საბანკო სისტემის ინფორმაციული უსაფრთხოების ამაღლების შესაძლებლობები ბიომეტრიული ტექნოლოგიის გამოყენებით

თინათინ კაიშაური, კორნელი ოდიშარია, დავით გომელაური
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განიხილება საბანკო სისტემის ინფორმაციული უსაფრთხოების ამაღლების მიზნით პერსონალის ბიომეტრიული მახასიათებლების გამოყენების თავისებურებები და პერსპექტივები.

საკვანძო სიტყვები: ბანკი. ინფორმაცია. უსაფრთხოება. საბანკო სისტემა. ბიომეტრია. ბიომეტრიული ტექნოლოგია. ინფორმაციული უსაფრთხოება.

1. შესავალი

საბანკო სისტემა ნებისმიერი სახელმწიფოს ერთ–ერთი უმთავრესი ელემენტია. მისი უსაფრთხოდ ფუნქციონირება საარსებო მნიშვნელობისაა. საბანკო სისტემის უსაფრთხოების სფეროში არსებული მდგომარეობა ქვეყანის სოციალურ–ეკონომიკური სიძნელეების ერთგვარი ინდიკატორია. ეს გარემოება კი მოითხოვს სახელმწიფოსგან განსაკუთრებული ყურადღების მიქცევას აღნიშნული სისტემის სტაბილური განვითარებისათვის, შესაბამისი პირობების შექმნას, რაც პირველ რიგში უნდა იყოს განმტკიცებული ნორმატიულ–სამართებლივი მდგომარეობით.

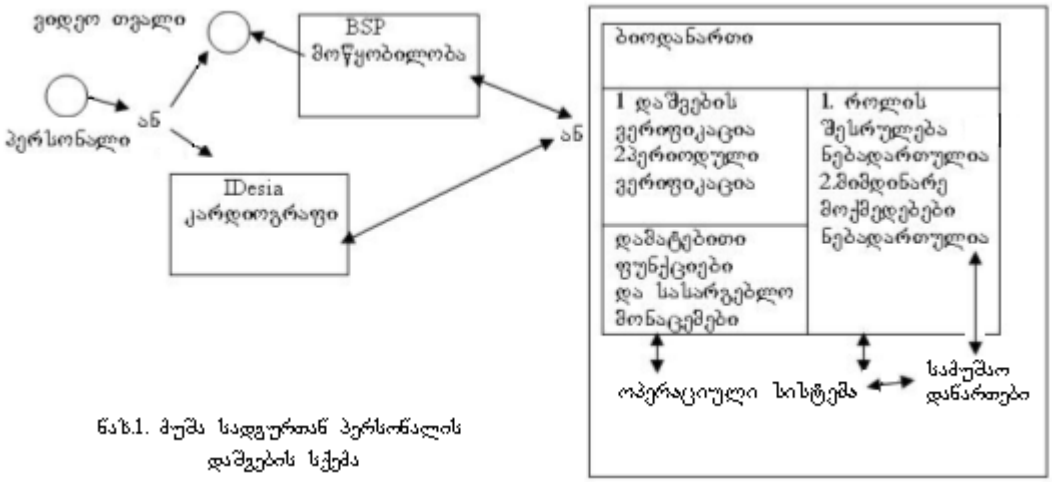
2. ძირითადი ნაწილი

საქართველოში ამ კუთხით ხელმისაწვდომი სამართებლივი დოკუმენტების ანალიზმა აჩვენა არც ისე სახარბიელო მდგომარეობა [1]. გასული წლის აგვისტოს მოვლენებმა კიდევ უფრო აქტუალური გახადა საბანკო სისტემის, მისი კლიენტების ინფორმაციული და სხვა რესურსების დაცულობის დონის მნიშვნელოვნად ამაღლება, ამის მიღწევა კი შესაძლებელია ინფორმაციულ ტექნოლოგიებში ამ მიმართულებით არსებული უახლესი მიღწევების ათვისებით და დანერგვით. ვფიქრობთ, რომ ამ თვალსაზრისით მნიშვნელოვანი დახმარების გაწევა შეუძლია საბანკო სისტემაში ბიომეტრიული ტექნოლოგიების გამოყენებას.

