

პერტონ პარკი

დემურ სიმონაძე

საბანკო საინფორმაციო სისტემები

დაგეგმვა სახელმძღვანელო

მეორე გამოცემა



ივანე ჯავახიშვილის სახელობის თბილისის
სახელმწიფო უნივერსიტეტი

მურთაზ მაღრაძე, დემურ სიჭინავა

საბანკო საინფორმაციო სისტემები

დახმარა სახელმძვანელო

მეორე გამოცემა გადაუხავებული



უნივერსიტეტის
გამომცემლობა

დამხმარე სახელმძღვანელოში განხილულია საბანკო სფეროში კომპიუტერული ტექნოლოგიების დანერგვის ეტაპები, საბანკო საინფორმაციო სისტემების ინფორმაციული უზრუნველყოფა, ბანკში გამოყენებული ტექნიკური საშუალებები, ბანკის ავტომატიზებული სამუშაო ადგილების სტრუქტურა და მათი კავშირი ბანკის საინფორმაციო სისტემასთან, პლასტიკური ბარათები, ელექტრონული ფული, კრიპტოვალუტის მაინინგი, ბლოკჩეინის ტექნოლოგია, ბიტკოინის ფასზე მოქმედი ფაქტორები, კრიპტოვალუტა ბიტკოინის ეკოსისტემა, კრიპტოვალუტის რეგულირება მსოფლიოში და საქართველოში, საერთაშორისო საფინანსო ტელესაკომუნიკაციო სისტემა, ბანკის საინფორმაციო სისტემების შეძენისა და ამორჩევის კრიტერიუმები, შექმნის ხერხები და საბანკო საინფორმაციო სისტემების უსაფრთხოების უზრუნველყოფა.

დამხმარე სახელმძღვანელო განკუთვნილია ეკონომიკისა და ბიზნესის ფაკულტეტის ინფორმაციული ტექნოლოგიების მენეჯმენტის მოდულის მაგისტრატურის სტუდენტებისათვის.

რედაქტორი: ლეილა ლუდუშაური, თსუ ასოცირებული პროფესორი
რეცენზენტები: მიხეილ ჩიკვილაძე, თსუ ასოცირებული პროფესორი
მზია ტიკიშვილი, თსუ ასისტენტ პროფესორი

ნიგნი ელექტრონულად გამოცემულია ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის საუნივერსიტეტო საგამომცემლო საბჭოს გადაწყვეტილებით.

© ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის საგამომცემლობა, 2026

ISBN 978-9941-36-528-7 (pdf)

სარჩევი

წინასიტყვაობა	7
თავი 1. ბანკის ინფორმაციული ტექნოლოგიები	10
1.1. საბანკო სფეროში კომპიუტერული ტექნოლოგიების დანერგვის ეტაპები	10
1.2. საბანკო სისტემების ფუნქციური ამოცანები და მოდულები	12
1.3. ბანკის საქმიანობის ინფორმატიზაციის პრინციპები.....	17
1.4. საინფორმაციო სისტემებისადმი წაყენებული მოთხოვნები.....	19
თავი. 2. საბანკო საინფორმაციო სისტემების ინფორმაციული უზრუნველყოფა	22
2.1. ინფორმაციული მოდელი	22
2.2. დაკრედიტების ამოცანის ავტომატიზებული გადაწყვეტის ორგანიზება	26
თავი 3. საბანკო ელექტრონული სისტემების ტექნიკური საშუალებები.....	41
3.1. ბანკში გამოყენებული ავტომატიზებული საინფორმაციო სისტემები	41
3.2. კომპიუტერის მუშაობის რეჟიმები	42
3.3. ტელესაკომუნიკაციო სისტემები.....	48
3.4. ბანკომატი, როგორც ელექტრონული გადახდების სისტემის ელემენტი.....	51
3.5. ნაღდ ფულთან მომუშავე სხვა მოწყობილობები	57
თავი 4. ბანკის ავტომატიზებული სამუშაო ადგილების სტრუქტურა და მათი კავშირი ბანკის საინფორმაციო სისტემასთან.....	62
4.1. ბანკის ავტომატიზებული სამუშაო ადგილების სტრუქტურა.....	62

თავი 5. პლასტიკური ბარათები.....	69
5.1. პლასტიკური ბარათების ისტორია	69
5.2. პლასტიკური ბარათების კლასიფიკაცია და სახეები.....	71
5.3. საქართველოს ბანკებში გამოყენებული პლასტიკური ბარათები.....	76

თავი 6. გადახდის სისტემები. საქონლის მიწოდებისა და გადახდის სახეები.....	85
6.1. საქონლის ტრანსპორტირებისა და გადახდის ხერხები	85
6.2. ანაზღაურება ნაღდი ფულით. ინტერნეტში ანაზღაურების ხერხები.	86
6.3. ანაზღაურება წინასწარ ანაზღაურების ბარათებით (სკრეტი-ბარათები)	86
6.4. ინტერნეტგადახდის სისტემა.....	89
6.5. ინტერნეტგადახდის სისტემები: სადებეტო სქემები	90
6.6. კლიენტის კომპიუტერის „ელექტრონულ საფულეზე“ მომუშავე სისტემები.....	90
6.7. სმარტ-ბარათებზე მომუშავე სისტემები	91
6.8. უნივერსალური ელექტრონული ბარათები	92

თავი 7. ელექტრონული ფული.....	95
7.1. ციფრული ფულის ცნება და ინტერნეტში ციფრული ფულით გადახდები	95
7.2. ჩეკებით ანგარიშსწორება	100
7.3. ვირტუალურ ანგარიშებზე დაფუძნებული საგადასახდელი ინტერნეტსისტემები	101
7.4. ინტერნეტბანკინგი.....	103
7.5. ანაზღაურება მობილური ტელეფონის ანგარიშიდან	106
7.6. რეალური დროის რეჟიმში მომუშავე გზავნილების საზღვარგარეთული ეროვნული სისტემები	107

თემა 8. კრიპტოვალუტა.....	119
8.1. კრიპტოვალუტის მაინინგი	119

8.2. ბლოკჩეინტექნოლოგია, კრიპტოვალუტა	
დაციფრული ვალუტა	126
8.3. ბიტკოინის ფასზე მოქმედი ფაქტორები	142
8.4. კრიპტოვალუტა ბიტკოინის ეკოსისტემა	150
8.5. კრიპტოვალუტის რეგულირება მსოფლიოსა და საქართველოში	155
თავი 9. საერთაშორისო საფინანსო ტელესაკომუნიკაციო სისტემა S.W.I.F.T.	165
9.1. S.W.I.F.T.-ის შექმნის ისტორია	165
9.2. დაცვის მექანიზმი S.W.I.F.T.-ში	171
9.3. S.W.I.F.T.-ის სტანდარტი	174
თავი 10. ბანკის საინფორმაციო სისტემების შექმნისა და ამორჩევის კრიტერიუმები	182
10.1. საინფორმაციო სისტემების ფლობის მთლიანი ღირებულება	182
10.2. ინფორმატიზაციის პროექტების რეალიზაციის ვარიანტების საერთო ანალიზი	183
10.3. გარე მომწოდებლისგან საინფორმაციო სისტემის შექმნის ფლობის მთლიანი ღირებულების მოდელი	185
10.4. ფლობის მთლიანი ღირებულების საფუძველზე საკუთარი ძალებით საინფორმაციო სისტემის შექმნის მოდელი	188
10.5. საინფორმაციო სისტემების შექმნის ვარიანტების შედარება	192
10.6 ტენდერის ჩატარება	199
თავი 11. საბანკო საინფორმაციო სისტემის თაობების განვითარება და შექმნის ხერხები	205
11.1. საბანკო საინფორმაციო სისტემის თაობების განვითარება	205
11.2. საბანკო საინფორმაციო სისტემის შექმნის ხერხები	209

თავი 12. საბანკო საინფორმაციო სისტემების	
შემმუშავებელი კომპანიების დახასიათება	216
12.1. ავტომატიზებული საბანკო საინფორმაციო	
სისტემის სტრუქტურა	216
12.2. საბანკო საინფორმაციო სისტემების	
შემმუშავებელი კომპანიების დახასიათება	217
 თავი 13. საბანკო საინფორმაციო სისტემების	
უსაფრთხოების უზრუნველყოფა.....	228
13.1. საზოგადოების ახალი საფრთხეები	228
13.2. კომპიუტერული დანაშაულებების კლასიფიკაცია	239
13.3. კომპიუტერული დანაშაულებებისა და	
ინფორმატიზაციის უარყოფითი შედეგების	
აღმოფხვრის ღონისძიებები და საშუალებები	256
13.4. კომპიუტერთან ხანგძლივი მუშაობით	
გამონვეული შესაძლო დაავადებები	263
13.5. კრიპტოგრაფია.....	266
13.6. ინფორმაციის დაცვის ბიომეტრიული სისტემები.....	272
13.7. ინფორმაცია როგორც სამართლებლივი	
რეგულირების სფერო	273
13.8. საბანკო საინფორმაციო სისტემების	
უსაფრთხოება	275
დასკვნა.....	289
ქართულ-ინგლისური აბრევიატურა.....	290
გამოყენებული ლიტერატურა	291

წინასიტყვაობა

საბაზრო ეკონომიკის პირობებში საბანკო ტექნოლოგიების ავტომატიზაციას საფუძველი ჩაეყარა გასული საუკუნის 90-იანი წლების დასაწყისში, როცა ქვეყანაში აღმოცენდნენ კომერციული ბანკები. ინფორმაციული ტექნოლოგიების ბაზარზე, კერძოდ კი, პროგრამული პროდუქტების ბაზარზე, ყოფილ საბჭო კავშირში ფუნქციონირებას იწყებენ საბანკო საინფორმაციო სისტემების პროგრამული უზრუნველყოფის შემმუშავებელი ფირმები „R-Style Soft-lab“, „Асофт“, „Програм-Банк“, „Диасофт“ და სხვ.

ვინაიდან ამ მომენტისთვის შესრულებული ფუნქციების, სიდიდის და საბანკო საქმიანობის მიხედვით მრავალი ბანკი ფუნქციონირებდა, საჭირო გახდა თითოეულისთვის შესაბამისი საინფორმაციო სისტემის შემუშავება.

მიუხედავად იმისა, რომ ქვეყნის ეკონომიკური განვითარების მაჩვენებლები მცირდებოდა, საბანკო სისტემა სწრაფი ტემპით ვითარდებოდა, ბანკები სულ უფრო მაღალ მოგებას ღებულობდნენ. ფიზიკურ პირებს აღარ შეეძლოთ სწრაფი ტემპით მიმდინარე ინფლაციასთან გამკლავება, ამიტომ იძულებული იყვნენ, თავიანთი დანაზოგები შეეტანათ ბანკში. ბანკები უზარმაზარ მოგებას ღებულობდნენ მოსახლეობის მიერ ქვეყნის ვალუტის დოლარზე გაცვლის შედეგად.

კონკურენციის გაძლიერებამ, ბანკის ფულადი საშუალებებისა და მოკლევადიანი კრედიტების შემცირებამ ბანკები აიძულა, მოგების მიღების ექსტენსიური ხერხებიდან გადასულიყვნენ მოგების მიღების ინტენსიურ მეთოდებზე. საბანკო სისტემაში აქტიურად იწყება ახალი მომსახურებების დანერგვა: საფონდო და საბარათო, იპოთეკური, სავაჭრო, საინვესტიციო, მოქალაქეების ანაბრების აღრიცხვის ოპერაციები და ა. შ.

ბანკში შესრულებული ოპერაციების ერთგვარობა ბანკებს საშუალებას აძლევს, უარი თქვან ბანკის საქმიანობის ავტომატიზაციის არსებულ სისტემებზე და ფართოდ დანერგონ მსოფლიოს მოწინავე ბანკებში არსებული თანამედროვე ინფორმაციული ტექნოლოგიები, კონკურენტუნარიანი საინფორმაციო სისტემები.

ვინაიდან ბანკების ფინანსური შესაძლებლობები გაცილებით დიდია, ვიდრე წარმოება-დანესებულებების, თანამედროვე ინფორმაციული ტექნოლოგიების აპრობაცია და დანერგვა, პირველ რიგში, წარმოებს ბანკებში და შემდეგ ხდება ამ გამოცდილების გაზიარება.

ბანკის ინტეგრირებული საინფორმაციო სისტემის საფუძველია ერთიანი ინფორმაციული სივრცის ფორმირება.

იმისთვის, რომ ბანკებმა გაიმარჯვონ კონკურენციულ ბრძოლაში, მათ აუცილებლად უნდა შეამცირონ მომსახურების თვითღირებულება, გააფართოონ კლიენტისთვის მიწოდებული პროდუქტების რაოდენობა და ხარისხი. აღნიშნულის მიღწევა შესაძლებელი გახდება, თუ ბანკები ტელესაკომუნიკაციო საშუალებების გამოყენებით უზრუნველყოფენ:

- ანგარიშსწორებას პლასტიკური ბარათებით;
- „კლიენტიბანკის“ ურთიერთობის ორგანიზებას;
- ბანკთაშორის ურთიერთობების ავტომატიზაციას;
- სისტემა S.W.I.F.T-ის მეშვეობით კლიენტებს შორის საერთაშორისო ურთიერთობების დამყარებას;
- ეფექტური, საიმედო და უსაფრთხო ელექტრონული საგადამხდელო სისტემის ორგანიზებას.

ავტომატიზაცია ბანკის თვითმზანი კი არა, წარმატების მიღწევის ინსტრუმენტია.

ბანკის თანამშრომლები, რომლებიც უშუალოდ ბანკის ინფორმაციას ამუშავებენ, ბანკის კლიენტები (ფიზიკური და ურთიერთობის პირები) გარკვეული ზომით უნდა ფლობდნენ ბანკის საინფორმაციო სისტემით სარგებლობის უნარ-ჩვევებს. წინააღმდეგ შემთხვევაში, ერთი მხრივ, შეუძლებელი იქნება საბანკო საინფორმაციო სისტემების ეფექტიანი ფუნქციონირება და, მეორე მხრივ, შეუძლებელი გახდება, ფართო მასებმა ისარგებლონ ბანკების მიერ დანერგილი თანამედროვე ინფორმაციული ტექნოლოგიებით (პროდუქტებით). ეს უკანასკნელი საბოლოოდ გამოიწვევს საბანკო სისტემაში კონკურენტიანი, თანამედროვე მოთხოვნების შესაბამისი ინფორმაციული ტექნოლოგიების დანერგვის შეფერხებას.

„საბანკო საინფორმაციო სისტემები“ განკუთვნილია ინფორმაციული ტექნოლოგიების მენეჯმენტის მაგისტრანტებისთვის, რომლებიც სწავლობენ სასწავლო კურსს „**საბანკო საინფორმაციო სისტემები**“. პროფესიის სრულყოფილად დაუფლებისთვის, წიგნი ასევე გამოადგებათ ფინანსებისა და საბანკო საქმის მოდულის სტუდენტებს, ბანკში მომუშავე პერსონალს.

დამხმარე სახელმძღვანელო მომზადებულია საბანკო საინფორმაციო სისტემების კურსის შესასწავლად აკრედიტებული სილაბუსის მიხედვით და შედგება შემდეგი თემებისაგან: ბანკის ინფორმაციული ტექნოლოგიები; საბანკო საინფორმაციო სისტემების ინფორმაციული უზრუნველყოფა; საბანკო ელექტრონული სისტემების ტექნიკური საშუალებები; ბანკის ავტომატიზებული სამუშაო ადგილების სტრუქტურა და მათი კავშირი ბანკის საინფორმაციო სისტემასთან; პლასტიკური ბარათები; გადახდის სისტემები; საქონლის მიწოდებისა და გადახდის სახეები; ელექტრონული ფული; კრიპტოვალუტა, საერთაშორისო საფინანსო ტელესაკომუნიკაციო სისტემა **S.W.I.F.T.**; ბანკის საინფორმაციო სისტემების შეძენისა და ამორჩევის კრიტერიუმები; საბანკო საინფორმაციო სისტემის თაობების განვითარება და შექმნის ხერხები; საბანკო საინფორმაციო სისტემების შემმუშავებელი კომპანიების დახასიათება; საბანკო საინფორმაციო სისტემების უსაფრთხოების უზრუნველყოფა.

შემოთავაზებული დამხმარე სახელმძღვანელო მნიშვნელოვნად დაეხმარება მკითხველს საბანკო ინფორმაციული ტექნოლოგიების პრობლემების გაგებასა და მათ გადაწყვეტაში.

თავი 1. ბანკის ინფორმაციული ტექნოლოგიები

1.1. საბანკო სფეროში კომპიუტერული ტექნოლოგიების დანერგვის ეტაპები

მართალია, საბანკო საქმიანობამ დასაწყისიდან დღემდე, რამდენიმე ეტაპი (ი. კოვზანაძე, გ. კონტრიძე, გვ. 15) [1] განვლო, თუმცა საბანკო სფეროში კომპიუტერების გამოყენება დაიწყო აშშ-ში 1950 წლიდან.

ადამიანის საქმიანობათა შორის საბანკო სფერო არის ერთ-ერთი, სადაც კომპიუტერული ტექნოლოგიების დანერგვა ყველაზე ეფექტურია. პირველად საბანკო სფეროში კომპიუტერები გამოყენებულ იქნა აშშ-ში 1950 წელს. 1959 წელს აშშ-ის ერთ-ერთ წამყვან ბანკში „Bank of America“ პირველად დაინერგა ჩეკებისა და მიმდინარე ანგარიშების ავტომატიზებული დამუშავების სისტემა. თუმცა საბანკო მომსახურების ავტომატიზაციის პირველი ცდები არ იყო წარმატებული იმიტომ, რომ ვერ გაამართლა მიდგომამ **ფასი/მწარმოებლურობა**, ანუ შექმნილმა საინფორმაციო სისტემებმა ვერ შეძლეს საკუთარი თავის გამოსყიდვა. ბანკში კომპიუტერების გამოყენებაში ცვლილებები მოხდა გასული საუკუნის 80-იან წლებში, რაც დაკავშირებული იყო ინფორმაციის დამუშავების საშუალებების სრულყოფასთან. შეიქმნა მიკროპროცესორებზე აგებული კომპიუტერები. მესამე თაობის დიდ ელექტრონულ გამომთვლელ მანქანებთან შედარებით მათი ღირებულება იყო დაბალი, მწარმოებლურობა კი – მაღალი. შესაძლებელი გახდა სპეციალისტის სამუშაო ადგილის აღჭურვა პერსონალური კომპიუტერით. შეიცვალა პროგრამული უზრუნველყოფისადმი მიდგომა. იგი გახდა მეგობრული მომხმარებლის მიმართ, რაც გამოიხატებოდა იმაში, რომ მომხმარებელს შეეძლო ამოცანების გადაწყვეტა ინფორმატიკის ცოდნის გარეშეც.

საბანკო საქმიანობაში კომპიუტერების გამოყენების აუცილებლობის საკითხი დადგა მაშინ, როდესაც დასამუშავებელი ჩეკების რაოდენობამ მიაღწია რამდენიმე ათეულ მილიარდს. მაგ., აშშ-ში 1986-1995 წლებში დასამუშავებელი ჩეკების რაოდენობა 47 მილიარდიდან 75 მილიარდამდე გაიზარდა. კატასტრო-

ფულად იზრდებოდა ჩეკების მომსახურების ხარჯები. შეიქმნა სიძნელეები საბანკო საქმიანობის ოპერატიულ მომსახურებაში. აუცილებელი გახდა მომსახურე პერსონალის რაოდენობის გაზრდა. დაისვა საკითხი ელექტრონული ფულის გამოყენების აუცილებლობის, დაგეგმვისა და სხვა ტექნიკური მოწყობილობების სრულყოფის თაობაზე. აშშ-ის ბანკების მიერ განეული დანახარჯების ნახევარზე მეტი მოდიოდა კომპიუტერებისა და სხვა ტექნიკური საშუალებების შეძენაზე.

საბანკო საქმიანობის კომპიუტერიზაციას უნდა შეემცირებინა კლიენტების მომსახურების ხარჯები და გაეუმჯობესებინა მომსახურების ხარისხი. ბანკში განეული დანახარჯებიდან ყველაზე მეტი მოდიოდა ბანკის თანამშრომლების შენახვასა და საგადამხდელო დოკუმენტების დამუშავებაზე, წვრილი მენაბრეების მომსახურებაზე. საბანკო საქმიანობის ავტომატიზაციას უნდა შეემცირებინა შტატების რაოდენობა და დანახარჯები შენობებისა და ნაგებობების იჯარაზე.

