფრასტრუქტურის დაცვა და ნდობის უზრუნველყოფა. მნიშვნელოვანია ციფრული სერვისების ტექნიკური, პოლიტიკური და საგანმანათლებლო ღონისძიებების ერთობლიობა. შესაბამისად გაუმჯობესდება კიბერუსაფრთხოება თანამედროვე კიბერ საფრთხეების სრული სპექტრის მოსაგვარებლად.[2]

კიბერუსაფრთხოების ბიუროს ერთ-ერთ მიდგომას წარმოადგენს ტექნოლოგიური მდგრადობის უზრუნველყოფა. გარდაუვალი გაციფრულების პროცესის კვალდაკვალ, ხდება საქმისწარმოების გამარტივება და პროცესები ეფექტიანობის სხვა დონეზე გადადის. მნიშვნელოვანია უსაფრთხოე-

ბის უზრუნველყოფა და პროაქტიული კიბერთავდაცვითი მექანიზმების შემუშავება. სტრატეგიის მიზნები და სამოქმედო გეგმა სამი მიმართულებით ყალიბდება. ეს არის ადამიანი, პროცესი და ტექნოლოგია.[3]

კრიპტოგრაფია არის უმნიშვნელოვანესი ტექნიკა, რომელიც ციფრულ ინფორმაციას გარდაქმნის ერთი ფორმატიდან მეორეზე. იგი ეფუძნება რიცხვით მნიშვნელობას და ცნობილია, როგორც დაშიფვრის გასაღები.

დაშიფვრის პროცესი შერეულია და ხდება შეტყობინებების მიღება. მისი გაშიფვრა შეუძლია მიმღებს და მისი უზრუნველყოფა ხდება ორიგინალური გასაღებით (სიმეტრიული დაშიფვრა). ან განსხვავებული, თუმცა დაკავშირებული გასაღებით (ასიმეტრიული დაშიფვრა). ანუ ცნობილია - საჯარო გასაღები კრიპტოგრაფია. იგი აკავშირებს ნყვილ გასაღებს. ერთი არის კერძო და ხოლო მეორე - საჯარო. საჯარო გასაღების მეშვეობით დაშიფრული ინფორმაცია შეიძლება მხოლოდ შესაბამისი პირადი გასაღების გამოყენებით. ასევე, საჯარო და პირადი გასაღებები გამოიყენება ციფრული ხელმოწერების შესაქმნელად და შესამოწმებლად. ციფრული ხელმოწერა ემატება შეტყობინებებს. ხდება მათი ავთენტიფიკაცია დაცული და სანდო ტრანზაქციების შესასრულებლად. ეს ყოველივე ინფორმაციის უსაფრთხოების ჩარჩოს მდგრადობის ამაღლებას უზრუნველყოფს. კრიპტოგრაფიული უსაფრთხოების პოლიტიკა გამოიყენება ციფრული სერტიფიკატების შენახვის, მართვისა და გენერირებისათვის.

ზოგიერთ კომპანიაში შესაძლებელია დაინერგოს მაგალითად ღრუბლოვანი ტექნოლოგიების პლატფორმა - Nextcloud. იგი არის გარანტი ორგანიზაციის შიგნით, შიდა ქსელის მეშვეობით, ერთმანეთში ფაილების მიმოცვლის კონფიდენციალურობისა. იგი არსებობს პროგრამული პაკეტის, აგრეთვე ვირტუალური სახითაც.[4]

დასკვნა

დასკვნის სახით უნდა ითქვას, რომ ინფორმაციის უსაფრთხოების მნიშვნელობა დიდია მდგრადი განვითარების საკითხში. უსაფრთხოების ტექნოლოგიას უაღრესად დიდი როლი აქვს მდგრადი განვითარებისათვის. დაკმაყოფილებული უნდა იყოს ინფორმაციული უსაფრთხოების სხვადასხვა მოთხოვნა მდგრადი განვითარებისთვის. მაგალითად ეს ეხება სხვადასხვა ინფრასტრუქტურის საიმედოობას სხვადასხვა ელექტრონული აპლიკაციის შემთხვევაში. საინფორმაციო ქსელის ღიაობის გამო და ასევე იმიტომაც, რომ ინტერნეტს შეუზღუდავი ბუნება აქვს, ჰაკერობისაგან დაცვა უფრო და უფრო რთული ხდება. გამომდინარე აქედან, აუცილებელია უსაფრთხოებასთან დაკავშირებული საკითხების მოგვარება. ინფორმაციის დაცვისა და უსაფრთხოების გაზრდის მიზნით, არსებობს სხვადასხვა ტექნიკა, რაც გულისხმობს დროებით შესწორებებს. ეს ყოველივე აგვარებს ინტერნეტ უსაფრთხოების პრობლემების ფართო სპექტრის მხოლოდ მცირე ნაწილს. აღსანიშნავია ცვლილება მიდგომებში, ინერგება აპლიკაციები. ასევე ხდება დაზისტებები ინტერნეტის სტრუქტურაში.

გამოყენებული ლიტერატურა:

- 1) Sulicha A., Rutkowskab M., Krawczyk-Jezierskaa A., Jezierskib J., Zemaa T., „Cybersecurity and Sustainable Development“, 25th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, Published by Elsevier B.V., 2021, p.-9;
- 2) OCSC AND THE 2030 AGENDA „CYBERSECURITY AND SUSTAINABLE DEVELOPMENT An Intersectional Analysis“ 2022, p. 7-21;
- 3) კიბერუსაფრთხოების ბიურო, „საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების სტრატეგია“ 2021-2024, გვ.14-21;
- 4) ქართველიშვილი ი., „ინფორმაციის დაცვა და კიბერუსაფრთხოების სისტემები“, „სტუ-ს IT კონსალტინგის სამეცნიერო ცენტრი“, თბილისი 2020, გვ. 30-50.