ნებისმიერი ბანკის ავტომატიზებული საბანკო სისტემა (ასს) შეიძლება მივაკუთვნოდ რთულ, ინტეგრირებულ კორპორაციულ სისტემათა კლასს, რომლის ინფორმაციული უსაფრთხოების უზრუნველყოფაც საკმაოდ რთული პრობლემაა და მოითხოვს ერთიან კომპლექსურ მიდგომას ჩვენ პირველ რიგში გვინდა ყურადღება გავამახვილოთ ბიომეტრიის გამოყენებაზე [1,2], ბანკის პერსონალის ასს–ის რესურსებთან მუშაობის, და ამ შემთხვევაში მათ მიერ განსაზღვრული როლის შესრულების უზრუნველყოფის კონტროლზე.

განვიხილავთ პერსონალის მუშაობას საკუთარ მუშა სადგურთან (პერსონალურ კომპიუტერთან) და ასს მონაცემთა ბაზების სერვერთან. მუშა სადგური ჩართვისას ოპერაციული სისტემის (ოს) მიერ ხდება „ბიოდანართის აქტივირება“. აღნიშნული დანართი აუცილებლად უნდა მუშაობდეს ავტომატურ რეჟიმში და მან უნდა მოითხოვოს ბიომეტრიული მოწყობილობისაგან მოცემულ მომენტში რესურსთან მყოფი ვიდეო გამოსახულება, რომლის ვერიფიკაციაც უნდა მოახდინოს მის მახსოვრობაში შენახულ პერსონალის შაბლონთან. ცხადია პერსონალის ასს რესურსთან მუშაობისას მის მიერ ნებადართული როლის შესრულების კონტროლისათვის აღნიშნული ბიომეტრიული მახასიათებლის გამოყენება მოითხოვს გარკვეულ ხარჯებს და ამასთან ერთად შეიცავს ბიომეტრიული მახასიათებლებით პერსონალის ამოცნობის ალბათობის მნიშვნელობასთან დაკავშირებულ რისკს, რაც ამ ტიპის ბიომოწყობილობებისათვის შეიძლება იყოს შედარებით დაბალი და მის ასამაღლებლად საჭიროა სპეციალური მეთოდების გამოყენება [3]. ბიომეტრიული მახასიათებლების ვერიფიკაციის სიზუსტის (პიროვნების ამოცნობა მაღალი ალბათობით) ამაღლება მეცნიერების ინტენსიური ყურადღების ქვეშაა. ამის დასტურად გამოდგება ებრაული კომპანია Idesia–ს მიერ ლას–ვეგასში გამართულ გამოფენა CES 2009–ზე წარმოდგენილი ელექტროკარდიოგრამით პირთა იდენტიფიკაციის ახალი სისტემა რომლის

სიზუსტეც სისტემის შემქმნელების განცხადებით, დაახლოებით 99%-ია, რაც საკმაოდ მაღალი მაჩვენებელია. ამას ისიც ემატება, რომ ელექტროკადრიოგრამით ინდენტიფიცირების უპირატესობას წარმოადგენს აპარატურის შედარებითი ღირებულობა და უფრო კომპაქტური ზომები. აღსანიშნავია, რომ აპარატურის მონტაჟი დაახლოებით 1 აშშ დოლარს შეადგენს, რაც განპირობებულია მოწყობილობის სიმარტივით: გულის სიგნალების გასაზომათ საკმარისია მხოლოდ ორი ელექტროდი (ერთი მარჯვენა ხელის, ხოლო მეორე – მარცხენა ხელის თითისათვის) ამასთან სხვა ბიომეტრიული სისტემებისაგან განსხვავებით Idesia პროდუქტი არ მოითხოვს სპეციალური სენსორების ან კამერების დამონტაჟებას, ხოლო სისტემის სიმარტივე განაპირობებს მის მომცრო ზომებს, რაც საშუალებას იძლევა მისი ინტეგრირების უპრობლემოდ მოხდენას ისეთ პატარა მოწყობილობებშიც, როგორიცაა, მაგალითად სმარტ ბარათი. ამრიგად პერსონალის ასს–ის რესურსთან მუშაობა (ვგულისხმობთ სისტემაში ნებისმიერ მუშა სადგურს) იწყება მისი ბიომეტრიული მახასიათებლის შეტანით და ვერიფიკაციის შემთხვევაში სუბიექტ–პერსონალს ეძლევა ნებართვა იმუშაოს რესურსთან მართვის დაწესებული როლის ფარგლებში (ნახ.1)