საგადამხდელო დოკუმენტების დამუშავებაზე განეული დანახარჯების შესამცირებლად ბანკებში დაიწყო კლიენტების მომსახურების ისეთი ახალი ტექნოლოგიების დანერგვა და გამოყენება, როგორიცაა:

- პლასტიკური ბარათების გამოყენებით უნაღდო ანგარიშსწორების განხორციელება;
- კლიენტების თვითმომსახურების მოწყობილობების გამოყენება. ძირითადად, ბანკომატების საშუალებით ნაღდი ფულის გაცემა;
- სავაჭრო ნერთილებში ელექტრონული ანგარიშსწორების სისტემების დანერგვა, რამაც მნიშვნელოვნად შეამცირა ნაღდი ფულის მოცულობის ბრუნვა;
- კლიენტების მომსახურება სახლიდან და ოფისებიდან გაუსვლელად (კლიენტს სახლიდან და ოფისიდან პერსონალური კომპიუტერისა და ქსელის საშუალებით შეუძლია საბანკო ოპერაციების შესრულება).

ტექნიკურმა პროგრესმა შესაძლებელი გახადა, კლიენტი დისტანციურად დაეკავშირებინა ბანკთან, რათა მას შეესრულებ-

ბინა სხვადასხვა საბანკო ოპერაციები. ამასთან, კლიენტს საშუალება მიეცა, ბანკის გეოგრაფიული მდებარეობის მიუხედავად აერჩია სასურველი ბანკი. აღნიშნული ტექნოლოგია მისაღები და ხელსაყრელი იყო ბანკისთვისაც, რადგან ბანკს შეეძლო შეემცირებინა ხელფასისა და კაპიტალურ მშენებლობის დანახარჯები. თუმცა, ახალი ინფორმაციული ტექნოლოგიები ბანკს უქმნიდა ისეთ პრობლემებს როგორცაა:

- უსაფრთხოებისა და კონფიდენციალურობის უზრუნველყოფა;
- კომპიუტერული ტექნოლოგიების დანერგვის საწყის ეტაპზე დიდი მოცულობის დანახარჯების გაღების აუცილებლობა და სხვ.

1.2. საინფორმაციო საბანკო სისტემების ფუნქციური ამოცანები და მოდულები

ავტომატიზებული საბანკო სისტემების ფუნქციების გაფართოება დაკავშირებულია ქვეყანაში საბანკო საქმიანობის განვითარების თავისებურებებზე. თუ იზრდება ბანკის სხვადასხვა მომსახურებაზე მოთხოვნა, მაშინ ავტომატიზებული საბანკო სისტემების ბაზარზე ჩნდება ახალი საბანკო დანართები, საბანკო ტექნოლოგიების ახალი სახეები.

ავტომატიზებული საბანკო სისტემის საბაზო კომპლექტი საშუალებას იძლევა, ფართო სპექტრით მოემსახუროს კლიენტებს.

სისტემის ძირითად ფუნქციურ მოდულებს შეუძლიათ შემდეგი ამოცანების რეალიზაცია:

- იურიდიული პირების საანგარიშსწორებო საკასო მომსახურება;
- ბანკ-კორესპონდენტის ანგარიშების მომსახურება;
- საკრედიტო, სადეპოზიტო და სავალუტო მომსახურება;
- კერძო პირების ნებისმიერი ანაბრის და მათზე შესრულებული ოპერაციების მომსახურება;
- საფონდო ოპერაციები;

- ანგარიშსწორება პლასტიკური ბარათების გამოყენებით;
- საბუღალტრო აღრიცხვის ფუნქციების რეალიზაცია;
- ანალიზი, გადანყვეტილების მიღება, მენეჯმენტი, მარკეტინგი და ა. შ.

მეოთხე თაობის ავტომატიზებული საბანკო საინფორმაციო სისტემები დაფუძნებულია „კლიენტ-სერვერულ“ ტექნოლოგიაზე და იყენებს აგებისა და ფუნქციონირების ერთიან პრინციპებს.

უკანასკნელ პერიოდში დიდ ყურადღებას უთმობენ ფინანსური ანალიზის და ბიზნესის მართვის საკითხებს. ჯერჯერობით სათანადო დონეზე არ არის: ფინანსური რისკების კონტროლის სისტემები, რესურსების მართვა, ოპერაციების მომგებიანობის ანალიზი.

განვიხილოთ ფორმა „**Инверсия**“-ს მიერ შემუშავებული ავტომატიზებული საბანკო საინფორმაციო სისტემის ძირითადი ქვესისტემები: ბანკის ოპერაციული დღე, როგორც პროგრამულ-ტექნოლოგიური კომპლექსი, უზრუნველყოფს შრომატევადი საბანკო ოპერაციების აღრიცხვის ავტომატიზაციას; კლიენტების პირად ანგარიშებთან დაკავშირებული ყველა ოპერაცია სრულდება საგადამხდელო დოკუმენტების მიხედვით; სისტემა ახორციელებს ფულადი საშუალებების ფაქტობრივ და გეგმიურ მოძრაობის რეალიზაციას.

პირადი ანგარიშების მიხედვით დოკუმენტები გადიან კონტროლს და შეცდომების არარსებობის შემთხვევაში დგება ამ დოკუმენტების ჩამონათვალი. ფორმირდება საანგარიშო-სათავო ცენტრში გასაგზავნი ფაილი. სალაროს დოკუმენტების მოძრაობას გააჩნია თავისებურებები, რომელთა შორის მთავარს წარმოადგენს ბანკის სხვა სამსახურებთან კავშირი.

„**ბანკის ოპერაციული დღე**“. კომპლექსს გააჩნია მულტივალუტური თვისება. ფილიალების საქმიანობის აღრიცხვის კომპლექსის დანიშნულებაა ბუღალტერიაში სამუშაო ადგილებისა და ფილიალების სხვა განყოფილებების სამუშაოების ავტომატიზაცია. „ბანკ-ფილიალების“ დონეზე ავტომატიზაცია ხდება ფილიალებიდან შემოსული ინფორმაციის შეგროვების, დამუშავე-

ბის და ანალიზის საფუძველზე. ფილიალთა შორის ურთიერთობის ორგანიზება წარმოებს პირდაპირ ცენტრალური ბანკის განყოფილების მეშვეობით. ფილიალების ფარგლებში კომპლექსი მოიცავს სავალუტო და სალაროს ოპერაციებს. ფილიალების მიხედვით წარმოებს ბალანსის გაანგარიშება.

ხელშეკრულებების ქვესისტემა მუშაობს საკრედიტო, სადეპოზიტო და ბანკთაშორის ოპერაციებზე, ახორციელებს სავალუტო დილინგს. ხელშეკრულების ჟურნალში აისახება მონაცემები მიმდინარე, დამთავრებული, ვადაგადაცილებული და იმ ხელშეკრულებების შესახებ, რომელთა გადახდის ვადაც დადგა.

ფირმა „ინვერსიის“ პროგრამულ-ტექნიკური კომპლექსი „ფირმის დეპოზიტები“ უზრუნველყოფს ისეთი ფუნქციების რეალიზაციას როგორცაა:

- კლიენტების სიების ფორმირება და მათი ტიპის განსაზღვრა (ინვესტორი, დილერი, ემიტენტი, დეპოზიტორი, საცავი);
- დეპოზიტარების, საბალანსო ანგარიშებისა და ანგარიშგებების ფორმირება;
- ფასიანი ქაღალდების გამოშვება;
- ფასიან ქაღალდებზე ოპერაციების (მიღება, აღრიცხვიდან მოხსნა, მფლობელისა და შენახვის ადგილის ცვლილების ასახვა. დეპო ანგარიშის მიხედვით ამონაწერის მიღება) შესრულება;
- ოპერაციების კატალოგის წარმოება და ფასიანი ქაღალდების განთავსება;
- კრებსითი ანგარიშგებების მომზადება.

ფირმა „ინვერსიის“ მიერ შემუშავებული პროგრამულ-ტექნოლოგიური კომპლექსი „საბირჟო ოპერაციები“ ახდენს:

- ვალუტის ყიდვა-გაყიდვის შესახებ კონტრაქტების ავტომატიზაციას;
- განაცხადების რეგისტრაციის ავტომატიზაციას;
- სავალუტო გადახდებისა და მაჩვენებლების კონტროლსა და ანალიზს;
- ვალუტით ვაჭრობის სტატისტიკას;

- ანგარიშგებითი ფორმების გენერაციას.

კომპლექსი „ოპერაციები სახელმწიფო მოკლევადიანი ობიგაციების ბაზარზე“ უზრუნველყოფს შემდეგი ფუნქციების რეალიზებას:

- ბანკი დილერისათვის, კლიენტებისათვის და ფილიალებისათვის ანგარიშდებოს შექმნას;
- ფასიანი ქაღალდების ყიდვა-გაყიდვის ოპერაციების აღრიცხვას. ოპერაციების მიხედვით საკომისიოსა და გადასახადების აღრიცხვას;
- ვაჭრობის შედეგების მიხედვით ფასიანი ქაღალდების პორტფელის გადაფასებას;
- ბანკისა და მისი კლიენტების შემოსავლების გაანგარიშებას;
- გატარებებისა და ოპერაციების ჟურნალის ფორმირებას, ანგარიშების მიხედვით ამონაწერების გაკეთებას;
- სხვადასხვა მაჩვენებლების მიხედვით ფასიანი ქაღალდების შემოსავლიანობის ანალიზს.

ავტომატიზებული საბანკო საინფორმაციო სისტემის ყველაზე გავრცელებული ქვესისტემებია:

- კლიენტი-ბანკი;
- მუშაობა პლასტიკურ ბარათებთან;
- ვალუტის გაცვლის პუნქტების ოპერაციები.

ფირმა „ინვერსიის“ მიერ შემუშავებული „კლიენტი-ბანკის“ პროგრამულ-ტექნოლოგიური კომპლექსი შედგება შემდეგი მოდულებისაგან: „ბანკი“ და „კლიენტი“, რომელთა დაყენება წარმოებს ბანკისა და კლიენტის პერსონალურ კომპიუტერზე, რაც კლიენტს შესაძლებლობას აძლევს, თავისი სამუშაო ადგილიდან (ოფისიდან) განახორციელოს სტანდარტული საბანკო ოპერაციები. კომპლექსი ასრულებს საგადამხდელო დოკუმენტების გაგზავნისა და მიღების ფუნქციებს, ანგარიშების მიხედვით ამონაწერის მიღებას, ვალუტის ყიდვა-გაყიდვაზე შეკვეთებს, ოპერაციებს ფასიან ქაღალდებზე.

კლიენტების მომსახურების ეფექტური ფორმაა პლასტიკური ბარათების გამოყენება.

საბანკო მომსახურების შემადგენელი ნაწილია ბანკომატები (ავტომატ-მოლარეები). მათი დამონტაჟება წარმოებს ორგანიზაციებში.

ბანკში საინფორმაციო სისტემის ქვესისტემების გამოყოფა ძირითადად ხდება ბანკში შესასრულებელი ფუნქციების მიხედვით, ბანკის ორგანიზაციულ-ფუნქციური სტრუქტურის მიხედვით. ქვემოთ მოვიყვანოთ იმ ქვესისტემების ჩამონათვალი, რომელიც შეიძლება გააჩნდეს ბანკს:

- საბუღალტრო აღრიცხვის ქვესისტემა;
- ბანკის კლიენტების ანგარიშების წარმოების ქვესისტემა – **Reitail**-ოპერაციები (მიმდინარე ანგარიშები, სწრაფი ანაბრები, საცალო მომსახურებები);
- ბანკის ბარათებთან მუშაობის ქვესისტემა;
- დაკრედიტების ქვესისტემა;
- დეპოზიტების ქვესისტემა;
- ვალუტის გაცვლის ოპერაციების ქვესისტემა;
- ფასიან ქაღალდებთან მუშაობის ქვესისტემა;
- ინკასოს ოპერაციების ქვესისტემა;
- ბანკთაშორისი ურთიერთობების ქვესისტემა;
- რესურსების მართვის ქვესისტემა (დილინგი);
- უსაფრთხოების უზრუნველყოფის ქვესისტემა;
- გაანგარიშების გენერაციის, ბანკის საქმიანობის დაგეგმვისა და ანალიზის ქვესისტემა;
- დისტანციური მომსახურების ქვესისტემა;
- ბანკის, როგორც ეკონომიკური სუბიექტის, შიგა საქმიანობის უზრუნველყოფის ქვესისტემა.

1.3. ბანკის საქმიანობის ინფორმატიზაციის პრინციპები

დღეისათვის ბანკის წარმატებული მუშაობა შეუძლებელია მისი საქმიანობის ინფორმატიზაციის გარეშე. საინფორმაციო სისტემებმა ბანკს უნდა მისცეს საბანკო სისტემის განვითარების, გაფართოებისა და წარმატებების მიღწევის საშუალება. ბანკს საინფორმაციო სისტემების გამოყენების საფუძველზე შეუძლია კლიენტებთან მუშაობის გაუმჯობესება, ბაზრის გამოკვლევა, ფინანსების მართვა და უფრო მომგებიანი მომსახურების დანერგვა. ბანკების მუშაობის პრაქტიკამ აჩვენა, რომ ხშირ შემთხვევაში ბანკების ინფორმატიზაცია მიმდინარეობს სტიქიურად. ადგილი აქვს ბანკის ზოგიერთი ფუნქციის ავტომატიზაციას, რაც არსებით შედეგს არ იძლევა. აუცილებელი ხდება ბანკის ავტომატიზაციის სტრატეგიის შემუშავება. დასაწყისში უნდა განისაზღვროს, რომელი ფუნქციებისა და ამოცანების გადაწყვეტა უნდა განხორციელდეს კომპიუტერების დახმარებით და ავტომატიზაციის რომელი კონკრეტული საშუალებები უნდა იქნეს გამოყენებული. საწყის ეტაპზე დაშვებულმა შეცდომებმა ბანკს შეიძლება მიაყენოს დიდი ზარალი. ამ შემთხვევაში ცუდი შედეგი მოაქვს ტექნიკურ საშუალებებზე, მათი პროგრამული უზრუნველყოფის შეძენასა და დანერგვაზე დასაქმებულ პერსონალის შენახვაზე გაწეულ დანახარჯებს.

ბანკის საქმიანობის საინფორმაციო სისტემების შერჩევისა და დანერგვისას გასათვალისწინებელია შემდეგი პრინციპები [2]:

შეთანხმებულობის პრინციპი. ამ პრინციპის გათვალისწინება უზრუნველყოფს ინფორმატიზაციის ისეთი სახით განხორციელებას, რომ სისტემის ნაწილობრივი ცოდნა საშუალებას მოგვცემს სისტემა წარმოვიდგინოთ მთლიანობაში;

ორთოგონალობისა და შესაბამისობის პრინციპი მოითხოვს, რომ სისტემაში ჩართული იქნეს მხოლოდ ის ფუნქციები, რომელთა ავტომატიზაცია აუცილებელია და რომლებიც შეესაბამებოდნენ სისტემის არსებით მოთხოვნებს.

ეკონომიურობისა და სისრულის პრინციპი ნიშნავს, რომ სისტემაში ადგილი არ უნდა ჰქონდეს ფუნქციების დუბლირებას, თუ-

მცა სისტემაში ჩართულმა ფუნქციებმა ტექნიკური და ეკონომიკური შეზღუდვების გათვალისწინებით სრულყოფილად უნდა დააკმაყოფილოს მომხმარებლის სურვილები და საჭიროებები.

გახსნილობის პრინციპი. პროგრამული კომპლექსების შემუშავებისა და ექსპლუატაციის მსოფლიო პრაქტიკამ აჩვენა, რომ სისტემების შემუშავებისას აუცილებელია რიგი შეთანხმებების დაცვა. ასეთი შეთანხმებები შემუშავებულია. ისეთ სისტემებს, რომელშიც ეს შეთანხმებები სრულდება, ღია სისტემები ეწოდება. ღია სისტემების სტანდარტების გამოყენება საშუალებას იძლევა, შემცირდეს სისტემების ექსპლუატაციისა და მოდერნიზაციის ხარჯები. სისტემების გახსნილობა ნიშნავს, რომ შესაძლებელია სისტემის გაფართოება არსებული ძირითადი გადაკეთების გარეშე. ეს შეთანხმებები მდგომარეობს შემდეგში:

- ფაქტობრივად მოქმედი სტანდარტების საერთაშორისო და სახელმწიფო სტანდარტებთან შესაბამისობა;

- სხვა სისტემებთან თავსებადობა;

- მუშა პროგრამული პროდუქტის მინიმალური დანახარჯებით სხვა ტექნიკურ და ოპერაციულ გარემოში (პლატფორმაზე) გადატანა;

- მასშტაბურობა, უფრო ძლიერი ტექნიკური საშუალებების გამოყენებით, არსებითი გადაკეთების გარეშე, სისტემის მწარმოებლურობის ამაღლება.

ტექნიკური გადანაცვებების ამორჩევისას ამ წესებს უნდა შეესაბამებოდეს:

- მომხმარებლის პროგრამული დანართები;

- მომხმარებლის გრაფიკული ინტერფეისი;

- სისტემის შემუშავების საშუალებები;

- ოპერაციების შესრულება (ტრანზაქცია);

- მუშაობა ქსელებში;

- სხვა მონაცემთა ბაზებთან ერთობლივი მუშაობა;

- გამოყენებული ოპერაციული სისტემები;

- გამოყენებული ტექნიკური პლატფორმები.

- სისტემის ცალკეული ნაწილის გამტარუნარიანობა.

ღია სისტემებისათვის ჩამოთვლილი მოთხოვნები გვიჩვენებენ, რომ ღია სისტემის შეძენა და შემუშავება უნდა მოხდეს შესაბამისი სტანდარტების, ტექნოლოგიებისა და მისი განვითარების პროგნოზის გათვალისწინებით.

1.4. საინფორმაციო სისტემებისადმი წაყენებული მოთხოვნები

თავიდან, საბანკო საინფორმაციო სისტემებისადმი წაყენებული მოთხოვნების განხილვამდე, საჭიროა განვსაზღვროთ, ვინ ისარგებლებს ამ სისტემით, ვის მოუტანს იგი სარგებელს, რა სახის ინფორმაციის დამუშავება უნდა მოხდეს სისტემაში. მაგ., თუ საინფორმაციო სისტემამ უნდა დააკმაყოფილოს ბიბლიოთეკაში მკითხველის მომსახურება, მაშინ მისთვის წაყენებული მოთხოვნები განსხვავებული იქნება იმ მოთხოვნებისაგან, რომელიც წაყენება თვითმფრინავზე ბილეთების ავტომატიზებული გაყიდვის სისტემას. აღნიშნულიდან გამომდინარე, უნდა გაანალიზდეს საბანკო საინფორმაციო სისტემა, გამომდინარე იქიდან, რომ ამ სისტემის მომხმარებელი იქნება ბანკის თანამშრომელი, რომელსაც გამოთვლითი ტექნიკისა და ინფორმატიკის სფეროში არ გააჩნია სპეციალური პროფესიული განათლება. ასეთი თანამშრომლისთვის კომპიუტერი ძირითადი სამუშაოების შესრულებისას დამხმარე ინსტრუმენტია. ამიტომ ერთ-ერთი მოთხოვნა, რომელიც წაყენება ბანკის საინფორმაციო სისტემას, არის სისტემის დაცულობა მომხმარებლის არაკორექტული მოქმედებისაგან. ამ შემთხვევაში არაკორექტულ მოქმედებში იგულისხმება სისტემის მომხმარებლის მხრიდან პროგრამულ და აპარატურულ საშუალებებზე არასწორი მოქმედება, კომპიუტერის ჩართვის ან გამორთვის ღილაკზე შეცდომით თითის დაჭერა. ასეთ სისტემებს უნდა გააჩნდეს მომხმარებლისადმი მეგობრული ინტერფეისი, ანუ იგი მაქსიმალურად გასაგები და მოხერხებული უნდა იყოს მომხმარებლისთვის. ბანკში დასამუშავებელი და შენახული ინფორმაცია წარმოადგენს რეალურ ფულს. საბანკო სისტემაში არსებული ინფორმაცია ეხება უამრავ ადამიანს, წარმოება-დანესხებულებებს, ბანკის კლიენტებს. როგორც წესი, ეს

ინფორმაცია არის კონფიდენციალური და ბანკი პასუხისმგებელია კლიენტების წინაშე ინფორმაციის საიდუმლოდ შენახვაზე. წინააღმდეგ შემთხვევაში მისი რეპუტაცია აღმოჩნდება დიდი რისკის ქვეშ. ამიტომ ბანკის საინფორმაციო სისტემა მაქსიმალურად უნდა იყოს დაცული სხვადასხვა შეფერხებებისაგან, მავნებელთა მოქმედებებისაგან.

ბანკის საინფორმაციო სისტემებისადმი წაყენებული ძირითადი მოთხოვნებია:

- ბანკის საინფორმაციო სისტემის არქიტექტურა ისეთი უნდა იყოს, რომ მომხმარებლის შეგნებული ან შემთხვევითი მოქმედებისას მინიმუმამდე შემცირდეს სისტემის საშტატო მუშაობის რეჟიმის დარღვევის ალბათობა, რომელიც გულისხმობს სისტემის გამოსვლას მწყობრიდან, საინფორმაციო სისტემის დანგრევას, ინფორმაციის დამახინჯებას და დაკარგვას;

- ტერიტორიული განაწილება, რომელიც გულისხმობს სისტემის ელემენტების სივრცობრივი განაწილების ინფორმაციულ გაერთიანებას;

- ინფორმაციულად დაკავშირებული სისტემის ელემენტებს შორის ინფორმაციის გაცვლა უნდა განხორციელდეს ინფორმაციული ნაკადების შესაბამისად. აღნიშნული მოთხოვნის განხორციელება იძლევა იმის საშუალებას, რომ სისტემაში ინფორმაციის შეყვანა მოხდეს ერთხელ;

- ინფორმაციული საკმარისობა, ანუ ინფორმაციის გაცვლის სისწრაფე და მოცულობა უნდა შეესაბამებოდეს ბანკში რეალურად მიმდინარე პროცესების ინტენსივობას;

- გარე პირობების ცვლილებებთან ადაპტაცია;

- სისტემის სიცოცხლისუნარიანობა, რომელიც მოიცავს სისტემის ტექნიკურ შესაძლებლობებს. მათ შორის: მწარმოებლურობას, საიმედოობას და სხვა.

საიმედოობა არის საშუალო დრო ორ შეფერხებას შორის და იზომება საათებში.

ბანკის საქმიანობაში საინფორმაციო სისტემას დიდი მნიშვნელობა გააჩნია. ინფორმაციის არასაკმარისი სისრულე, არადროულობა ან შეცდომები ინფორმაციის დამუშავებაში იწვევს

არა მარტო ფინანსურ დანაკარგებს, არამედ ბანკისადმი ნდობის დაკარგვას. საბანკო საინფორმაციო სისტემების საიმედოობის გაზრდა შეიძლება შემდეგი ღონისძიებების გატარების საფუძველზე: მაქსიმალურად საიმედო ელემენტების შერჩევით; ცნობილი ფირმებისგან პროგრამული და ტექნიკური უზრუნველყოფის შეძენით; სისტემის ექსპლუატაციაში შეყვანამდე განხორციელებული თითოეული ელემენტის შემოწმებით, ტესტირებით, კრიტიკული ელემენტების დარეზერვირებით.

საბანკო საინფორმაციო სისტემამ უნდა უზრუნველყოს:

- სინთეზური და ანალიზური აღრიცხვის ერთიანობა;
- მულტივალუტიანობა;
- აქტივებისა და პასივების პორტფელების მართვის შესაძლებლობა;
- ერთიანი ინფორმაციული სივრცის უზრუნველყოფა;
- ფილიალების ქსელის კონსოლიდაცია და მართვადობა;
- შიდა და გარე გარემოს მდგომარეობის (რესურსები და ბაზრები) მართვა.

კითხვები თვითშემოწმებისთვის

1. რა მოთხოვნები წაყენება ბანკის საინფორმაციო სისტემას?
2. დაახასიათეთ ბანკის საქმიანობის ავტომატიზაციის პრინციპები.
3. რომელი ფუნქციური ამოცანების გადაწყვეტა წარმოებს ბანკის საინფორმაციო სისტემების გამოყენებით?
4. რა მოდულებისაგან შედგება ბანკის საინფორმაციო სისტემა?
5. დაახასიათეთ საბანკო სფეროში კომპიუტერული ტექნოლოგიების დანერგვის ეტაპები.

თავი. 2. საბანკო საინფორმაციო სისტემების ინფორმაციული უზრუნველყოფა

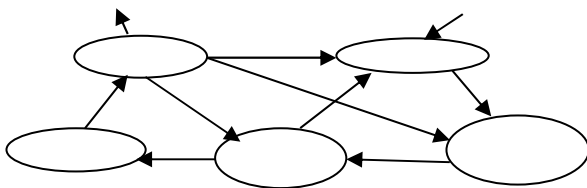
2.1. ინფორმაციული მოდელი

ინფორმაციული უზრუნველყოფა არის საინფორმაციო სისტემაში მომხმარებლის ნორმალური მუშაობისათვის საჭირო და საკმარისი ინფორმაციის მიწოდება და შენახვა. აღნიშნული ინფორმაცია შეიძლება დავაჯგუფოთ რამდენიმე კლასად: ძირითადი და დამხმარე; ტექსტური და ციფრული.

ძირითადი ინფორმაცია დამახასიათებელია იმ საგნობრივი არის ობიექტებისათვის, რომლებშიც გამოიყენება კომპიუტერული სისტემები, ჩვენს შემთხვევაში – საბანკო სფერო. სისტემაში საქმე გვაქვს აგრეთვე დამხმარე ინფორმაციასთან, რომელიც აღწერს ძირითად ინფორმაციას ან მისი დამუშავების ალგორითმებს. საგნობრივი არის ობიექტები შეიძლება აღწერილ იქნეს სხვადასხვა ხერხით.

როგორც წესი, ეკონომისტებს აინტერესებთ ობიექტის რაოდენობრივი მახასიათებლები, ე. ი. ციფრული ინფორმაცია. იმავედროულად, ეკონომიკური ურთიერთობები და კავშირები ეკონომიკურ სივრცეში აღიწერება ტექსტებით, კანონებით, მთავრობის დადგენილებებით, ინსტრუქციებით. გარდა აღნიშნულისა, სისტემის მომხმარებლებმა ერთმანეთში შეიძლება ინფორმაცია გაცვალონ ტექსტური შეტყობინებებით, წერილებით და სხვა სახით. ბანკის წარმატებული ინფორმატიზაციის მიზნით აუცილებელია ბანკის ინფორმაციული მოდელის აგება და ანალიზი. მზა პროგრამული პროდუქტის შეძენისას აუცილებელია გვესმოდეს და ვიცოდეთ კონკრეტული ბანკის თავისებურებები, რათა რეალურად შევაფასოთ შეძენილი სისტემის შესაძლებლობები.

ინფორმაციული მოდელი შეიძლება წარმოდგენილ იქნეს გრაფის სახით (სურ. 2.1.), რომლის წვეროებსაც წარმოადგენენ ინფორმაციული ბლოკები, რომლებიც შეესაბამებიან სისტემის ობიექტებს და განიხილებიან, როგორც „შავი ყუთები“.



სურ. 2.1. ინფორმაციული მოდელი

გრაფის წვეროები შეერთებული არიან მოგეზილი რკალე-ბით. ინფორმაციის გაცვლის წესის შესაბამისად, გრაფის რკა-ლებზე ან სპეციფიკაციებში მითითებულია გადასაცემი დოკუ-მენტებისა და მასივების დასახელება. გარდა აღნიშნულისა, თან-დართული უნდა იყოს დოკუმენტების ფორმები ან მათში მოთა-ველი ინფორმაციის აღწერა, და, აგრეთვე, მასივების სტრუქ-ტურა. კონკრეტული ბანკისთვის პროგრამული და აპარატურუ-ლი უზრუნველყოფის ამორჩევისთვის საჭიროა შესწავლილ იქ-ნეს ბანკში გამოყენებული ტექნოლოგია, ადმინისტრაციული სტრუქტურა და დოკუმენტბრუნვა. სანყის ინფორმაციას წარმო-ადგენს ბანკში შესრულებულ ოპერაციათა ნუსხა, ბანკის ადმი-ნისტრაციული სქემა, ოპერაციების განაწილება ბანკის განყო-ფილებებს შორის. ბანკის ინფორმაციულ მოდელში ასახვა უნდა პოვოს: სისტემის ობიექტებმა და მათ შორის ურთიერთობებმა, ინფორმაციულმა ნაკადებმა და მათი მოძრაობის მიმართულე-ბებმა, ინფორმაციის მატარებლებმა (ქაღალდის დოკუმენტები, სატელეფონო და ელექტრონული შეტყობინებები, ინფორმაცი-ულ ნაკადებზე შესრულებული ოპერაციები, მათი შეცვლა ან ახ-ლის აღმოცენება).

ისე, როგორც სხვა საპროექტო მასალები, ინფორმაციული მოდელი გადის რამდენიმე სტადიას. პირველ სტადიაზე უნდა დაკონკრეტდეს სისტემის ობიექტები და იმ ინფორმაციის მოცუ-ლობა, რომელთა ცირკულირება წარმოებს ობიექტებს შორის, და აგრეთვე, ბანკსა და გარე სამყაროს შორის. ამ უკანასკნელის სა-ფუძველზე უნდა მოხდეს ტექნიკური საშუალებებისა და მონა-ცემთა გადაცემისთვის ქსელების შერჩევა. შემდეგ ეტაპზე კო-დირებისა და უნიფიკაციის წესების გათვალისწინებით წარმოებს

დოკუმენტების ფორმების აღწერა, შემუშავდება ინფორმაციული ბაზის სტრუქტურა (მონაცემთა შიგამანქანური წარმოდგენა), განისაზღვრება ბაზის ტიპური შეკითხვები (მოთხოვნები).

ბანკის მონაცემთა ბაზა სტრუქტურულად რთული და ცვალებადია. ამიტომ ინფორმაციული მოდელის შექმნა წარმოებს ნაწილობრივ განუსაზღვრელ პირობებში. გამომდინარე აღნიშნულიდან, მონაცემთა მოდული უნდა იყოს მოქნილი, ადვილად შესაცვლელი და ითვალისწინებდეს საბანკო სისტემებისათვის წაყენებული მოთხოვნების ცვლილებას. ინფორმაციული მოდელი უნდა იყოს რეალური, სამყაროს ზოგიერთი სფეროს ადეკვატური. არაადეკვატურობის მიზეზი შეიძლება იყოს: არასწორი ცნობების არსებობა; ინფორმაციის მოძველება (რაოდენობრივი კრიტერიუმების არასწორი მონაცემების გადაცემის სიხშირე); არასრული ინფორმაცია; ინფორმაციის არსებობის პირობებში შეფერხებები; ინფორმაციული ხმაური (სისტემაში არსებული სწორი ინფორმაციის შემთხვევაში არასწორი ინფორმაციის გაცემა).

ინფორმაციული ნაკადების ანალიზი საშუალებას იძლევა, გავითვალისწინოთ „ვინრო ადგილები“ (კვანძები, რომლებზედაც ინფორმაციის დამუშავებისას მოდის ყველაზე დიდი დატვირთვა) და ის ადგილები, სადაც პერსონალის სიჭარბე ან ინფორმაციაზე ნაკლები მოთხოვნაა.

ასეთი ანალიზის საფუძველზე შესაძლებელია გაიცეს რეკომენდაციები დოკუმენტბრუნვის ოპტიმიზაციაზე, ოპერაციული მუშაკების დატვირთვაზე, ტექნიკურ გადაიარაღებასა და ინფორმაციის მატარებლების შეცვლაზე. ტექნიკური საშუალებების განვითარებამ შესაძლებელი გახადა ბანკში უქალაქოდ ტექნოლოგიაზე გადასვლა. მონაცემების დამუშავებისას ძირითადი აქცენტი უნდა გადავიდეს მათ ელექტრონული სახით წარმოდგენაზე, რა თმა უნდა, გარკვეული ზომით შენარჩუნებული უნდა იქნეს ინფორმაციის ქალაქდური დოკუმენტებიც, სადაც ეს აუცილებელია სამართლებრივი კუთხით (აუდიტორების საქმიანობა, კონტროლის მიზნით, პარტნიორებთან მუშაობის დოკუმენტური გაფორმება). ცალკეულ შემთხვევებში, როცა ელექტრონული დოკუმენტის იურიდიული სტატუსი გათანაბრებულია ქალაქდის დო-

კუმენტის სტატუსთან, შესაძლებელია, უარი ვთქვათ ქაღალდის დოკუმენტბრუნებაზე. უქაღალდო ტექნოლოგიის უპირატესობაა: მონაცემების სწრაფი გადაცემა; შენახვის უნიკალურობა; დაცვის გაუმჯობესება; დოკუმენტების დამუშავების შრომატევადობის შემცირება.

აქვე უნდა აღინიშნოს, რომ უქაღალდო ტექნოლოგიაზე გადასვლას გააჩნია გარკვეული პრობლემები – მონაცემთა ავტორიზაციის, და მათი ნამდვილობის დამტკიცების. უქაღალდო ტექნოლოგიაზე გადასვლა მოითხოვს ინფორმაციის ავტომატიზებული დამუშავების კულტურის ამაღლებას. ზოგიერთ შემთხვევაში აუცილებელია ბანკის სტრუქტურის გადაკეთება. აგრეთვე, ერთ-ერთ პრობლემას წარმოადგენს ინფორმაციის ოპტიმალური განაწილება ელექტრონულ და ქაღალდის მატარებლებს შორის. აღნიშნულიდან გამომდინარე, საბანკო ოპერაციები იყოფა სამ კლასად:

- გაანგარიშებებში მონაწილე მონაცემები (ასეთი მონაცემები აუცილებლად უნდა იქნეს წარმოდგენილი ელექტრონული სახით);
- ხშირად გამოყენებული და ფორმალიზაციას დაქვემდებარებული დამატებითი ინფორმაცია;
- დეტალური და ძნელად ფორმალიზებადი. კერძოდ, ტექსტური ინფორმაცია (უმჯობესია, ინახებოდეს ქაღალდის მატარებლებზე).

მონაცემთა ბაზებში შენახული ინფორმაცია განსხვავდება სხვა ხერხით შენახული ინფორმაციისგან:

- მონაცემთა ბაზაში ასახული ინფორმაცია იძლევა სხვადასხვა დანართებთან ინტეგრაციის შესაძლებლობას;
- შესაძლებელია მონაცემთა ბაზაში განთავსებული ინფორმაციის მრავალმიზნობრივი, ერთობლივი გამოყენება;
- მონაცემთა ბაზები არსებობს კონკრეტული მონაცემთა ბაზების მართვის სისტემებიდან დამოუკიდებლად;
- მონაცემთა ბაზების საშუალებით შესაძლებელია თავიდან ავიცილოთ მონაცემთა დუბლირება;
- მონაცემთა ბაზები, შექმნილი სათანადო სტანდარტების დაცვით, ამარტივებს მის შექმნასა და მომსახურებას.

პროგრამები, რომლებიც უზრუნველყოფს ზემოთ ჩამოთვლილი ყველა თვისების რეალიზაციას, გაერთიანებულია მონაცემთა ბაზების მართვის სისტემაში.

მონაცემთა ბაზების მართვის სისტემები ორიენტირებულია მონაცემების განსაზღვრულ მოდელებზე და სტრუქტურებზე. მიუხედავად იმისა, რომ მონაცემების წარმოდგენა ხდება ქსელური და იერარქიული მოდელების სტრუქტურების სახით, პრაქტიკაში ყველაზე უფრო მეტად გავრცელებულია მონაცემთა წარმოდგენის რელაციური მოდელი. მონაცემთა რელაციური მოდელი შეიძლება განხილულ იქნეს, როგორც ცხრილების კრებული, რომლებზედაც შესაძლებელია განსაზღვრული პირობების მიხედვით შესრულდეს ამორჩევისა და გაერთიანების ოპერაციები.

ყველაზე გავრცელებულ მონაცემთა ბაზების მართვის სისტემებს მიეკუთვნებიან:

DBase, Paradox, Fox Base, Fox Pro, Clipper. ზემოთ ჩამოთვლილი მბმს-ებიდან ვერც ერთი სრულად ვერ აკმაყოფილებს „კლიენტ-სერვერული“ ტექნოლოგიის მოთხოვნებს, ამიტომ ბანკის საინფორმაციო სისტემებში მონაცემთა ბაზების შექმნა წარმოებს **Orac-le-ის, Sybas-ის, Informix-ის მბმს-ის** და სხვათა გამოყენებით.

მონაცემთა ბაზების შექმნისა და გამოყენების პრაქტიკას მივყავართ თეორიებს უფრო ფართო ცნებამდე – მონაცემთა საცავები, რომელთა საფუძველზეც შესაძლებელია ბანკის ერთიანი ინფორმაციული სივრცის ფორმირება, „კლიენტ-სერვერული“ ტექნოლოგიის რეალიზება, ბანკის სპეციალისტებისა და მართვის პერსონალის მიერ სტრატეგიული და ტაქტიკური გადაწყვეტილებების მიღება.

2.2. დაკრედიტების ამოცანის ავტომატიზებული გადაწყვეტის ორგანიზება

საბანკო ოპერაციების ტექნოლოგია პირობითად შეიძლება დავყოთ მაკრო და მიკრო ტექნოლოგიად.

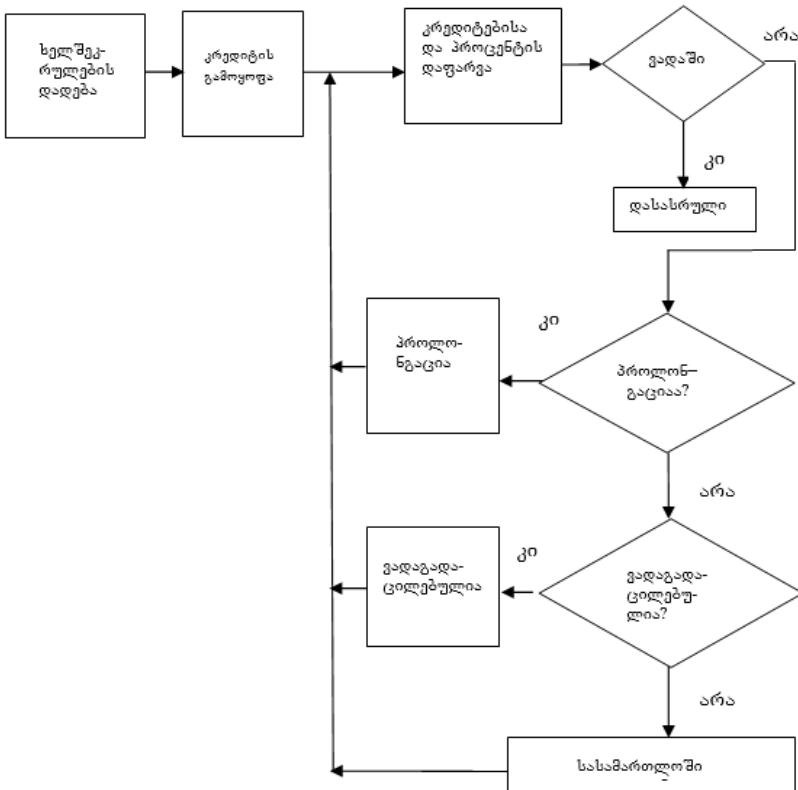
მაკროტექნოლოგია განსაზღვრავს ბანკის თანამშრომლის მიერ საბანკო მომსახურების შესრულებისას მოქმედებათა

(ფუნქციათა) თანმიმდევრობას. მიკროტექნოლოგია კი წარმოადგენს იმ ოპერაციების ჩამონათვალს, რომელსაც ბანკის თანამშრომელი ასრულებს ამა თუ იმ ფუნქციის შესრულებისას.

იმ შემთხვევაში, თუ საწარმოს არ ყოფნის საშუალებები სამეურნეო ამოცანების გადასაწყვეტად, იგი კრედიტის მისაღებად მიმართავს ბანკს. სურ. 2.2-ზე მოცემულია კრედიტის მომსახურების მიკროტექნოლოგია [3], რომელსაც გააჩნია შემდეგი სტრუქტურა: ხელშეკრულების დადება, კრედიტის გაცემა, კრედიტისა და პროცენტის დაფარვა. თუ კრედიტისა და პროცენტის დაფარვა მოხდა ხელშეკრულებით გათვალისწინებულ ვადებში, მაშინ ხდება მისი დახურვა. კრედიტის მომსახურების სქემა მოცემულია სურ. 2.2.-ზე, და გააჩნია შემდეგი სტრუქტურა: ხელშეკრულების დადება, კრედიტის გაცემა, კრედიტისა და პროცენტის დაფარვა. თუ კრედიტისა და პროცენტის დაფარვა მოხდა ხელშეკრულებით გათვალისწინებულ ვადებში, მაშინ ხდება მისი დახურვა, ან პროლონგირება, ე.ი. დაფარვის ვადის გაგრძელება, ან სასამართლოში გადაცემა.