ნახ.1. მუშა სადგურთან პერსონალის დაშვების სქემა

„ბიო დანართს“ უნდა გააჩნდეს ის თავისებურება, რომ მან დროის ალბათურ მომენტებში (რესურსთან მომუშავე პერსონალისაგან დამოუკიდებლად) მოახდინოს ბიო-მოწყობილობის აქტივირება და სუბიექტის მომენტალური ვერიფიკაცია. „ბიო დანართი“ ასს–ის დაცულობის კონტროლის სისტემას აწვდის ალბათური შემოწმების შედეგებს, ერთდროულად დანართი შეიცავს აღნიშნული სისტემისათვის პერსონალის როლის შესაბამის მოდელს, რომლითაც ხდება პერსონალის მოქმედებათა კონტროლი და შედეგების ისევ საერთო კონტროლის სისტემისათვის მიწოდება. იმ შემთხვევაში, თუ სუბიექტი ცდილობს მიმართოს მისთვის აკრძალულ მოქმედებებს „ბიო დანართი“ ახდენს სუბიექტის რესურსთან მუშაობის პროცესის ბლოკირებას და კონტროლის სისტემის და საკრედიტო ორგანიზაციის ინფორმაციული უსაფრთხოების (იუ) სისტემის ადმინისტრატორის ინფორმირებას.

ვთვლით, რომ „ბიო დანართში“ სასურველია რეალიზებულ იყოს ისეთი შესაძლებლობები, რომლებიც საშუალებას იძლევა დაკომპესირდეს ბიომეტრიული ტექნოლოგიებისათვის დამახასიათებელი მხარეები, კერძოდ:

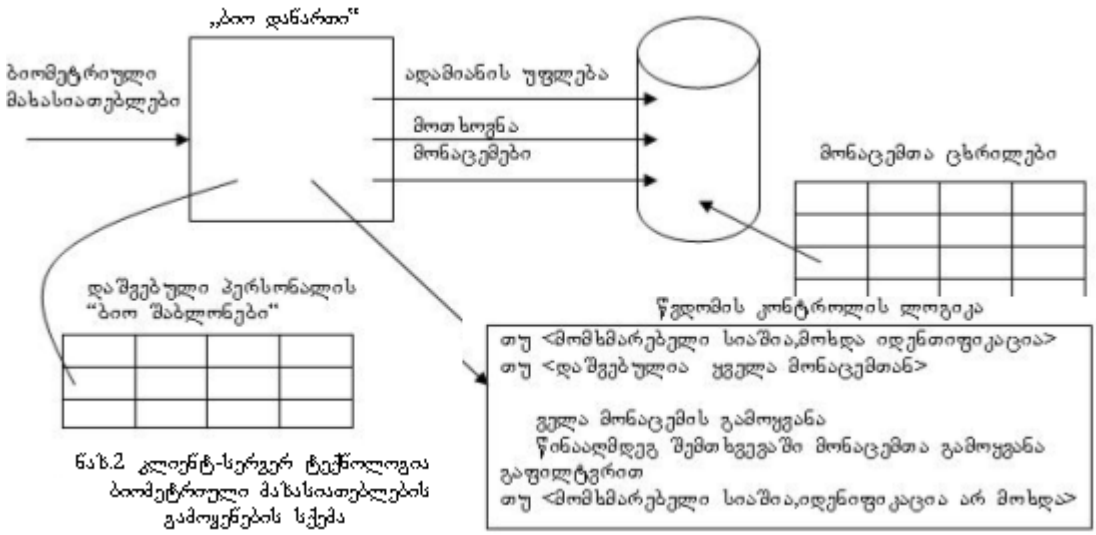
- ბიომეტრიულ მონაცემთა დაფიქსირების და დამუშავების ხარისხის შესახებ მონაცემების მიღება;
- რესურსის მომხმარებელი სუბიექტის (პერსონალის) ბიომეტრიული მახასიათებლების შესახებ რეალური ალბათურ შეფასებათა მიღება ბიომეტრიული მოწყობილობისაგან ან სისტემისაგან;
- ბიოდანართის მხრიდან რესურსის მომხმარებლის გრაფიკული ინტერფეისის მართვა;
- კლიენტ–სერვერ ტექნოლოგიის გამოყენება;
- შაბლონების ადაპტაცია;
- მუშაობა სხვადასხვა ტიპის ავტონომიურ ბიომეტრიულ მოწყობილობებთან;
- ძებნის სივრცის განზომილების შეზღუდვა მონაცემთა ბაზაში ერთის მრავალთან იდენტიფიკაციის პროცესში;