ბანკი, სესხის ამღებს, იურიდიულ პირს, კრედიტის გასაფორმლებად სთხოვს სხვადასხვა დოკუმენტების წარმოდგენას. მიუხედავად იმისა, რომ თითოეულ ბანკს თავისი მოთხოვნები გააჩნია წარმოსადგენი დოკუმენტების ჩამონათვალის მიმართ, ბანკების უმრავლესობა მოითხოვს შემდეგი დოკუმენტების წარდგენას: ნოტარიუსით დამოწმებული ორგანიზაციის დებულება; დამოწმებული სადამფუძნებლო ხელშეკრულება; კრედიტის №1 ოქმი; სახელმწიფო რეგისტრაციის დამადასტურებელი დოკუმენტი, დადგენილი წესით დამოწმებული ხელის მოწერის ნიმუშების ბარათები; განცხადება კრედიტის მიცემის შესახებ (კრედიტის თანხის, კრედიტის დანიშნულების, კრედიტის გაცემის ვადის მითითებით); კრედიტის ტექნიკურ-ეკონომიკური დასაბუთება; ინფორმაცია კრედიტის დაფარვის წყაროს შესახებ. ბანკმა კრედიტის ამღებ ორგანიზაციას შეიძლება აგრეთვე მოსთხოვოს გირაოდ ჩადებული საქონლის შეფასების დოკუმენტი, ორგანიზაციის მოკლე დახასიათება (სპეციალიზაცია, საკრედიტო ისტორია, მფლობელები, ადგილი ბაზარზე, პროექ-

ტის ბიზნესგეგმა, საგადასახადო ინსპექციის დამოწმებული ბალანსი და სხვა).



სურ. 2.2. კრედიტის მომსახურების მიკროტექნოლოგია

კლიენტის მიერ დოკუმენტების წარდგენის შემდეგ საკრედიტო განყოფილების თანამშრომელი შეისწავლის დოკუმენტებს, სესხის ამლების პოტენციურ ფინანსურ მდგომარეობას და დადებითი გადანყვეტილების მიღების შემთხვევაში, აფორმებს კლიენტთან ხელშეკრულებას, რომელშიც მითითებულია კრედიტის გაცემის წესი და პირობები. კონკრეტულად იგი მოიცავს: ხელშეკრულებაში მონაწილეთა დასახელებას; კრედიტის სახეს; კრე-

დიტის თანხას; ხელშეკრულების მოქმედების ვადას; კრედიტით სარგებლობისათვის საპროცენტო განაკვეთს; პროცენტის გადახდის წესს (ყოველთვიურად, ყოველკვარტალურად, ხელშეკრულების დამთავრების შემდეგ); იმ დოკუმენტების ჩამონათვალს, რომლებიც კლიენტმა ბანკის მოთხოვნით უნდა წარადგინოს (ანგარიშსწორების ანგარიშის ნომერი და იმ ბანკის დასახელება, რომელიც ემსახურება კლიენტს); ხელშეკრულებაში მონაწილეთა იურიდიული მისამართები.

კრედიტით სარგებლობის საპროცენტო თანხა იანგარიშება სესხის რაოდენობისა და კრედიტის დაფარვის დროის სიდიდისგან გამომდინარე.

კრედიტით სარგებლობისათვის გადასახდელი თანხა K იანგარიშება შემდეგი ფორმულით:

$$K = (CK * D * CP) / (360 * 100)$$

სადაც CK არის ხელშეკრულებით გათვალისწინებული კრედიტის თანხა;

D – ხელშეკრულების მოქმედების დღეთა რაოდენობა;

CP – საპროცენტო განაკვეთი [3].

სასესხო ანგარიშის გასახსნელად საკრედიტო განყოფილების თანამშრომელი გამოწერს განკარგულებას სასესხო ანგარიშის გახსნის შესახებ და გადასცემს საოპერაციო დღის დისპეტჩერს. გამოყოფილი თანხის მაშინვე სასესხო ანგარიშზე გადასარიცხად გადაეცემა მემორიალური ორდერი. კრედიტის გაცემა კლიენტზე შეიძლება განხორციელდეს სასესხო ანგარიშიდან ანგარიშსწორების ანგარიშზე, მთლიანად ან ნაწილ-ნაწილ, სესხის ამლების მიერ შეძენილ ან განუღო მომსახურებაზე დამატებული დოკუმენტების წარმოდგენის შემდეგ. საკრედიტო ხელშეკრულების შევსებისა და ხელის მოწერის შემდეგ ხდება მისი რეგისტრაცია ჟურნალში, რომელშიც მითითებულია ხელშეკრულების ძირითადი პუნქტები. შემდეგ ბუღალტერიას გადაეცემა განკარგულება კლიენტისათვის სასესხო ანგარიშის, მემორიალური ორდერის გახსნისა და კლიენტის სასესხო ანგა-

რიშიდან კლიენტის ანგარიშსწორების ანგარიშზე საჭირო თანხის ჩარიცხვის შესახებ.

თუ კლიენტისათვის კრედიტის თანხის გაცემა წარმოებს უშუალოდ, მაშინ რეგისტრაციის ჟურნალში მიეთითება ხელშეკრულების ნომერი ხელშეკრულების დადების თარიღი, გაცემული კრედიტის თანხა, ანგარიშიდან ფულის გადარიცხვის თარიღი, პროცენტის დარიცხვისა და დამთავრების თარიღი, ხელშეკრულების დამთავრებისა და პროცენტის დარიცხვის დამთავრების თარიღი.

კლიენტის მიერ კრედიტის დაფარვა ხორციელდება სააღრიცხვო-საოპერაციო სამუშაოების განყოფილების მეშვეობით. კრედიტის დაფარვისა და პროცენტის გადახდის მიკროტექნოლოგია მდგომარეობს იმაში, რომ სესხის ამღები ხელშეკრულებით გათვალისწინებულ ვადაში საგადამხდელო დავალების საფუძველზე ახდენს გატარების ინსცენირებას, მისი ანგარიშსწორების ანგარიშიდან ბანკის სასარგებლოდ საჭირო თანხის გადარიცხვის შესახებ. თუ სესხის ამღებმა კრედიტის თანხა დადარიცხული პროცენტის თანხა თავის დროზე ვერ გადაიხადა, მიუხედავად იმისა, რომ კლიენტის ანგარიშზე საკმარისი ფულია, ბანკს უფლება არ აქვს მოხსნას ფული კლიენტის ანგარიშიდან. პროცენტის გადახდა წარმოებს ან ყოველთვიურად, ან კიდევ ხელშეკრულების დამთავრებისას, სესხის დაბრუნების მომენტი-სათვის. ამ დღისთვის სესხის ამღები ვალდებულია, გადარიცხოს აუცილებელი თანხა. ბანკში შესაბამისი საგადამხდელო დოკუმენტის მიღების შემდეგ აფიქსირებენ კრედიტისათვის თანხის გადახდას. პროცენტის დაბრუნება წარმოებს სესხის ამღების ანგარიშსწორების ანგარიშიდან საგადამხდელო საფუძველზე, რომელშიც მიეთითება, რომ გადარიცხული თანხა არის კრედიტით სარგებლობისათვის თანხა. როგორც ზემოთ აღვნიშნეთ, ეს გაანგარიშებები სრულდება სააღრიცხვო-საოპერაციო სამუშაოების ქვესისტემაში. თუ სესხის ამღებმა დაარღვია პროცენტის გადახდის ვადა ან სრულად ვერ დაფარა კრედიტი, ბანკი მას დაარიცხავს ჯარიმას და საურავს (პენიის). თუ სესხის ამღებმა დაარღვია ხელშეკრულებაში კრედიტის დაფარვის ვადა, მაშინ საკრედიტო განყოფილების თანამშრომელი, რომელსაც ევალება

გაცემული კრედიტების სიტუაციის კონტროლი, გადაიტანს მოცემულ კრედიტს ვადაგადაცილებული სესხების სიაში ან დაარიცხავს საურავს (პენიე), ან, სესხის ამლების თხოვნით, ახორციელებს ხელშეკრულების პროლონგაციას (ვადის გაგრძელებას). ამ მიზნით დგება დამატებითი ხელშეკრულება, რომელშიაც შეიძლება უცვლელი დარჩეს ძველი პირობები, გარდა კრედიტის დაფარვის გრაფიკისა, ან მოხდეს პირობების გადახედვა. თუ ხელშეკრულება შესრულდა ორივე მხრიდან, მაშინ იგი იხურება, ანალიზური სასესიო ანგარიში უქმდება და ყველა საბუთი თავსდება კლიენტის ისტორიის საქაღალდეში.

ბანკის საქმიანობის ანალიზი და მისი ეფექტიანობის შეფასება ხდება საკრედიტო ხელშეკრულებების დახასიათებების საფუძველზე (თანხის რაოდენობის, მათი შესრულების მიმდინარეობა, საპროცენტო განაკვეთების დონე, დაფარული კრედიტები და ვადაგასული კრედიტები). ინფორმაციის ხელით დამუშავების შემთხვევაში, ანგარიშგებების შედგენა წარმოებს დადებული ხელშეკრულებებისა და მათი რეგისტრაციის ჟურნალის საფუძველზე.

ახლა განვიხილოთ კრედიტების აღრიცხვის ტექნოლოგია საკრედიტო განყოფილების თანამშრომლის ავტომატიზებული სამუშაო ადგილის (სგასა) ფუნქციონირების შემთხვევაში.

სგასა კომპლექსის საშუალებით შესაძლებელია როგორც საკრედიტო გარიგების გაფორმება, ასევე, საკრედიტო ხელშეკრულების წარმოება მისი მოქმედების მთლიან პერიოდში. საკრედიტო განყოფილების თანამშრომელს უნდა გააჩნდეს სრული ინფორმაცია, დაწყებული კრედიტის გაცემის რეგისტრაციიდან, დამთავრებული სხვადასხვა სტატისტიკური ანგარიშგებითი ფორმების ავტომატიზებული მიღებით.

დასახული ამოცანის ავტომატიზებული გადანაცვებისათვის საჭიროა შემდეგი ნომენკლატურის კოდების შემუშავება: ფულადი საშუალებების გადაცემის მდგომარეობის (0 – არ დაწყებულა, 1 – არ დამთავრებულა, 2 – დამთავრდა, 3 – დაიფარა, 4 – ვადა გადაცილდა, 5 – გადაყვანილია „ვადაგადაცილებულის“ მდგომარეობაში, 7 – გადაყვანილია „პროლონგირების“ მდგომარეობაში).

პროცენტის დაფარვის ტიპის კოდია ორნიშნა პოზიციური, რომლის პირველი თანრიგი მარცხნიდან მიუთითებს დაფარვის ხასიათზე (1 – ერთდროული, 2 – ნაწილ-ნაწილ). ხოლო მეორე თანრიგი მიუთითებს დაფარვის სახეს (ყოველკვირეულად, ყოველდეკადურად, ყოველთვიურად, ყოველკვარტალურად, ერთხელ წელიწადში). პროცენტის დაფარვის კოდია ერთთანრიგა რიგითი, ხელშეკრულების მდგომარეობის კოდი ერთთანრიგა რიგითი და შეიძლება მიიღოს შემდეგი მნიშვნელობები: შავი, პირობითად შესასრულებელი, რეალურად შესასრულებელი და დამამთავრებელი. რეალურად შესასრულებელმა ხელშეკრულებამ შეიძლება მიიღოს შემდეგი მნიშვნელობები: ნორმალური, ვადაგადაცილებული და პროლონგირებული. ხელშეკრულების მოქმედების დაწყების კოდი არის ერთნიშნა რიგითი: 1 – ფულადი საშუალებების შემოსვლისთანავე და ხელშეკრულებაზე ხელის მოწერის მომენტიდან. კრედიტის დაბრუნების საიმედოობის კოდი არის ერთთანრიგა და იცვლება 0-დან 9-მდე, ოპერაციის სახის კოდი არის ორნიშნა რიგითი; 01 – სესხის სრულად გაცემა, 02 – სესხის ნაწილობრივ გაცემა, 03 – სესხის დაფარვა გრაფიკის მიხედვით, 04 – „ვადაგადაცილებულ“ მდგომარეობაში გადაყვანა, 05 – „პროლონგირებულ“ მდგომარეობაში გადაყვანა, 06 – ვადაგადაცილებული სესხისათვის პროცენტის დარიცხვა, 07 – ვადაგადაცილებული სესხისათვის ვალის დაფარვა, 08 – ზარალში ჩამოწერა, 09 – პროცენტის დაფარვა, 10 – პროცენტის გადაყვანა „ვადაგასულის“ მდგომარეობაში, 11 – პროცენტის გადაყვანა „პროლონგირების“ მდგომარეობაში, 12 – პროცენტის დაფარვა სურვილის მიხედვით, 13 – სესხზე საურავის დაფარვა, 14 – პროცენტზე საურავის დაფარვა, 15 – სესხზე საურავის სურვილის მიხედვით დაფარვა, 16 – პროცენტზე საურავის სურვილის მიხედვით დაფარვა.

გადახდების რეგისტრაციისათვის გამოიყენება ხელშეკრულების მიხედვით გადახდების ფაილი და ბანკის დაწესებულებათა ცნობარის ფაილი. კრედიტის გაცემა, კრედიტით სარგებლობისათვის თანხის გადახდა და კრედიტის დაფარვის რეგისტრაცია ხორციელდება შესაბამისი დოკუმენტების არსებობისას. საგადახდელო მოთხოვნა შეიცავს შემდეგ რეკვიზიტებს: დავა-

ლების ნომერი; გაფორმების თარიღი; გადამხდელის რეკვიზიტები; მიმღების რეკვიზიტები; სადებეტო ანგარიში; საკრედიტო ანგარიში; გადარიცხული თანხა, ოპერაციის სახე (გადახდის მიზეზი). საგადამხდელო დავალებას გამოწერს კლიენტი და აბარებს სააღრიცხვო-საოპერაციო სამუშაოთა განყოფილებაში, რომლის საფუძველზეც ხდება შესაბამისი პირადი და სინთეზური ანგარიშების კორექტირება. ყოველდღიურად სააღრიცხვო-საოპერაციო სამუშაოთა განყოფილებიდან საკრედიტო განყოფილებაში გადაეცემა გატარებები. ხელშეკრულების შესრულების ისტორია ასახულია ხელშეკრულების მდგომარეობის ფაილში.

სგასა-ს მთავარი მენიუ შედგება შემდეგი ფუნქციებისაგან: ხელშეკრულებებთან მუშაობა; გატარებებთან მუშაობა; ანგარიშგებების ფორმირება და სხვადასხვა.

ხელშეკრულებებთან მუშაობის ფუნქციაში შედის: ხელშეკრულების შეტანის, კონტროლის და კორექტირების სამუშაოები. ამ დროს წარმოებს კრედიტით სარგებლობისათვის გადასახდელის გაანგარიშება და კრედიტის დაფარვის გრაფიკის ფორმირება.

გატარებებთან მუშაობის ფუნქცია ახორციელებს იმ გატარებების ამორჩევას, რომელიც დაკავშირებულია საკრედიტო განყოფილების თანამშრომლის მიერ კრედიტის მომსახურებასთან. კერძოდ: საკრედიტო ჟურნალში კრედიტის გაცემის რეგისტრაცია; კრედიტის მიხედვით გადახრათა რეგისტრაცია; კრედიტის გადაყვანა ვადაგასულთა სიაში; ხელშეკრულების გადაყვანა პროლონგაციაში; ხელშეკრულების დახურვა.

ფუნქცია სხვადასხვა ითვალისწინებს ცნობარებთან მუშაობას (საპროცენტო განაკვეთის შეცვლა, ცნობარის დათვალიერება და კორექტირება).

ბაზასთან მუშაობის ფუნქცია: ბაზის კოპირება, აღდგენა, რეორგანიზაცია და სხვა. მენიუში შეიძლება აისახოს ისეთი ფუნქცია, როგორიცაა ბანკთაშორის კრედიტებთან მუშაობა; საკრედიტო ხელშეკრულების ღირებულების განსაზღვრა; კრედიტის ამღების გადახდისუნარიანობის შეფასება; კრედიტის რისკების შეფასება.

გარდა ჩამოთვლილი სტატისტიკური ანგარიშგებითი ფორმებისა, დაკრედიტების განყოფილების თანამშრომლების მიერ გადანყევტილების მისაღებად ავტომატიზებულ სამუშაო ადგილზე ფორმირდება შემდეგი უწყისები:

თვის განმავლობაში დარიცხული და ანაზღაურებული პროცენტები; ფაქტობრივად და გეგმიურად გადახდილ თანხათა რეესტრი; ცნობა შესრულებული ხელშეკრულებების შესახებ; ვადაგადაცილებული სესხების უწყისი და ა. შ.

განვიხილოთ საკრედიტო განყოფილების თანამშრომლის მიერ ავტომატიზებულ სამუშაო ადგილზე ამოცანების გადანყევტიის ტექნოლოგია: საკრედიტო განყოფილების თანამშრომელი მონაცემთა ბაზაში არსებული ხელშეკრულებების შაბლონების საფუძველზე ადგენს კრედიტის გაცემის ხელშეკრულებას, ტექსტური ფორმით, რომელსაც გააჩნია შავად ნაწერის (სამუშაო ვარიანტი) სტატუსი. საკრედიტო ხელშეკრულება, როგორც ტექსტური დოკუმენტი, შეიცავს: ხელშეკრულებაში მონაწილეთა დასახელებას, კრედიტის სახეს, კრედიტის თანხას, კრედიტის ვადას, საპროცენტო განაკვეთს, პროცენტის გადახდის წესს, კრედიტის უზრუნველყოფის სახეს, ბანკის მოთხოვნით წამოდგენილი დოკუმენტების ჩამონათვალს, ანგარიშსწორების ანგარიშის ნომერს და იმ ბანკის რეკვიზიტებს, რომელიც ემსახურება მოცემულ წარმოება-დანესებულებას, იურიდიულ მხარეთა მისამართებს. აღნიშნული მონაცემები წარმოდგენილია ორი ფაილის სახით: საანგარიშო მონაცემების ხელშეკრულების ფაილი (ხელშეკრულება მონაცემები) და ტექსტური ინფორმაციის ფაილი (ხელშეკრულება ტექსტი).

ახალი საკრედიტო ხელშეკრულების რეგისტრაციისა და მისი ეკრანზე დათვალიერებისა და რედაქტირების მიზნით, გამოიყენება შესაბამისი მაკეტი. ამ უკანასკნელის საფუძველზე წარმოებს ხელშეკრულების ვიზუალური და ლოგიკური კონტროლი. შეტანილი ინფორმაციის კონტროლი აუცილებელია, ვინაიდან ინფორმაციის შეტანისას დაშვებული შეცდომები საბოლოოდ გამოიწვევს გაანგარიშებული შედეგების შეუსაბამობას რეალურ მდგომარეობასთან.

ტექნოლოგიური თვალსაზრისით ხელშეკრულებას შეიძლება გააჩნდეს სხვადასხვა სტატუსი: შავი ხელნაწერის (სამუშაო ვარი-

ანტი), პირობითად მოქმედის, რეალურად მოქმედის და დამამთავრებლის. თავდაპირველად შავი ხელნაწერი ხელშეკრულება ხელის მოწერის შემდეგ ღებულობს პირობითად მოქმედი ხელშეკრულების სტატუსს. ეს უკანასკნელი რეალურად მოქმედი ხელშეკრულების სტატუსს ღებულობს მის საფუძველზე განხორციელებული ფინანსური საშუალებების გადაადგილების შემდეგ. რეალურად მოქმედი ხელშეკრულების სტატუსს იგი ღებულობს ბანკსა და სესხის ამღებს შორის ფაქტობრივად და გეგმის მიხედვით ანგარიშსწორების დამთავრების შემდეგ. რეალურად მოქმედი ხელშეკრულების სტატუსის მქონე ხელშეკრულებას გააჩნია დაზუსტებული სტატუსი: ნორმალურად მოქმედი, ვადაგადაცილებული, პროლონგირებული (ვადაგაგრძელებული). მონაცემთა ბაზაში შესაძლებელია მხოლოდ შავი ხელშეკრულების ნაშლა. რაც შეეხება დანარჩენი სტატუსის მქონე ხელშეკრულებებს, შესაძლებელია მხოლოდ მათი დათვალიერება.

სასესხო და ანგარიშსწორების ანგარიშზე ფულის ჩარიცხვის, ხელშეკრულების პროლონგაციისა და ხელშეკრულების ვადაგადაცილებულში გადაყვანის დროს წარმოებს გატარებების ფორმირება და მათი გადაცემა სააღრიცხვო-საოპერაციო სამუშაოთა განყოფილებაში. გატარებებისა და დარიცხული პროცენტების ფაილების საფუძველზე, ხელშეკრულებების მიხედვით ფორმირდება გეგმიური გადახდების ფაილი, რომლის დამუშავება წარმოებს გატარებების ფაილთან ერთად, რის შედეგადაც წარმოიქმნება ხელშეკრულებების მიხედვით გადასახდელთა ფაილი. ამ უკანასკნელის საფუძველზე კი მიიღება ხელშეკრულებების მდგომარეობის უწყისი, კრედიტების ჟურნალი და ა. შ. პროლონგაციის დროს აღნიშნული ტექნოლოგია მეორდება, მაგრამ ხელშეკრულების სტატუსი იცვლება. თუ ხელშეკრულების გადაყვანა ხდება ვადაგადაცილებულში, მაშინ იცვლება არა მარტო სტატუსი, არამედ მას დამატებით დაერიცხება საურავი. როგორც პირველ, ისე მეორე შემთხვევაში, ხდება სათანადო გატარებების ფორმირება. ხელშეკრულების დახურვისას იცვლება მხოლოდ სტატუსი.

შესაძლებელია საპროცენტო განაკვეთების ცალკე ფაილად გატანა. ამ ფაილში ანგარიშსწორების ანგარიშის ნომერი შეიძლება არ იყოს, იქიდან გამომდინარე, თუ ცალკე შექმნილია კლიენტის ფაილთან დამაკავშირებელი ფაილი. ასევე ანგარიშსწორების ანგა-

რიშის ნომერი შეიძლება ნულის ტოლი იყოს, თუ კლიენტს ანგარიში გახსნილი აქვს სხვა ბანკში, ამ შემთხვევაში გამოიყენება ბანკების საცნობარო ფაილი.

პროცენტების დარიცხვის (მათ შორის, საურავის) ფაილი შეიცავს შემდეგ რეკვიზიტებს: ხელშეკრულების ნომერი; პროცენტის დარიცხვის საბაზისო თანხა; პროცენტების სახე (სხვადასხვა სახის პროცენტები და საურავები); პროცენტის დარიცხვის დაწყების თარიღი; პროცენტის დარიცხვის დამთავრების თარიღი; ანაზღაურების თვე; ანაზღაურების დღე; საპროცენტო განაკვეთი; დარიცხვის ალგორითმის ტიპი;

ხელშეკრულების მიხედვით, თანხის გადახდის ფაილს გააჩნია შემდეგი სტრუქტურა: ვალის ძირითადი ნაწილის გადახდის ნომერი; გეგმიური გადახდის თარიღი (მითითებული უნდა იყოს კრედიტის დაფარვის ბოლო თარიღი); გეგმის მიხედვით გადასახდელი თანხა. ფაქტობრივი გადახდის თარიღი; კლიენტის ანგარიშიდან თანხის გადარიცხვის თარიღი; ფაქტობრივად შეტანილი თანხა; გატარების ნომერი; გადახდის სახე; საშუალებების გადაცემის მდგომარეობა. ამოცანის გადანაცემის მსვლელობაში შესაძლებელია სხვადასხვა უწყისების ფორმირება, რომელთა საფუძველზედაც საკრედიტო განყოფილების თანამშრომელი მიიღებს შესაბამის გადანაცემილებას. საშედეგო ინფორმაციის გამოტანა შეიძლება, როგორც ცხრილური, ასევე გრაფიკული სახით.

ამოცანის გადანაცემის შედეგად მიიღება შემდეგი საშედეგო ფორმები: კრედიტების ჟურნალი (ფორმა 2.1.); დარიცხული და გადახდილი პროცენტების უწყისი (ფორმა 2.2.); პროცენტის გეგმიური გადახდის უწყისი (ფორმა 2.3.); საკრედიტო ოპერაციების მიხედვით პროცენტისთვის გადახდილი თანხების უწყისი (ფორმა 2.4.); ხელშეკრულების მიხედვით გადასახდელთა უწყისი (ფორმა 2.5.); მოცემული პერიოდისთვის ხელშეკრულებების შესრულების ცნობა (ფორმა 2.6.); მოცემული პერიოდისთვის დაფარული კრედიტების უწყისი (ფორმა 2.7.); მოცემული ვადაგასული კრედიტების უწყისი (ფორმა 2.8.); დროის მიხედვით ხელშეკრულების სტატისტიკა (ფორმა 2.9.); ცნობა ხელშეკრულების მოქმედების დროის შესახებ (ფორმა 2.10); და ა. შ. განვიხილოთ ზოგიერთი საშედეგო ფორმის სტრუქტურა:

კრედიტების ჟურნალი. ფორმა 2.1.

სესხის ამლები ორგანი- ზაციის დასახე- ლება	მოცემული პერიოდისთვის დაფარული კრედიტების უწყისი; სასესხო ანგარიში	ხელშეკ- რულების გაფორმებ- ის თარიღი	თანხა	პერიოდი (დღეები)	პროცენტებ- ის დარიც- ხვის დაწყების თარიღი	პროცენ- ტების დარიცხვის დამთავ- რების თარიღი
--	---	--	-------	------------------	---	---

ფორმა 2.1.-ის გაგრძელება

მიმდინარე წლის გადასახდელები			ხელშეკ- რულების დამთავრე ბის თარიღი	დავა- ლი- ანება სესხზე	დავალი- ანება პროცენტ ებზე
კრედი- ტის დაბრუნ ება	პროცენტე ბის გადახდა	პირ- გასამტეხლო ს თანხა			

დარიცხული და გადახდილი პროცენტების უწყისი

თვე-----2025 წელი ფორმა 2.2.

სესხის ამლები ორ- განი-ზაციის დასახელება	ხელშეკრუ- ლების ნომერი	ხელშეკ- რულების გაფორმების თარიღი	დარიცხულია	
			პროცენტი	პირგასა- ტეხლის თანხა

ფორმა 2.2.-ის გაგრძელება

გადახდილია			დავალიანება
თანხა	თარიღი	დოკუმენტის ნომერი	

პროცენტის გეგმიური გადახდის უწყისი. ფორმა 2.3.

საბალანსო ანგარიშის	პირადი ანგარიშის ნომერი	სესხის ამლები ორგანიზაციის დასახელება	ხელშეკრუ- ლების ნომერი	ხელშეკ- რულების გაფორმების თარიღი
------------------------	-------------------------------	---	------------------------------	--

ფორმა 2.3.-ის გაგრძელება

თანხის გადარიცხვის ვადა	კრედიტის დაბრუნების თარიღი	კრედიტის პროცენტის სიდიდე	კრედიტის თანხა
-------------------------------	----------------------------------	---------------------------------	-------------------

საკრედიტო ოპერაციების მიხედვით პროცენტებისთვის გადახდილი თანხების უწყისი. ფორმა 2.4.

პერიოდი	დარიცხული პროცენტები (ლარი)	გადახდილია კრედიტისთვის (ლარი)	გადახრა	
			დავალი- ანება	ზედმეტად გადახდილი თანხა (ლარი)

ხელშეკრულების სასესხო ანგარიშის მიხედვით გადასახდელთა უწყისი. ფორმა 2.5.

თარიღი	სადებეტო ანგარიში	საკრედიტო ანგარიში	ოპერაციის კოდი (გადახდის სახე)	თანხა
--------	----------------------	-----------------------	--------------------------------------	-------

მოცემული პერიოდისთვის ხელშეკრულებების შესრულების ცნობა. ფორმა 2.6.

ხელშეკრულებები	ხელშეკრულებათა რაოდენობა	თანხა ხელშეკრულების მიხედვით
----------------	-----------------------------	------------------------------------

დამთავრებული *

მოქმედი *

სულ დადებული ხელშეკრულებები *

მოცემული პერიოდისთვის დაფარული კრედიტების უწყისი. ფორმა 2.7.

ხელშეკრუ- ლების	ორგანიზაციი ს დასახელება	კრედიტ ის თანხა	ხელშეკრ ულების დაბრუნე ბის თარიღი	პრო- ლონ- გაციის ბოლო თარიღი	ხელშეკრ ულების დახურვი ს თარიღი
--------------------	-----------------------------	-----------------------	---	--	--

**მოცემული პერიოდისთვის ვადგასული
კრედიტების უწყისი. ფორმა 2.8.**

ხელ- შეკრუ- ლების	ორგანი- ზაციის დასა- ხელება	დავალი- ანების თანხა	კრედიტის გეგმით დაბრუნების თარიღი	ვადაგა- დაცი- ლებლი (დღეები)	ჯარ- იმის პრო- ცენტი	საურ- ავის თანხა
-------------------------	--------------------------------------	----------------------------	--	---------------------------------------	-------------------------------	------------------------

დროის მიხედვით ხელშეკრულების სტატისტიკა.ფორმა 2.9.

ხელშეკრულების მოქმედების ვადა	ხელშეკრულებების რაოდენობა	თანხა	ხვედრიითი წილი %
----------------------------------	------------------------------	-------	---------------------

ერთ თვემდე * * *

ორ თვემდე * * *

სამ თვემდე * * *

სამ თვეზე მეტი * * *

**ცნობა ხელშეკრულების მოქმედების დროის
შესახებ. ფორმა 2.10.**

ხელშეკ- რულების ნომერი	ორგანიზ- აციის დასა- ხელება	ხელშეკრუ- ლების გა- ფორმების თარიღი	ხელშეკრუ- ლების დამთავრები ს თარიღი	ხელშეკრუ- ლების მოქმედების დანწყების თარიღი	დამატებითი- თი ხელშეკრულე- ბების რაოდენობა
------------------------------	--------------------------------------	--	--	---	--

მსხვილი სესხები;

მოცემულ პერიოდში მოქმედი ხელშეკრულებების რაოდენო-
ბა;

კლიენტების ჩამონათვალი;

ხელშეკრულებების მიხედვით ნეგატიური სიტუაციები.

კითხვები თვითშემოწმებისთვის

1. რას მოიცავს ბანკის ინფორმაციული მოდელი?
2. რატომ არის საჭირო ბანკში ინფორმაციული ნაკადების ანალიზი?
3. რა დოკუმენტები უნდა წარადგინოს იურიდიულმა პირმა ბანკში კრედიტის გასაფორმებლად?
4. როგორია კრედიტით სარგებლობისათვის გადასახდელი თანხა?
5. რა სახის კოდებია საჭირო დაკრედიტების ამოცანის ავტომატიზებული გადანაცვებისთვის?
6. რა თანმიმდევრობით ხდება საკრედიტო განყოფილების თანამშრომლის ავტომატიზებული სამუშაო ადგილის ფუნქციონირების შემთხვევაში დაკრედიტების ამოცანის რეალიზაცია?
7. რომელი ინფორმაციული ფაილები გამოიყენება დაკრედიტების ამოცანის გადანაცვების ავტომატიზაციისათვის?
8. დაახასიათეთ დაკრედიტების ამოცანის ავტომატიზებული გადანაცვებისას მიღებული საშედეგო ფორმები.

თავი 3. საბანკო ელექტრონული სისტემების ტექნიკური საშუალებები

3.1. ბანკში გამოყენებული ავტომატიზებული საინფორმაციო სისტემები

ბანკში გამოყენებული ავტომატიზებული საინფორმაციო სისტემები შეიძლება მივაკუთვნოთ ქვემოთ ჩამოთვლილიდან ერთ-ერთს:

- სისტემები, რომლებიც იყენებენ პერსონალურ კომპიუტერებს ქსელის გარეშე. მონაცემების შენახვა ასეთ სისტემებში წარმოებს ფაილების სახით, ინფორმაციის გაცვლა ხდება დისკების საშუალებით;

- პერსონალური კომპიუტერები გაერთიანებულია ქსელში და ორგანიზებულია „ფაილ-სერვერული ინტელექტუალური მუშა სადგურების“ სქემის მიხედვით. პერსონალური კომპიუტერი ინტელექტუალური ტერმინალის რეჟიმში უზრუნველყოფს ჩვეულებრივი ტერმინალის ყველა ფუნქციის რეალიზაციას. მას შეუძლია ინფორმაციის ადგილზე დამუშავება, მუშაობა ავტონომიურ რეჟიმში (როგორც ავტომატიზებული სამუშაო ადგილი, საკუთარი რესურსებით);

- სპეციალიზებული დანართების სერვერების საფუძველზე აგებული სისტემები, ე.ი. მაღალმწარმოებლური კომპიუტერი, რომელიც მუშაობს მრავალამოცანიანი და მრავალმომხმარებელიანი სისტემების მართვის მეშვეობით და მუშა სადგურებს ემსახურება „კლიენტ-სერვერის“ რეჟიმში;

- სისტემები, რომლებიც იყენებენ განაწილებულ მონაცემთა ბაზებს. მაგ., მთავარი ოფისისა და ფილიალის ინფორმაციის დამუშავება კომპიუტერში წარმოებს ერთიანი, მთლიანი ფაილის სახით.

საბანკო აღჭურვილობის მახასიათებლები. საბანკო აღჭურვილობა გამოიყენება არა მხოლოდ საბანკო დაწესებულებებში, არამედ საცალო მაღაზიებში, სანარმოებსა და ბენზინგასამართ

სადგურებში, გაცვლის ოფისებში და გადახდების ადგილებზე. აღჭურვილობა შეიძლება იყოს ძვირი და გონივრულ ფასად; ზოგიერთი მოწყობილობა ასრულებს ერთ ფუნქციას, ზოგი კი მრავალ-ფუნქციურია. სწორი არჩევანის გასაკეთებლად, საჭიროა ვიცოდეთ არა მხოლოდ მოწყობილობების მახასიათებლები, არამედ ნათლად გესმოდეს ბიზნესის საჭიროებები.

მოწყობილობა უნდა აკმაყოფილებდეს რამდენიმე მოთხოვნას:

- უნდა იყოს საიმედოობა და ეფექტიანი;
- უნდა ხასიათდებოდეს დაბალი ცვეთის დაბალი ხარისხით;
- უნდა გააჩნდეს მაღალი პროდუქტიულობა და ეფექტიანობა;
- მიმწოდებლისა და მწარმოებლის კარგი რეპუტაცია;
- მწარმოებლის გარანტია [4].

3.2. კომპიუტერის მუშაობის რეჟიმები

კომპიუტერის გამოყენების საწყის ეტაპზე მისი გამოყენების დრო უფრო ძვირად ფასობდა, ვიდრე მასზე მომუშავე სპეციალისტის დრო, ამიტომ გამოთვლითი პროცესების ორგანიზებისას მეტი ყურადღება ეთმობოდა კომპიუტერის მოცდენას. ამოცანების ფორმირება მანქანურ მატარებლებზე წარმოებდა პაკეტების სახით, რომელიც მოიცავდა ამოცანის გადანყვეტის პროგრამას და საჭირო საწყის მონაცემებს. მსგავსი დავალებების შესრულება ხდებოდა ერთიმეორის მიყოლებით, დროის მინიმალური დანაკარგებით. მათი გაშვება და შესრულება არ მოითხოვდა რთულ სისტემურ პროგრამებს, აუცილებელი მანიპულაციები კომპიუტერზე ხორციელდებოდა პროგრამისტის ან ოპერატორის მიერ. თითოეულ მოცემულ მომენტში კომპიუტერზე სრულდებოდა მხოლოდ ერთი ამოცანა (პროგრამა), მუშაობდა მხოლოდ ერთი მოწყობილობა, დანარჩენი მოწყობილობები ელოდებოდნენ პროგრამის შესაბამის ბრძანებებს. აპარატურის გამოყენების დრო იყო მცირე. კომპიუტერის მუშაობის ასეთ რეჟიმს ეწოდება ერთპროგრამული.

მცდელობას, აემაღლებინათ მოწყობილობების დატვირთულობა და, შესაბამისად გაეიაფებინათ ინფორმაციის დამუშავების ღირებულება, მოჰყვა კომპიუტერის სტრუქტურის ცვლილებას, რის გამოც შესაძლებელი გახდა, კომპიუტერზე ერთდროულად შესრულებულიყო რამდენიმე პროგრამა. სანამ ერთი პროგრამა დაკავებული იყო მონაცემების შეყვანით, მონაცემების დამუშავების ბრძანებების შესრულება შეუძლებელი იყო, პროცესორი სხვა პროგრამას ასრულებდა, ბეჭდვის მოწყობილობას ბეჭდვაზე გამოჰქონდა მეორე პროგრამის მიერ გაანგარიშებული შედეგები. ინფორმაციის დამუშავების ასეთ რეჟიმს მრავალპროგრამული რეჟიმი ეწოდება.

საიმედოობის ამაღლების შესაბამისად, კომპიუტერის გამოყენება ხდებოდა არა მარტო საინჟინრო ამოცანების ამოსახსნელად, არამედ ტექნოლოგიური მოწყობილობების, ობიექტების მოძრაობისა და სხვა პროცესების მართვისათვის. კომპიუტერის ასეთი გამოყენება საჭიროებდა ინფორმაციის დამუშავების პროცედურების შესრულებას პროცესების მიმდინარე ტემპების შესაბამისად. აღმოცენდა ინფორმაციის რეალური დროის მასშტაბში დამუშავების რეჟიმი. კომპიუტერის არქიტექტურისა და ოპერაციული სისტემების განვითარებამ და აპარატურის ღირებულების შემცირებამ შექმნა წანამძღვრები, პროგრამის შესრულების პროცესში ოპერატორს დაემყარებინა ურთიერთობა პროგრამასთან. მომხმარებლის მხრიდან შესაძლებელი გახდა პროგრამის შესრულების პროცესის მართვა, ანუ კომპიუტერთან დიალოგის დამყარება.

დიალოგის პროცესში ოპერატორს ტერმინალის კლავიატურის დახმარებით შეეძლო, მონაცემები შეეტანა კომპიუტერში, გაანგარიშებული შედეგები გამოეტანა, მიეღო გადანაცვტილება პროგრამის შემდგომი მუშაობის შესახებ. ყოველივე ამან გამოიწვია მომხმარებლის შრომისნაყოფიერების გაზრდა, განსაკუთრებით, პროგრამის შესრულებისას. აღმოცენდა ინფორმაციის დამუშავების დიალოგური რეჟიმი.

ბუნებრივია, კომპიუტერის რესურსები მულტიპროგრამულ რეჟიმში მუშაობისას ერთი მომხმარებლისათვის იყო ჭარბი და ძვირი, ამიტომ კომპიუტერის გამოყენება დაიწყეს მრავალმომ-

ხმარებლიან რეჟიმში, რომლის დროსაც გამოთვლითი სისტემის რესურსები ნაწილდებოდა მრავალ მომხმარებელზე. ანგარიშ-სწორების ამოცანის ამოხსნის პროცესში მომხმარებლის მონაწილეობის მიხედვით კომპიუტერის მუშაობის რეჟიმები იყოფა პაკეტურ და დიალოგურ რეჟიმებად. პაკეტურ რეჟიმში გადაწყვეტილ ეკონომიკურ ამოცანებს გააჩნიათ შემდეგი თავისებურებები:

- ამოცანის გადაწყვეტის ალგორითმი ფორმალიზებულია და მისი გადაწყვეტა არ მოითხოვს ადამიანის ჩარევას;
- გააჩნია დიდი მოცულობის შემავალი და საშედეგო მონაცემები, რომელთა დიდი ნაწილი განლაგებულია მაგნიტურ მატარებლებზე;
- ამოცანის გადაწყვეტა მოითხოვს დიდ დროს, რაც განპირობებულია მონაცემების დიდი მოცულობით;
- ეკონომიკური ამოცანებისათვის დამახასიათებელია რეგლამენტურობა, ანუ ამოცანების გადაწყვეტა წარმოებს დადგენილი პერიოდულობით.

პაკეტური რეჟიმის გამოყენება შესაძლებლობას იძლევა, შემცირდეს ადამიანის ჩარევა ამოცანის გადაწყვეტის პროცესში. დიალოგურ რეჟიმში ამოცანის გადაწყვეტისას არ არსებობს მონაცემების დამუშავების ოპერაციების წინასწარ დადგენილი თანმიმდევრობა.