ასს–ში საერთო დანიშნულების რესურსებიდან უმნიშვნელოვანესია კორპორატიულ მონაცემთა ბაზებთან პერსონალის როლების შესაბამისად დაშვება. ვთქვათ მონაცემთა ბაზა (მბ) შედგება {Oi} დასაცავი ობიექტების სიმრავლისაგან. რეალურ მონაცემთა ბაზაში დასაცავმა ობიექტმა შეიძლება

მიიღოს ნებისმიერი მნიშვნელობა სიმრავლიდან. მბ–ს შეიძლება ყავდეს {S} მომხმარებელი. მბ–ში შესაძლებელია შემდეგი ოპერაციები: „წაკითხვა“, „ჩაწერა“, „შეცვლა“, „დამატება“, „განადგურება“. შეღწევის მეთოდი ავღნიშნოთ t ცვლადით, რომელსაც შეუძლია მიიღოს ნებისმიერი მნიშვნელობა სიმრავლიდან (t1, t2,..., tn).

იმისათვის, რომ გაკონტროლდეს სუბიექტის უფლებები, შემოგვაქვს ლოგიკური პრედიკატი P, რომელიც შეგვიძლია დავაკავშიროთ რესურსით სარგებობლის უფლების მქონე პერსონალის ბიომეტრიული იდენტიფიკაციის შედეგთან. ამიტომ დაშვების წესს ექნება ვექტორის სახე <S,O,T,P>. ეს კი იმას ნიშნავს , რომ S სუბიექტს შეუძლია გამოიყენოს O ობიექტთან დაშვების ტიპი t თუ პრედიკატ P-ს აქვს ჭეშმარიტი მნიშვნელობა, ე.ი. თუ სუბიექტის ბიომეტრიული მონაცემები შეესაბამება შაბლონს, რომელსაც აქვს მოცემული ტიპის დაშვების უფლება.

ასს განაწილებული ვარიანტისათვის სუბიექტის ბიომეტრიული მახასიათებლები ფიგურირებს დაცვის სისტემის ყველა დონეზე. პირველი ბარიერი – ესაა მუშა სადგური ან მობულური ტერმინალი, მეორე ბარიერი – ქსელში შეღწევა და ბოლოს, შეღწევა ასს–ის კორპორატიულ მონაცემთა ბაზაში. ცხადია, აქ აუცილებლად სუბიექტს მოუწევს მონაცემთა ბაზების მართვის სისმტემის (მბმს) დაცვის გადალახვა. ამასთან ერთად საჭიროა გამოვიყენოთ თვით ბიო–დანართთან სუბიექტის დაშვების მოთხოვნის მართვის შესაძლებლობა, რაც დაცვის კიდევ ერთ ბარიერს წარმოადგენს. ამ შემთხვევაში „ბიო დანართი“–ს გამოყენების უფრო მოქნილ ვარიანტია კლიენტ–სერვერ ტექნოლოგია (ნახ.2):



ნახ.2 კლიენტ-სერვერ ტექნოლოგია ბიომეტრიული მახასიათებლების გამოყენების სქემა

ეს ვარიანტი საკმაოდ რთულია, მაგრამ საიმედო. საქმე იმაშია, რომ დაცვის სისტემის ორგანიზებისას, ამ შემთხვევაში, შესაძლებელია საკმაოდ რთული–ძნელად ამოსაცნობი შემოწმების მეთოდების ჩადება, რომლებიც უნდა განსხვავდებოდეს სტანდარტულისაგან, რაც კარგადაა ცნობილი ბოროტგანმზრახველებისთვის.