დროის დაყოფის რეჟიმი წარმოადგენს კომპიუტერის რესურსების მომხმარებელთა შორის განაწილების ერთერთ ხერხს. ამ შემთხვევაში კომპიუტერის კრიტიკული რესურსის, პროცესორის დრო იყოფა ქვანტებად და თითოეულ მომხმარებელს თანმიმდევრულად ეძლევა პროცესორული დროის ქვანტი.

დროის დაყოფის სისტემები წარმოადგენენ ონლაინური სისტემების ერთერთი კლასს. ამ შემთხვევაში მომხმარებელს შეუძლია პირდაპირ შეაღწიოს კომპიუტერთან და მართოს პროგრამის შესრულების მიმდინარეობა, დაუსვას კითხვები (მიწოდოს მოთხოვნები) კომპიუტერს, მიიღოს მათზე პასუხები.

ონლაინრეჟიმი ყველაზე ხშირად და მარტივად რეალიზებულია მონაცემების ცენტრალიზებული დამუშავებისას. მონაცემე-

ბის ცენტრალიზებული დამუშავება საჭიროებს ხარისხიან საკომუნიკაციო სისტემის არსებობას, რათა მომხმარებელმა, მიუხედავად მისი დაცილებისა (ეს მანძილი შეიძლება იყოს რამდენიმე ათასი კილომეტრი), შეძლოს კომპიუტერთან კავშირის დამყარება, რეალური ან ვირტუალური კავშირის არხებით.

განსხვავებული ვარიანტია მონაცემების განაწილებული დამუშავება, რომლის დროსაც ერთმანეთის დაშორებული კომპიუტერის მართვა ხორციელდება სხვადასხვა ოპერაციული სისტემების მეშვეობით, მათ შორის კავშირის განხორციელება კი ორგანიზებულია შეტყობინებების გაცვლით, მონაცემთა გადაცემის ქსელის საფუძველზე.

როგორც ერთი, ისე მეორე სისტემისათვის აქტუალურია ტრანზაქციის ცნება. ტრანზაქცია ეს არის პროცესი, რომელიც დაკავშირებულია ერთ ან რამდენიმე ბაზაში ცვლილებების შეტანასთან. ეს ცვლილება არ უნდა განხორციელდეს ნაწილ-ნაწილ. თუ ცვლილება ვერ განხორციელდა სრული მოცულობით მოწყობილობების მუშაობის შეფერხების ან სხვა მიზეზის გამო, მაშინ მონაცემთა ბაზები უნდა დაბრუნდეს საწყის მდგომარეობაში.

ფინანსური ინფორმაციის დამუშავებისას ტრანზაქციის მაგალითს წარმოადგენს საბანკო სისტემაში ერთი ანგარიშიდან მეორე ანგარიშზე რაიმე თანხის გადაგზავნა. ტრანზაქციის მაგალითია აგრეთვე პლასტიკური ბარათით მაღაზიაში ანგარიშსწორებისას კომპიუტერული ავტორიზაციის პროცედურა. მომხმარებელი ბარათს დებს ნამკითხველ მოწყობილობაში, შესაბამისი შეტყობინება მაღაზიიდან გადაეცემა საპროცესინგო ცენტრში, ცენტრალურ კომპიუტერს, რომელიც ასრულებს ტრანზაქციას. წარმოებს მყიდველის ანგარიშის შემოწმება და მყიდველის ანგარიშიდან მოთხოვნილი თანხის გაცემის ნებართვის გაცემა. როდესაც მყიდველი და მოლარე საბოლოოდ მიიღებენ გადაწყვეტილებას შესრულებული ანგარიშსწორების შესახებ, მყიდველის ანგარიშიდან თანხა გაიგზავნება მაღაზიის ანგარიშზე. ამით ტრანზაქცია მთავრდება.

უკანასკნელ პერიოდში „კლიენტ-სერვერულმა“ ტექნოლოგიამ, როგორც პერსპექტიულმა ტექნოლოგიამ, შეცვალა „ფაილ-

სერვერული“ ტექნოლოგია. განვიხილოთ „კლიენტ-სერვერული“ ტექნოლოგიის რეალიზაციის სხვადასხვა ვარიანტი:

- ტექნოლოგია „კლიენტ-სერვერ“ ორიენტირებულია ავტონომიურ კომპიუტერზე, ე.ი. კლიენტი და სერვერი მოთავსებულია ერთ კომპიუტერზე. ფუნქციური შესაძლებლობების მიხედვით, ასეთი სისტემა მონაცემების ცენტრალიზებული დამუშავების ანალოგიურია;

- „კლიენტ-სერვერული“ ტექნოლოგია ორიენტირებულია ცენტრალურ განაწილებაზე. ამ ტექნოლოგიის გამოყენებისას კლიენტს ეძლევა შესაძლებლობა, მიწვდეს ერთ სერვერს, საიდანაც შეიძლება მხოლოდ მონაცემების ნაკითხვა. მონაცემებთან წვდომა რეალიზებულია დაშორებული ტრანზაქციისა და მოთხოვნების საშუალებით. მათი რაოდენობა არ უნდა იყოს დიდი, რათა არ მოხდეს სისტემის მწარმოებლურობის შემცირება;

- „კლიენტ-სერვერული“ ტექნოლოგია ორიენტირებულია ლოკალურ გამოთვლით ქსელზე. ამ ტექნოლოგიას გააჩნია შემდეგი თავისებურებები: ერთ-ერთი სერვერი უზრუნველყოფს ბაზასთან წვდომას. კლიენტი ახდენს პროცესის ფორმირებას. ის პასუხისმგებელია მონაცემების შინაარსობრივ დამუშავებაზე, მათ წარმოდგენასა და ბაზასთან ლოგიკურ წვდომაზე. მონაცემთა ბაზასთან წვდომა შენელებულია, რადგან კლიენტი და სერვერი ერთმანეთთან დაკავშირებული არიან ლოკალური ქსელის საშუალებით;

- „კლიენტ-სერვერული“ ტექნოლოგია ორიენტირებულია მხოლოდ ერთ ბაზაში მონაცემების შეცვლაზე. ამ ტექნოლოგიის გამოყენების შემთხვევაში შესაძლებელი ხდება ტრანზაქციის განაწილებული დამუშავება. დაშორებული სერვერები ერთმანეთთან დაკავშირებულია კომპიუტერული ქსელით. კლიენტს შეუძლია მონაცემები შეცვალოს მხოლოდ საკუთარ ბაზაში. მონაცემების განაწილება წარმოებს დაყოფის მეთოდით;

- „კლიენტ-სერვერული“ ტექნოლოგია ორიენტირებულია მონაცემების რამდენიმე ბაზაში ცვლილებაზე. წინა ტექნოლოგიისაგან განსხვავებით, აქ გვაქვს სერვერ-კორდინატორი, რომელიც ეხმარება ორ სერვერს შორის მონაცემების გადაცემას,

რაც ქმნის მონაცემთა ბაზების მართვის სისტემის შემუშავების ნანამძღვრებს;

- „კლიენტ-სერვერული“ ტექნოლოგია ორიენტირებულია მონაცემთა განაწილებული მართვის სისტემაზე. იგი უზრუნველყოფს დაყოფისა და დუბლირების სტრატეგიას, საშუალებას იძლევა, მონაცემებთან წვდომა განხორციელდეს უფრო სწრაფად. მონაცემთა განაწილებული მართვის სისტემა უზრუნველყოფს, რომ კლიენტი არ იყოს დამოკიდებული სერვერის განთავსების ადგილზე, რათა შესაძლებელი გახდეს ბაზის მთლიანობის განაწილებული კონტროლი და განაწილებული ადინისტრირებული მართვა.

ბანკის ელექტრონული სისტემის ტექნიკური პლატფორმის ამორჩევისას მიზანშეწონილია, მხედველობაში იქნეს მიღებული შემდეგი პარამეტრები:

- კომპიუტერის მწარმოებლობა შესაბამისობაში
- უნდა იყოს სტანდარტულ ტესტებთან;
- დისკური და ოპერატიული მეხსიერების რესურსები;
- უნდა გაგვაჩნდეს ერთიანი ოჯახის პროცესორზე დაფუძნებული კომპიუტერი;
- ტექნიკური პლატფორმის დონეზე რეზერვირების შესაძლებლობა;
- მონაცემები „ფასი / მწარმოებლობა“ და ერთ
- წამში ტრანზაქციის შესრულების რაოდენობა;
- აპარატურული და პროგრამული უზრუნველყოფის დონეზე თავსებადობა (შეძენილი აპარატურული და პროგრამული უზრუნველყოფის თავსებადობა არსებულთან);
- ფირმა-მწარმოებელს უნდა გააჩნდეს სერვისცენტრი და მასში მომსახურების სათანადო პირობები;
- სწავლების ცენტრის არსებობა და მისი ხელმისაწვდომობა ორგანიზაციულად და ფინანსურად;
- ფირმა-მწარმოებლის ტექნიკური და ფინანსური მდგომარეობის სტაბილურობა.

3.3. ტელესაკომუნიკაციო სისტემები

მწარმოებლურობისა და საიმედოობის ამალღების მიზნით, განსაზღვრული ტექნიკური და პროგრამული საშუალებების დახმარებით ავტონომიური კომპიუტერების გაერთიანება ხდება კომპლექსებში.

ქსელი ეწოდება აპარატურულ საშუალებებს, რომლებიც უზრუნველყოფენ აბონენტების ურთიერთდაკავშირებასა და მათ შორის მონაცემების გაცვლას. მონაცემთა გადაცემის ქსელი გამოიყენება ერთმანეთისაგან დაშორებული გამოთვლითი სისტემის ან ტერმინალური მოწყობილობების ერთმანეთთან დაკავშირების მიზნით. ქსელმა უნდა უზრუნველყოს დაშორებული აბონენტების სწრაფი მოძებნა და მათი სწორად შეერთება, სეანსის განმავლობაში კავშირის შენარჩუნება და ინფორმაციის გადაცემის სიზუსტე. ცნობილია ქსელის კავშირის შემდეგი სახეები:

- შიდა ქსელი. ეს ქსელი იყენებს ორწერტილოვან შეერთებას კომპიუტერსა და ტერმინალებს შორის;
- ქსელი, რომელიც იყენებს მოდემს და საკომუტაციო ანალოგიურ არხებს (მაგ., საერთო დანიშნულების სატელეფონო ქსელი), შესაძლებელია ოპერაციების რეზერვირება, ავტომატური გამოძახება და ავტომატური პასუხი;
- ქსელი, რომელიც დაფუძნებულია გამოყოფილი ციფრული არხების გამოყენებაზე;
- ინტეგრირებული მომსახურების ციფრული ქსელი მულტიპლექსურ ბაზაზე დაფუძნებული ქსელი რომელიც იყენებს ანალოგიურ ან ციფრულ არხებსა და მოდემებს;
- პაკეტების კომუტაციის ქსელი;
- ლოკალური ქსელი.

საერთაშორისო და ნაციონალური სტანდარტები ქსელის მოწყობილობებსა და პროგრამულ საშუალებებს უყენებს სხვადასხვა მოთხოვნებს. მოთხოვნები ეხება შემდეგ კომპონენტებს: მოდემებს, მონაცემთა გადაცემისათვის სიმბოლოთა კრებულს (ალფაბეტს), დიალოგს (პროტოკოლს), რომელიც აუცილებელია ქსელში შეტყობინების ან მონაცემთა გადაცემის კოორდინაცი-

სათვის, აგრეთვე, შეცდომებისაგან დაცვას, რომელსაც შეიძლება ადგილი ჰქონდეს ქსელში აღმოცენებული შეფერხებების გამო.

დაკავშირებული ინტერფეისები ერთმანეთისაგან ძირითადად განსხვავდებიან კავშირის დამყარების მეთოდებით, ავტომატურ რეჟიმში მომსახურების სახეებით, შეერთებულ ხაზების მაქსიმალური სიგრძით და მონაცემების გადაცემისა და სისწრაფის მეთოდებით. მაგალითად, ტელეგრაფი უზრუნველყოფს 110-მდე ბიტის, ხოლო ტელექსი 50 ბიტამდე წამში ინფორმაციის გადაცემას.

მოდემი (მოდულატორი/დემოდულატორი) არის მონყობილობა, რომელიც თანმიმდევრულ ციფრულ სიგნალებს გარდაქმნის ანალოგურ სიგნალებად და პირიქით. ზოგიერთ თანამედროვე მოდელებს მონაცემების შესაკუმშად და კავშირის არხების გამტარუნარიანობის შესაძლებლობების სრულად გამოყენებისათვის გააჩნიათ ჩაშენებული მონყობილობა.

საერთო დანიშნულების სატელეფონო ხაზების გამოყენებისას მოდელები უზრუნველყოფენ მონაცემების გადაცემას – 2400, 4800, 9600, 14400 და 19200 ბიტი წამში სიჩქარით. უფრო მწარმოებლური სისტემები აგებულია მულტიპლექსორებზე. მულტიპლექსორული არხის მუშაობა მდგომარეობს იმაში, რომ მაღალი გამტარუნარიანობის ხაზის ერთ ბოლოს მულტიპლექსორი აერთიანებს მონაცემებს, რომელიც შემოვიდა რამდენიმე არხით, ხოლო არხის მეორე ბოლოში სრულდება საპირისპირო პროცესი – მონაცემთა არხების გათიშვა.

ქსელში ინფორმაციის გაცვლის მიზნით შემუშავებულია შეთანხმება, რომელსაც პროტოკოლი ეწოდება. ის განსაზღვრავს გადასაცემი შეტყობინების ტიპს, ფიზიკურ სიგნალებს, დროში მათი თანმიმდევრობით მიღების, გადაცემის და კონტროლის ალგორითმებს, აგრეთვე, სამომსახურო ინფორმაციის შედგენილობას. გავრცელებულია პროტოკოლების რამდენიმე საერთაშორისო სტანდარტი: ტექნიკური საშუალებების, ოპერაციული სისტემების და ტელეკომუნიკაციის პაკეტების.

ქსელებში გამოყენებული კავშირის არხები შეიძლება დავყოთ ორ ჯგუფად – სადენიანი ხაზები და რადიოხაზები.

საკაბელო არხები. საკაბელო არხები – ესაა სადენიანი არხები, რომლებიც დაფარულია საიზოლაციო ფენით და მოთავსებულია დამცავ გარსში. ცნობილია საკაბელო ხაზების ორი ტიპი – სიმეტრიული წყვილები და კოაქსალური კაბელები. სიმეტრიული წყვილი წარმოადგენს სპილენძის დაგრეხილ მავთულს და იზოლირებულია ქაღალდით ან პოლიეთილენით. კაბელში შეიძლება იყოს 20-დან 2000-მდე წყვილი. კოაქსალური კაბელი შედგება წყვილისაგან. მისი პარამეტრებია: სადენის შიდა და გარე დიამეტრი. სიმეტრიულ კაბელთან შედარებით, კოაქსალურ კაბელს გააჩნია მაღალი სიხშირე და კარგად არის დაცული შეფერხებებისაგან. სიმეტრიული და კოაქსალური კაბელების მოხერხებულობა მდგომარეობს იმაში, რომ მათი საშუალებით შეიძლება როგორც ანალოგური, ისე ციფრული ინფორმაციის გადაცემა. ხოლო რაც შეეხება ოპტიკურ-ბოჭკოვან კაბელს, მისი საშუალებით შესაძლებელია მხოლოდ ციფრული ინფორმაციის გადაცემა.

ოპტიკურ-ბოჭკოვანი არხები. ოპტიკურ-ბოჭკოვანი არხების შექმნა განაპირობა დასამუშავებელი ინფორმაციის მოცულობის მნიშვნელოვნად გაზრდამ და მისმა მაღალტექნიკურმა შესაძლებლობებმა.

ოპტიკური ბოჭკო წარმოადგენს კვარცის მინის გამტარს, რომელშიც წარმოებს ინფრანითელი დიაპაზონის სინათლის სხივების გადაცემა. საკაბელო არხებთან შედარებით, ოპტიკურ-ბოჭკოვან არხებს გააჩნიათ შემდეგი უპირატესობები: მცირე მილევადობა, ძალიან დიდი გამტარიანობა (10 გიგაბაიტამდე წამში), კაბელის მცირე მოცულობა, მასა და კარგი ელასტიკურობა; არ გააჩნია ელექტროგამტარიანობა და, როგორც შედეგი, არ საჭიროებს დაცვას ბუნებრივი მოვლენებისაგან (მაგ., ელვა და სხვა ელექტრო-მაგნიტური გამოსხივებები). ოპტიკურ-ბოჭკოვანი არხების გამოყენება მიზანშეწონილია მაშინ, როცა დიდია გადასაცემი ინფორმაციის მოცულობა. თუ გადაცემის სიჩქარე არ იქნება 2 გიგაბაიტი წამში, მაშინ ოპტიკურ-ბოჭკოვანი არხების გამოყენება არახელსაყრელია.

თანამგზავრული არხები. თანამგზავრული კავშირის სისტემებში გამოყენებულია ზესიხშირიანი გამოსხივების დიაპაზონის ანტენები, რომელთა საშუალებითაც წარმოებს მიწისზედა გა-

დამცემი სადგურებიდან გაგზავნილი სიგნალების მიღება და მათი რეტრანსლაცია მიწისზედა სადგურებზე. თანამგზავრული სისტემები მუშაობენ ორ რეჟიმში: პირველ რეჟიმში მუშაობისას გადამცემი სადგურის სიგნალები შეიძლება მიიღოს ნებისმიერმა მიწისზედა სადგურმა, თუ იგი იმყოფება თანამგზავრის მიღების ზონაში. ასეთ რეჟიმს ეწოდება ფართომაუწყებლიანი. მას ძირითადად იყენებენ სატელევიზიო და რადიომაუწყებლობის სისტემებში. მეორე რეჟიმის დროს თითოეული თანამგზავრული არხი მკაცრად არის მიმაგრებული ორ მიწისზედა სადგურთან. დანარჩენ სადგურებს არ შეუძლიათ მიიღონ ამ თანამგზავრის სიგნალები. თანამგზავრული არხების მთავარ თავისებურება ისაა, რომ მონაცემების გადასაცემად საჭიროა დიდი დრო. კავშირის აღნიშნულ არხს თან ახლავს კონფიდენციალურობის უზრუნველყოფის პრობლემები, რამდენადაც, შესაძლებელია, სიგნალები დაიჭიროს არალეგალურმა სადგურებმა. თანამგზავრული არხების ღირსებას წარმოადგენს მაღალი გამტარიანობა. სიგნალის გადაცემის ღირებულება არ არის დამოკიდებული ორ სადგურს შორის არსებულ მანძილზე.

რადიორელური არხები. რადიორელური გადამცემი ხაზის გარემოს წარმოადგენს თავისუფალი სივრცე. გადამცემიდან მიმღებამდე მთელ მანძილზე ხდება რეტრანსლაციის ანძების დაყენება ისე, რომ ორი მეზობელი ანძა იყოს რადიომხედველობის პირდაპირ ზონაში. ამიტომ მათ შორის მანძილი დამოკიდებულია კონკრეტულ რელიეფზე და შეიძლება იყოს 30-დან 50 კილომეტრამდე. ასეთ კავშირზე გარკვეული ზომით ზემოქმედება შეუძლია ბუნებრივ პირობებს, რასაც თან სდევს ინფორმაციის გადაცემისას ძლიერი შეფერხებები, დაბალი სიჩქარე და არამდგრადი მუშაობა.

3.4. ბანკომატი, როგორც ელექტრონული გადახდების სისტემის ელემენტი

ბანკომატი (ATM) automated teller mashine) არის საბანკო ავტომატი, რომლის დანიშნულებაცაა ბანკის პერსონალის გარეშე კლიენტების მომსახურება. ყველაზე ხშირად ბანკომატს იყენებ-

დნენ ნაღდი ფულის გასაცემად. გარდა აღნიშნულისა, დღეს ბანკომატს შეუძლია შეასრულოს შემდეგი ფუნქციები:

- ნაღდი ფულის გაცემა და მიღება;
- ბარათის ნომრის გამოყენებით თანხების გადარიცხვა;
- კომუნალური გადასახადების, ჯარიმების და სხვადასხვა მომსახურების გადახდა;
- გადარიცხვები პლასტიკურ ბარათებზე და საბანკო ანგარიშებზე და სხვ. ვალუტის შეძენა;
- ინტერნეტბანკთან დაკავშირება.
- ნებისმიერი ოპერაციის დასადასტურებლად საჭიროა მხოლოდ 1 კოდი; არაა საჭირო პასპორტის მონაცემების ან სხვა დოკუმენტების დეტალების შეყვანა [5].

პირველად ბანკომატის გამოყენება დაიწყო 1962 წლიდან, ნაღდი ფულის შედარებით მცირე თანხის გასაცემად. ბანკომატის ფართო გამოყენება იწყება 1980-იანი წლებიდან. დღეისათვის ამ მოწყობილობას ფართო გამოყენება აქვს მოსახლეობის საბანკო მომსახურებაში. ბანკომატები შესაძლებლობის მიხედვით იყოფიან როგორც უნივერსალური (სრულფუნქციური) და სპეციალიზებული. ამ უკანასკნელის გამოყენება წარმოებს ნაღდი ფულის გასაცემად. ამ შემთხვევაში მისი სისწრაფეა ერთი ოპერაცია 15 წამში. ბანკომატებს, რომლებიც გამოიყენებიან საცნობარო-საინფორმაციო მომსახურებისათვის, „საინფორმაციო ჯიხურებს უწოდებენ“. ბოლო თაობის ბანკომატებს შეუძლიათ სხვადასხვა ფუნქციის შესრულება.

მოქმედების ავტონომიურობის მიხედვით, საბანკო ავტომატები შეიძლება დავეყოს როგორც მარტივი, საბოლოო მოწყობილობა, რომელიც ღებულობს დაკვეთებს და აფორმებს ცენტრალური კომპიუტერის მიერ შესრულებულ საბანკო ოპერაციების შედეგებს და ბანკომატები, რომლებსაც გააჩნიათ ფუნქციური დამოუკიდებლობა და მაღალი ავტომატიზაციის დონე, რომელიც ცენტრალური კომპიუტერიდან ღებულობს ნებართვას ოპერაციის ავტონომიურად შესრულების შესახებ.

დღეისათვის ბანკომატის მთავარ ფუნქციას წარმოადგენს ანგარიშიდან ნაღდი ფულის მოხსნა. იმისათვის, რომ კლიენტმა

ბანკომატის საშუალებით მიიღოს ნაღდი ფული, მან ქვემოთ ჩამოთვლილი თანმიმდევრობით უნდა შეასრულოს შემდეგი ოპერაციები:

- კლიენტი ბარათს ათავსებს ბანკომატის მიმღებ მონყობილობაში;

- კლიენტისათვის ბანკომატს ეკრანზე გამოაქვს შეტყობინება რათა მან შეიტანოს პერსონალური საიდენტიფიკაციო ნომერი (PIN-კოდი);

- კლიენტი კლავიატურაზე აკრეფს PIN-კოდს;

- ბანკომატი კითხულობს ბარათზე არსებულ ინფორმაციას და ამოწმებს შეესაბამება თუ არა აკრეფილი PIN-კოდი ბარათიდან ნაკითხულს. აგრეთვე ამოწმებს, არის თუ არა ეს ბარათი შეტანილი გაუქმებულ და ძალადაკარგულ ბარათთა სიაში;

- თუ ყველაფერი წესრიგშია, მაშინ ბანკომატი ეკრანზე გამოიტანს შეტყობინებას, კლიენტმა შეიტანოს (დააფიქსიროს) თანხის ის რაოდენობა, რომლის გამოტანაც სურს ნაღდი ფულის სახით;

- კლიენტი აკრეფს საჭირო თანხის რაოდენობას;

- ბანკომატი ამოწმებს, ხომ არ აღემატება კლიენტის მიერ მოთხოვნილი თანხა, მოცემულ საგადასხდელო სისტემაში დადგენილ ლიმიტს;

- თუ ყველაფერი წესრიგშია, ავტომატი გადათვლის საჭირო თანხას და ნაღდი ფულის გამომტანი მონყობილობის საშუალებით გამოიტანს მას;

- ბანკომატი კლიენტს უბრუნებს ბარათს.

რა თქმა უნდა, ზემოთ აღწერილი არის გამარტივებული ჩამონათვალი იმ მოქმედებებისა, რომელსაც ასრულებს ბანკომატი კლიენტის მომსახურებისას. მაგალითად, სადებეტო ბარათის გამოყენების შემთხვევაში, ბანკომატმა უნდა შეამოწმოს, ხომ არ აღემატება კლიენტის მიერ მოთხოვნილი თანხა მის საბარათო ანგარიშზე არსებულ ნაშთს. არსებობს აგრეთვე მულტიბარათული ბანკომატები, რომლებსაც შეუძლიათ მოემსახურონ სხვადასხვა საგადასხდელო სისტემის ბარათებს. გარდა აღნიშნულისა, კლიენტის მოთხოვნით, ბანკომატს შეუძლია დაბეჭდოს ქვი-

თარი, რომელიც ადასტურებს შესრულებულ ტრანზაქციას. ბეჭ-
დვა ხორციელდება კლიენტის მოთხოვნით, რისთვისაც კლიენ-
ტმა მენიუდან უნდა აარჩიოს შესაბამისი პუნქტი და დააჭიროს
თითი შესაბამის ლილაკს.

ზოგიერთი შემთხვევაში ჩამოთვლილი მოქმედების შესრულება
მოითხოვს ინფორმაციის გაცვლას ცენტრსა და ბანკომატს შო-
რის. კერძოდ, ეს საჭიროა კლიენტის საბარათო ანგარიშზე ნაშ-
თის, ბარათის ნომრისა და PIN-კოდის შესაბამისობისა და საკრე-
დიტო ბარათის მიხედვით ლიმიტით თანხის გაცემის შესამოწ-
მებლად.

ასეთი კავშირი აუცილებელია აგრეთვე კლიენტისათვის მისი
ანგარიშის მდგომარეობის შესახებ ინფორმაციის მისაწოდებ-
ლად და ამ მონაცემების დასაბეჭდად. ჩამოთვლილი ოპერაციე-
ბის შესრულებისათვის აუცილებელი ხდება ინფორმაციის გაც-
ვლა კლიენტსა და საგადასახდელ სისტემას შორის.

ონლაინრეჟიმში (რეალური დროის რეჟიმი) ბანკომატი მუდ-
მივად მიერთებულია საპროცესინგო ცენტრთან. ინფორმაციის
გაცვლა საპროცესინგო ცენტრსა და ბანკომატს შორის წარმო-
ებს უწყვეტად. ამ შემთხვევაში კლიენტის შესახებ ყველა მონა-
ცემი (ფულადი საშუალებების მოძრაობა, ნაშთი მის ანგარიშზე)
იმყოფება საპროცესინგო ცენტრში. საპროცესინგო ცენტრის
მიერ საბარათო ანგარიშზე ყველა ოპერაცია სრულდება რეალუ-
რი დროის რეჟიმში.

ოფლაინრეჟიმში (ავტონომიური რეჟიმი) ბანკომატს კავში-
რი არა აქვს საპროცესინგო ცენტრთან და მონაცემთა გაცვლა
მათ შორის ხორციელდება ხანგრძლივი ინტერვალით, მაგნიტურ
მატარებლებზე ინფორმაციის გადატანით. კლიენტის შესახებ ინ-
ფორმაცია (ფულადი საშუალებების მოძრაობა, ნაშთი საბარათო
ანგარიშზე) ინახება ბანკომატში. საბარათო ანგარიშზე განხორ-
ციელებული ტრანზაქცია აგრეთვე ინახება ბანკომატში. ინფორ-
მაცია ერთი დღე-ღამის შემდეგ გადაეცემა საპროცესინგო ცენ-
ტრს და იქ ხდება ამ ტრანზაქციის დამუშავება პაკეტურ რეჟიმში
და კლიენტის საბარათო ანგარიშის ნაშთის კორექტირება.

კვაზიონლაინრეჟიმში ბანკომატი კავშირის არხების საშუა-
ლებით უკავშირდება საპროცესინგო ცენტრს, მაგრამ ეს კავშირი

არ არის უწყვეტი. ეს კავშირი ხორციელდება წინასწარ შედგენილი განრიგის მიხედვით. იმაზე დამოკიდებულებით, თუ როგორ არის ეს კავშირი ორგანიზებული, განასხვავებენ სისტემებს ბანკომატიდან საპროცესინგო ცენტრში დარეკვით ან საპროცესინგო ცენტრიდან ბანკომატში დარეკვით. შესაძლებელია, ეს კავშირი შედგეს, ყოველ ერთ ან ორ საათში, ან კიდევ საჭიროების მიხედვით – მაგ., ტრანზაქციის განხორციელების მომენტისათვის.

ოფლაინრეჟიმში შემოწმება წარმოებს ბანკომატის ავტონომიური ბაზის გამოყენებით, რაც გარკვეულწილად ზღუდვას შემოწმების დიაპაზონს. კერძოდ, ტექნიკურად რამდენადაა შესაძლებელი ყველა კლიენტის საბარათო ანგარიშების ნაშთების შენახვა. ამ შემთხვევაში, გამომდინარე ბანკომატის მომსახურების დროის შუალედის ხანგრძლივობიდან (ბანკომატის მუშაობის შემოწმება, ნაღდი ფულის ჩატვირთვა), დანესებულია თანხის მოხსნის ლიმიტი, თუ ეს ლიმიტი არ აღემატება კლიენტის ანგარიშზე არსებულ ნაშთს, მაშინ ტრანზაქცია განხორციელდება.

სმარტ-ბარათების გამოყენების შემთხვევაში, მაგნიტურზოლიანი ბარათების გამოყენებისაგან განსხვავებით, ოფლაინ რეჟიმში არ ადებს რაიმე სერიოზულ შეზღუდვებს, რადგან ინფორმაცია მიმდინარე ნაშთისა და ინდივიდუალური ლიმიტის შესახებ მოთავსებულია კლიენტის ბარათზე. ფაქტობრივად, ამ შემთხვევაში აუცილებელია ბანკომატში ინახებოდეს მხოლოდ „სტოპ-ფურცელი“, რომლის დროული განახლება სისტემის უსაფრთხოებისთვის იმდენად კრიტიკული არ არის, რამდენადაც საბარათო ანგარიშის მდგომარეობის შესახებ ინფორმაციის დროული განახლება.

ავტონომიური რეჟიმის უპირატესობას წარმოადგენს მისი შედარებითი სიიაფე და კავშირის არხებისაგან დამოუკიდებლობა. თუმცა აღსანიშნავია, რომ დანადგარის დაბალი ღირებულება განაპირობებს ამ მოწყობილობის მომსახურების მაღალ ღირებულებას. იმისათვის, რომ „სტოპ-ფურცლის“ შესახებ ინფორმაცია იყოს აქტიურ მდგომარეობაში, აუცილებელია დღე-ღამის განმავლობაში მოწყობილობების განთავსების წერტილების შემოვლა--დათვალიერება და ინფორმაციის განახლება. ბევრი ბანკომატის ფუნქციონირების შემთხვევაში ამის გაკეთება გაძნელებულია.

აღნიშნული შემოვლა თუ არ განხორციელდა, ამან შეიძლება დიდი ზიანი მიაყენოს ბანკს. მაგ., პროგრამა **POLISCARD**-ის კრახის მიზეზად სპეციალისტები მიიჩნევენ, ბანკომანტების ოფლაინრეჟიმში მუშაობას – დროულად არ ხდებოდა მათი შევსება ნაღდი ფულით, რის გამოც კლიენტები ბანკომატს აღიქვამდნენ, როგორც ლითონის სალაროს, და ცდილობდნენ საბარათო ანგარიშიდან ფულის მთლიანად მოხსნას და მის ბანკში გადატანას.

მიუხედავად სიძვირისა, დროის რეალურ რეჟიმს ავტონომიურთან შედარებით გააჩნია უპირატესობა. ეს რეჟიმი მომხმარებელს საშუალებას აძლევს, ბანკომატის საშუალებით არა მარტო მიიღოს ნაღდი ფული, არამედ საბარათო ანგარიშზე განახორციელოს მანიპულაციებიც. დღეისათვის ფართოდაა გავრცელებული ბანკომატების ქსელში გაერთიანება. ქსელში ბანკომატების გაერთიანება ემსახურება შემდეგ მიზნებს:

ოპერაციის ღირებულების შემცირებას; კლიენტისათვის მოხერხებული გარემოს შექმნას (კლიენტს შეუძლია ქსელში ჩართული სხვადასხვა ბანკის ბანკომატით ნაღდი ფულის გამოტანა).

რადგან ბანკომატი არის მომსახურების საშუალება, იგი უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

- მართვა უნდა იყოს ცხადი და მარტივი. მომხმარებელს არ უნდა დასჭირდეს სპეციალური მომზადება ბანკომატის წარმატებით გამოყენებისათვის;

- ბანკომატი უნდა იყოს საიმედო და მუშა მდგომარეობაში. მოწყობილობის გაუმართაობის ან ტექნიკური შეფერხებების გამო, მომხმარებელმა არ უნდა მიიღოს უარი მოთხოვნილი ოპერაციის შესრულებისას;

- ბანკომატი უნდა იყოს უსაფრთხო და დაცული. მომხმარებელი დაცული უნდა იყოს მისი PIN-კოდის კონფიდენციალურობის დარღვევისაგან. ბანკი დაცული უნდა იყოს ყოველგვარი უსიამოვნებისაგან: ყალბი ბარათით

- სარგებლობა, თაღლითობა, გატეხვა. ავარიისა და სტიქიური უბედურების შემთხვევაში მასში მოთავსებული ნაღდი ფულის დაცვა;

- მისი ექსპლუატაციის ღირებულება უნდა იყოს დაბალი. ბანკომატის შენახვისა და მომსახურების ხარჯები უნდა იყოს რაც შეიძლება დაბალი, წინააღმდეგ შემთხვევაში ბანკისათვის არ იქნება ხელსაყრელი ბანკომატების დამონტაჟება და ქსელში განთავსება. იმისათვის, რომ საბარათო საგადამხდელო სისტემა იყოს მომგებიანი, საჭიროა ბანკომატების რამდენიმე წერტილში განლაგება. ბანკომატების მწარმოებელი ფირმებია: IBM, NCR, Olivetti, BULL, Siemens Nixdorf და სხვ.

ბანკომატების მწარმოებელი ფირმები დიდ ყურადღებას უთმობენ მათ დიზაინს. მაგ., იგი კარგად უნდა შეეხამებოდეს საერთო ინტერიერს და მოხერხებული იყოს მისი გამოყენება ფიზიკური ნაკლის მქონე მომხმარებლისათვის.

როგორი დიდი ტევადობისაც არ უნდა იყოს ბანკომატის კასეტები, მათში მოთავსებული ბანკნოტები შედარებით ჩქარა იხარჯება და საჭიროა მათი დროული შევსება. სასურველია, ცარიელი კასეტების „დატენვა“ განხორციელდეს ბანკში და დღეში ერთხელ შეიცვალოს ბანკომატში არსებული დაცარიელებული კასეტები, შევსებულით. ბანკომატში მოთავსებული ფულის რაოდენობა არ უნდა იყოს დიდი, ვინაიდან აღნიშნული თანხა მიმოქცევიდან გამოთიშულია, ანუ არ არის სასურველი ბანკომატში კუპიურების დიდი მარაგის მოთავსება [6].

3.5. ნაღდ ფულთან მომუშავე სხვა მოწყობილობები

ერთ-ერთი მოწყობილობა, რომელიც მუშაობს ნაღდი ფულის გამოყენებაზე, არის სალაროს მოწყობილობა „ელექტრონული მოლარე“-TCD (Teller Cash Dispenser).

ბანკში TCD-ს ამონტაჟებენ ოპერაციონისტის სამუშაო ადგილას. TCD-ის დანიშნულებაა ოპერაციონისტის მითითების მიხედვით ფულის გაცემა, შენახვა, ნომინალის მიღება, დათვლა, დახარისხება და სალაროში შემოსული დაზიანებული ან ყალბი ფულის ამორჩევა. TCD-ის გამოყენება ბანკს აძლევს მთელ რიგ უპირატესობებს: ადამიანისეული რესურსების შემცირება, მუშა-

ობის უსაფრთხოების ამაღლება. ასეთი მონყობილობის გამოყენება აუქმებს ოპერაციონისტის თანამდებობას. აღარ არის საჭირო ისეთი ოპერაციების ხელით შესრულება, როგორიცაა: ფულის გადათვლა, კუპიურების დახარისხება. ამ დროს მაღლდება ოპერაციების შესრულების სიზუსტე, მცირდება ისეთი კუპიურების მიღების ალბათობა, რომლებსაც დაკარგული აქვთ საგადამხდელო თვისებები (ფიზიკურად დაზიანებული კუპიურები). ამ მონყობილობის გამოყენების შემთხვევაში ბანკის პერსონალის ყურადღება გადატანილია კლიენტის მომსახურების ხარისხის გაუმჯობესებაზე. აღნიშნული მონყობილობის გამოყენება ამცირებს მომსახურების დროს, რაც საბოლოოდ ამაღლებს ბანკის კონკურენტუნარიანობას. უმჯობესდება ნაღდ ფულზე შესრულებული ოპერაციების კონტროლი, რაც მიიღწევა ფულადი საშუალებების მიღების ან გაცემის თითოეული ფაქტის ავტომატური რეგისტრაციით.

სალაროს მონყობილობა წარმოადგენს სეიფ-ყუთს, რომელსაც კუპიურების მისაწოდებლად აქვს ოთხი ან ექვსი კასეტა სხვადასხვა ნომინალის კუპიურებისათვის, ორი ან ოთხი კასეტა ნაღდი ფულის მისაღებად და ერთი კასეტა დაწუნებული კუპიურებისათვის. მონყობილობა მუშაობს ბანკის ავტომატიზებული სისტემის მართვის ქვეშ, რაც გამორიცხავს „ხელით“ ფულის გაცემის შესაძლებლობას. აღნიშნული მონყობილობის ღირებულება რამდენიმე ათასი დოლარია.

გაცილებით უფრო რთული მონყობილობაა ვალუტის გაცვლის მონყობილობა. ასეთი ავტომატების დაყენება წარმოებს რკინიგზის სადგურებში, აეროპორტებში, სუპერმარკეტებში და ა.შ. ის მუშაობს დღე-ღამის განმავლობაში პერსონალის მონაწილეობის გარეშე. ვალუტის გაცვლისას მომხმარებელს არ სჭირდება რაიმე დოკუმენტის წარდგენა (ჩვეულებრივ ბანკში აღნიშნული ოპერაციის შესასრულებლად საჭიროა პირადობის მოწმობის წარდგენა). ასეთ ავტომატს შეუძლია არა მარტო ეროვნული ვალუტის გადაცვლა 20-მდე სხვადასხვა ვალუტაზე, არამედ – დადგენილი კურსის მიხედვით მის მეხსიერებაში ჩატვირთული ვალუტების ერთიმეორეზე გადაცვლა.

ონლაინრეჟიმში ვალუტის კურსის შეცვლა წარმოებს ავტომატურად. გათვალისწინებულია დადგენილი საკომისიო მოსაკრებელი. სხვადასხვა ღირებულების კუპიურების შესანახად ავტომატი იყენებს „ინტელექტუალურ“ კასეტებს. ასეთი კასეტების გახსნა შესაძლებელია მხოლოდ სპეციალური მოწყობილობის გამოყენებით, რაც ფულის შენახვის დამატებითი გარანტიაა. იდენტიფიკაციისათვის თითოეულ კასეტას გააჩნია ელექტრონული ბლოკი. ეს ბლოკი ავტომატურად ითვლის კასეტაში დარჩენილი კუპიურების რაოდენობას. ვალუტის გადაცვლის მოწყობილობა მუშაობს 24 საათის განმავლობაში, არ თაღლითობს, არ ურევს აღრიცხვიანობას, არ მალავს ამონაგებს. ასეთი ავტომატები გათვალისწინებულია საშუალო და გაცვეთილი კუპიურების გადასაცვლელად, ამიტომ ზოგჯერ ავტომატი არ ღებულობს აბსოლუტურად ტკაცუნა კუპიურებს. გაცვლის სიზუსტის უზრუნველყოფის მიზნით, ავტომატი აღჭურვილია მონეტების ყუთით.