აღნიშნული მიდგომა აუცილებლად უნდა ატარებდეს კომპლექსურ ხასიათს, რაც იმას ნიშნავს რომ ასს უსაფრთხოების სისტემის შექმნისას ერთმანეთთან კარგად უნდა იყოს შეთანხმებული როგორც დაცვის სტანდარტული ასევე ორიგინალური, არასტანდარტული მექანიზმები.

ბიომეტრიის ალბათური ხასიათის გამო „ბიო დანართში“ აუცილებლად გასათვალისწინებელია შაბლონთან „სასარგებლო მონაცემების“ მიერთების შესაძლებლობა (ნახ.1). ამ მონაცემების გამოყენება შესაძლებელი უნდა იყოს წარმატებული ვერიფიკაციის შემდეგ, როგორც PI-კოდები ან კრიპტოგრაფიული გასაღებები. ეს კი დამოკიდებული უნდა იყოს ბიო-იდენტიფიკაციის სიზუსტეზე Pcp ალბათობაზე.

თუ მისი ფაქტობრივი მნიშვნელობა მეტი იქნება რაღაც ზღვრულ მნიშვნელობაზე, ე.ი. როცა სუბიექტის საიმედოთ ამოცნობა ეჭვს არ იწვევს. მიზანშეწონილია, ასეთი შესაძლებლობების გამოყენება ხდებოდეს განსაკუთრებულ შემთხვევებში, ავტომატიზებული საბანკო სისტემის დაცულობის საერთო პოლიტიკიდან გამომდინარე. საქმე იმაშია, რომ „სასარგებლო მონაცემების“ დაცვისათვის დამახასიათებელი იქნება იგივე სიძნელეები რასაც ვაწყდებით ჩვეულებრივი გასაღებების ინფორმაციის დაცვის დროს.

3. დასკვნა

საბანკო სისტემაში ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით ადამიანის ბიომეტრიული მახასიათებლების გამოყენება ინოვაციური მიდგომაა. ამ მხრივ მნიშვნელოვან შედეგებს უნდა ველოდეთ ებრაული კომპანია Idesia-ს ელექტროკარდიოგრამით პირთა იდენტიფიკაციის ახალი სისტემის დანერგვით, ვინაიდან აღნიშნული სისტემა გამოირჩევა არა მარტო სიმარტივით და დაბალი ღირებულებით, არამედ, რაც ყველაზე უფრო მთავარია,სიზუსტით-დაახლოებით 99%.

ლიტერატურა:

1. შონია ო., შონია ა., ოდიშარია კ., ცომაია ნ. ინფორმაციული უსაფრთხოების უზრუნველყოფის ძირითადი პრინციპები საბანკო სისტემაში. სტუ–ს შრომები. „მართვის ავტომატიზებული სისტემები“, № 2(5) , 2008

2. თევდორაძე მ., გედევანიშვილი მ., გოგოლაძე ს. კორპორაციული ინფორმაციული სისტემების კლასიფიკაცია. სტუ–ს შრომები „მართვის ავტომატიზებული სისტემები“, № 2(5), 2008

3 . Одишария К.М. , Хоштария С.Н. , Эбаноидзе Ж.В. Некоторые направления повышения эффективности обеспечения безопасности аэропорта. Межд.-научный жур. "Воздушный Транспорт", Тбилисию 2008.

ВОЗМОЖНОСТИ ПОВЕШЕНИЯ ИНФОРМАЦИОНИЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ СИСТЕМЫ С ПРИМЕНЕНИЕМ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИИ

Каишаури Т., Одишария К., Гомелаури Д.
Грузинский Техничесский Университет

Резюме

Рассматриваются особенности и перспективы исползивания биометрических характиристик персонала с целью повышения информационной безопасности в банковской системе.

OPPORTUNITIES OF IMPROVING INFORMATIOAL SAFETY SYSTEM OF BANK WITH APPLICATION BIOMETRIC TECHNOLOGIES

Kaishauri Tinatin, Odisharia Korneli, Gomelauri David
Georgian Technical Univercity

Summary

The work represents features and perspectives of application of biometric characteristics by personnel for increasing information security of bank system.