გარდა სპეციალიზებული მოწყობილობებისა, გამოშვებულია და ბანკებში ფართოდ გამოიყენება მრავალფუნქციური თვითმომსახურების მოწყობილობები. ასეთი მოწყობილობების ფუნქციური შესაძლებლობები დამოკიდებულია მასზე დაყენებულ მოწყობილობებსა და გამოყენებით პროგრამულ უზრუნველყოფაზე. მას დამოუკიდებლად შეუძლია გადახდის, ოპერაციების შესრულება, როგორც მაგნიტური, ასევე ელექტრონული ბარათების ან კიდევ ნაღდი ფულის საშუალებით (მაგ., კომუნალური გადასახადების გადახდა); ვალუტის გადაცვლა, საბარათო ანგარიშიდან ნაღდი ფულის მიღება, საცნობარო ინფორმაციის გაცემა, შეტონების გაყიდვა ნაღდ ფულზე. ასეთი ავტომატების ღირებულება დაახლოებით 90000 დოლარს შეადგენს. ბანკოტების ამოსაცნობად გამოიყენება ფირმა **De La Rue**-ს მიერ გამოშვებული მოწყობილობა.

ბანკომატების, „ელექტრონული მოლარის“ და ვალუტის გაცვლის მოწყობილობების „დასატენად“ გამოიყენება სპეციალური მოწყობილობები, რომლებსაც შეუძლიათ ნაღდი ფულის დახარისხება, გადათვლა, დანულებული, უვარგისი (ფიზიკურად გაცვეთილი ან ყალბი) კუპიურების ჩალაგება სპეციალურ ჯიბე-

ში. ერთ-ერთი ასეთი მონყოილობაა **Innomat**-ი, რომელიც შემუშავებულია ფირმა **De La Rue**-ს მიერ. ამის მსგავსი მონყოილობების გამოყენება ათავისუფლებს ბანკის თანამშრომლებს ფულის მასის ხელით გადათვლისაგან. **Innomat**-ის დაყენება შესაძლებელია არა მარტო ბანკებში, არამედ იმ დაწესებულებებშიც, სადაც ხდება ფულის დიდი მასის დაგროვება (მსხვილი მარკეტები, რკინიგზის სალაროები, აეროპორტები და ა. შ.). **Innomat**-ით ხდება კუპიურების შეფუთვა კასეტებში. „დატენილი“ კასეტები შემდეგ იგზავნება ბანკებში. ბანკები დატენილ კასეტებს ათავსებენ თვითმომსახურების მონყოილობებში. ასე წარმოებს ნაღდი ფულის ბრუნვა. ერთი კასეტის ტევადობაა 2500 ერთნაირი ნომინალის ბანკნოტი. თუ ბანკი თვითმომსახურების ყველა მონყოილობას ტელესაკომუნიკაციო სისტემაში გაერთიანებას, მაშინ მას ავტომატიზებული სისტემის მეშვეობით შეუძლია მიიღოს ინფორმაცია, სად და რომელ მონყოილობაში რა რაოდენობის ნაღდი ფული იმყოფება. აღნიშნული საშუალებას იძლევა, ოპერატიულად განხორციელდეს ფულის ინკასაცია. ამ მომენტში ინკასატორები ფულს ფიზიკურად ვერ ხედავენ, ისინი უზრუნველყოფენ მხოლოდ კასეტების გადატანას.

აღრიცხვისა და კონტროლის კასეტური სისტემის დანერგვა ამცირებს ნაღდი ფულის მიმოქცევასთან დაკავშირებულ დანახარჯებს. არსებული ტექნოლოგიის პირობებში ნაღდი ფულის მიმოქცევისათვის საჭიროა ერთ ციკლში შესრულდეს 20-მდე დათვლისა და შემოწმების ოპერაცია.

ამრიგად, დღეისათვის ბაზარზე მიმოქცევაშია მთელი რიგი მონყოილობები, რომელთა გამოყენებაც ბანკს საშუალებას აძლევს, შეამციროს ნაღდი ფულთან ფიზიკურ კონტაქტში მყოფი პერსონალის რაოდენობა. საბოლოოდ ადგილი აქვს აღრიცხვის საიმედოობისა და სიზუსტის გაზრდას, კლიენტებთან ურთიერთობის პროცესის შემსუბუქებას, ბანკის მუშაობის ეფექტიანობის ამაღლებას.

კითხვები თვითშემოწმებისთვის

1. რა სახის ავტომატიზებული საინფორმაციო სისტემები გამოიყენება ბანკში?
2. რა რეჟიმებში შეუძლია კომპიუტერს მუშაობა?
3. დაახასიათეთ ინფორმაციის გადაცემის არხები.
4. რას წარმოადგენს ბანკომატი და რა ფუნქციების შესრულება შეუძლიათ თანამედროვე ბანკომატებს?
5. დაახასიათეთ ნაღდ ფულთან მომუშავე მოწყობილობები („ელექტრონული მოლარე“ – TCD, ფულის გადაცვლის მოწყობილობა – Innomat).

თავი 4. ბანკის ავტომატიზებული სამუშაო ადგილების სტრუქტურა და მათი კავშირი ბანკის საინფორმაციო სისტემასთან

4.1. ბანკის ავტომატიზებული სამუშაო ადგილების სტრუქტურა

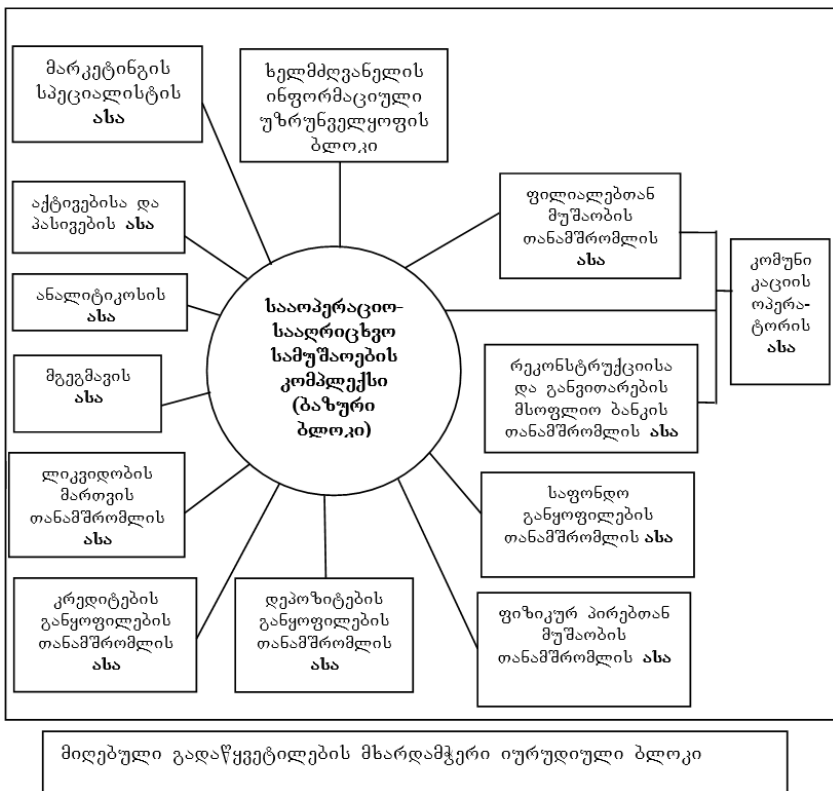
კლიენტის ბანკთან ურთიერთობის ტელესაკომუნიკაციო სისტემა (კლიენტი-ბანკი) საშუალებას იძლევა, შემცირდეს კლიენტის ბანკში ვიზიტების რაოდენობა, გამარტივდეს ბუღალტრული აღრიცხვის წარმოება. სისტემა უზრუნველყოფს, რომ კლიენტმა მოამზადოს სხვადასხვა საგადამხდელო დოკუმენტები და გადაგზავნოს ბანკში, მიიღოს პირადი ანგარიშიდან ამონაწერი, გადახდების რეესტრი და სხვ. კლიენტი-ბანკის სისტემა დაკავშირებულია საოპერაციო-სააღრიცხვო ბლოკთან (ბაზური ბლოკი), რომელიც უზრუნველყოფს საგადამხდელო დოკუმენტების დამუშავებას და აუცილებელი გამომავალი დოკუმენტების ფორმირებას.

კომუნიკაციის ავტომატიზებული სამუშაო ადგილი (ასა) უზრუნველყოფს სერვერთან შეღწევის კონტროლს, აბონენტის იდენტიფიკაციას, სეანსის გასაღების ფორმირებას, სეანსის მხარდაჭერას, სისტემური ჟურნალის წარმოებას, კლიენტების გასაღებების მონაცემთა ბაზის წარმოებას. იგი ახორციელებს გარე სამყაროსთან კავშირს, უზრუნველყოფს შეტყობინების ავტომატურ გადაცემას კლიენტსა და ბანკს შორის, ბანკსა და საკრილინგო ცენტრს შორის, ბანკებს შორის, ბანკსა და მის ფილიალებს შორის, ბანკსა და ვალუტის გაცვლის პუნქტებს შორის. კომუნიკაციების ასა ახდენს საგადამხდელო დოკუმენტებს მიღებას, ახორციელებს მათ ამოცნობას და გადაცემს საოპერაციო-სააღრიცხვო სამუშაოთა ბლოკს, სადაც შემოწმების შემდეგ განისაზღვრება იმ ოპერაციონისტის ნომერი, რომელიც კურირებს მოცემულ კლიენტს, ელექტრონული ხელმოწერის ალგორითმის დახმარებით გაშიფრავს შეტყობინებას.

ოპერაციონისტი, დაათვალიერებს რა შემოსულ დოკუმენტებს, გადაგზავნის შესასრულებლად ან უარს ამბობს სამუშაოს შესრულებაზე და მიუთითებს უარის მიზეზს. დოკუმენტი უბრუნდება კლიენტს. ზოგიერთ შემთხვევაში ოპერაციონისტი შემოსულ დო-

კუმენტს გადაუგზავნის ხელმძღვანელის ასა-ს, გადაწყვეტილების მისაღებად [7].

ბანკის ინტეგრირებული სისტემა შედგება სხვადასხვა ავტომატიზებული სამუშაო ადგილებისა და ბლოკების პროგრამული პოდუქტებისაგან (სურ.4.1.). ბანკის ინტეგრირებულ სისტემაში ასა-ის სრულფასოვანი მართვის მიზნით, დავახასიათოთ ბანკის ინტეგრირებული სისტემის ძირითადი ასა-ბი და ბლოკები.



სურ.4.1. ბანკის ინტეგრირებული საინფორმაციო სისტემის სტრუქტურა

სადეპოზიტო განყოფილების თანამშრომლის ასა უზრუნველყოფს დროებით თავისუფალი თანხების მოზიდვას. საგნობრივი ტექნოლოგიის მიმართებაში სადეპოზიტო **ასა** მოიცავს კრედიტების განყოფილების **ასა**-ის მსგავს ტექნოლოგიას: ხელშეკრულების დადება, სხვადასხვა სქემით პროცენტის გაანგარიშება, წინა ნაშთის კორექტირება და სხვ.

ფონდების პორტფელის ასა მოიცავს შემდეგ რეჟიმებს: საინვესტიციო ობიექტის ეკონომიკური მდგომარეობის შეფასება; ფასიანი ქაღალდების ანალიზური მაჩვენებლების გაანგარიშება; ობიექტის ფასიანი ქაღალდების საიმედოობის (მიმზიდველობის) შეფასება; ფასიანი ქაღალდების შემოსავლისა და მოძრაობის აღრიცხვა. ბანკის ტექნოლოგიის პრობლემას წარმოადგენს ფუნქციების გამიჯვნა ბაზურ მოდულსა და სხვა განყოფილებების **ასა**-ს შორის.

მაგ., დღეისათვის კრედიტებზე პროცენტების დარიცხვის ორი მეთოდია გავრცელებული. პირველი მეთოდის მიხედვით პროცენტის დარიცხვას აწარმოებს ბაზური მოდული, საკრედიტო განყოფილების თანამშრომლები ამ განყოფილებას აწვდიან პროცენტის გასაანგარიშებლად საჭირო ინფორმაციას, ხოლო საკრედიტო განყოფილების თანამშრომლები ახორციელებენ გადახდების გრაფიკის შესრულებისა და მათგან გადახრების კონტროლს. მეორე ტექნოლოგიით ამ განყოფილებებს შორის კავშირის განხორციელება წარმოებს ოპერაციების გატარებების დონეზე. საკრედიტო განყოფილების თანამშრომელი ახდენს მათ გენერაციას, ხოლო სააღრიცხვო-საოპერაციო სამუშაოების მოდული აწარმოებს საკრედიტო ანგარიშებს, ანგარიშების მიხედვით სამუშაოების დათვალიერებას, კრედიტების მიხედვით პროცენტების გაანგარიშებას. დადებული ხელშეკრულებების დოკუმენტების კონტროლი ხორციელდება საკრედიტო და სადეპოზიტო განყოფილებებში.

ავტომატიზებული სამუშაო ადგილების მუშაობა კონსტრუქციულად აგებულია მთელი რიგი უნივერსალური ბლოკების საფუძველზე.

ეს ბლოკებია: ხელშეკრულების, გადახდის გრაფიკის, ბანკის ნორმატივების კოეფიციენტების გაანგარიშების, კლიენტების

კრედიტუნარიანობის შეფასების, ბანკის თავისუფალი საშუალებების პროგნოზის.

ხელშეკრულებების ბლოკი უზრუნველყოფს ხელშეკრულებების მომზადებას, წარმოებას, აღრიცხვასა და ხელშეკრულების შესრულების კონტროლს, ბანკის ლიკვიდობის კოეფიციენტების გაანგარიშებას, კრედიტებისა და დეპოზიტების თანხების გაანგარიშებას, მოცემული მომენტისათვის ბანკის რესურსების მდგომარეობის პროგნოზს, შემოთავაზებული ხელშეკრულების ბანკის ფინანსურ მდგომარეობაზე ზემოქმედების პროგნოზს. ეს ბლოკი საშუალებას იძლევა, მივიღოთ ამონაწერი თითოეული ხელშეკრულების მდგომარეობის შესახებ და კრებსითი საანგარიშგებო დოკუმენტები,

გადახდების გრაფიკის ბლოკი საშუალებას იძლევა, კრედიტების დაფარვისა და დეპოზიტების გადახდის შესახებ მოხდეს სავარაუდო ვარიანტების გაანგარიშება, სესხის გაცემისას შედგეს პროცენტების გადახდის გრაფიკი, ხელშეკრულების დამთავრების ბოლოსათვის კრედიტის ერთდროულად დაფარვის გრაფიკი და სხვ.

ბანკის ნორმატივების გაანგარიშების ბლოკი უზრუნველყოფს ბანკის სისტემის მდგრადობას. ამ ბლოკში მოცემულია ნორმატიული კოეფიციენტების გაანგარიშების ალგორითმების ინსტრუქციები. ეს მოდული განთავსებულია სხვადასხვა ავტომატიზებულ სამუშაო ადგილებში, სააღრიცხვო-ოპერაციულ სამუშაოთა ბლოკში, ასევე მის გარეთ.

ოპერატორის ასა უზრუნველყოფს დასტაში გაერთიანებული დოკუმენტების ინფორმაციის და თითოეული დასტის მიხედვით გამოთვლილი საკონტროლო ჯამის გამოთვლით სისტემაში შეტანას.

უფროსი ოპერატორის ასა უზრუნველყოფს შეტანილი დოკუმენტების მიხედვით რეისების ფორმირებას და გამოთვლით ცენტრში გადაცემას.

დამხარისხებელის ასა იქმნება იმ დოკუმენტების დასტების შესამოწმებლად, რომელიც შეიტანა ოპერაციონისტმა, და მათ გადასაგზავნად გატარებისათვის; აქვე კონტროლდება ავიზოსა და რეესტრის ფორმირება და ბეჭდვა.

ბანკთაშორის ანგარიშსწორების განყოფილების ასა უზრუნველყოფს ანგარიშსწორებას სხვა კომერციულ ბანკებთან, ბანკთაშორის ოპერაციების კონტროლს, კორექტირებას. საპასუხო ავიზოებთან მუშაობისას ასა ახორციელებს შემავალ დოკუმენტებთან დაკავშირებულ სამუშაოთა კომპლექსს: მიმდინარე დოკუმენტების შეტანა, კორექტირება, საპასუხო ავიზოების გაქვითვა, გაქვითვების ჟურნალის წარმოება, საბოლოო ბრუნვის უწყისის გახსნა, წარმოება, დახურვა და სხვ.

საკრედიტო განყოფილების ასა უზრუნველყოფს ხელშეკრულებების დადებას, წარმოებას, პროლონგაციას, დახურვას, არქივში გადაცემას, ძირითადი ვალის დაფარვის გრაფიკის ფორმირებას, ამ გრაფიკის შესრულების კონტროლს, სხვადასხვა სქემით პროცენტების გადახდას, ძირითადი ვალისა და პროცენტების მიხედვით საურავის დარიცხვას, შესაბამისი უწყისების ფორმირებას.

ფიზიკურ პირებთან მუშაობის ასა ძალიან ხშირად შედის ბანკის ინტეგრირებული სისტემის შემადგენლობაში, რაც დაკავშირებულია ფიზიკური პირების ფულადი საშუალებების მოზიდვასთან. უნდა აღვნიშნოთ, რომ ეს ოპერაციები, მათი მასიურობის გამო, ხასიათდება დიდი შრომატევადობით. ეს ოპერაციები, ძირითადად, სადეპოზიტო ოპერაციებია.

მოლარე-ოპერატორის ასა უზრუნველყოფს: სალაროს საგადამხდელო დოკუმენტების შეტანას, ფულადი ჩეკების მიღებასა და დამუშავებას, ნაღდი ფულის შეტანის განცხადებების დამუშავებას.

ასევე შემოსავლებისა და გასავლების ნაერთი დოკუმენტების ფორმირებას, სალაროს ჟურნალის წარმოებას, სალაროს მომსახურებისათვის კლიენტების გადასახდელის გაანგარიშებას, სალაროს მიხედვით გატარებების უზრუნველყოფას, მემორიალური ორდერის ფორმირებას, სალაროს მიხედვით ცნობების ფორმირებას.

ეკონომისტის ასა ახორციელებს პირადი ანგარიშიდან ამონაწერების ფორმირებას, პირადი ანგარიშების მიხედვით დარიცხვების კონტროლს, ბანკის ნორმატივებისა და მაჩვენებლების გაანგარიშებას, პირადი ანგარიშების მიხედვით ნაშთებისა

და გატარებების კონტროლს, ფილიალების მუშაობის კონტროლს, საგადასახადო ინსპექციისათვის ცნობების ფორმირებას.

მთავარი ბუღალტრის ასა ახორციელებს: ბანკის მუშაობის შესახებ ინფორმაციის მიღებას, პირადი ანგარიშების გახსნასა და დახურვას, ბრუნვის უწყისების, საბალანსო და არასაბალანსო ანგარიშების დათვალიერებას და ბეჭდვას, კლიენტების ხელმოწერების ფაილის განახლებას, პირადი ანგარიშების გახსნას, დახურვასა და ცვლილებების უწყისების ფორმირებას.

ადმინისტრატორის ასა ბანკში წარმოადგენს ერთ-ერთ მნიშვნელოვანს და უზრუნველყოფს:

- გატარებების ოპერატიულ ასახვას;
- დოკუმენტების მიმდინარე ჩამონათვლის შედგენას;
- მიმდინარე შედარების განხორციელებას;
- დოკუმენტური ბალანსის შედგენას;
- ანგარიშგებების ბეჭდვას;
- ბანკის ოპერაციული დღის დაგეგმვასა და დამთავრებას;
- სააღრიცხვო-საოპერაციო განყოფილების მუშაობის დაგეგმვას და ამ განყოფილების თანამშრომლებისათვის უფლებამოსილების განსაზღვრას;

• მომხმარებლის სტატუსის რეგისტრაციას, გაუქმებას, შეცვლას;

- მომხმარებლის მუშაობის პროტოკოლის კონტროლს;
- ბანკის ინფორმაციულ რესურსებთან სანქცირებული შეღწევის ორგანიზებას;

• ნორმატიულ-საცნობარო ინფორმაციის ფონდის წარმოებას;

- მონაცემთა ბაზების ფაილების ადმინისტრირებას;
- ბანკის საინფორმაციო სისტემის სხვა მომხმარებლისათვის სამუშაო ადგილის ორგანიზებასა და კონფიგურაციას;
- კომპლექსში ამოცანის ჩართვას ან ამოღებას;
- კომპლექსის გამართვას;
- ბანკის საინფორმაციო სისტემის დანერგვისას სამუშაოების გაშვებას.

ბანკში ზემოთ ჩამოთვლილი ავტომატიზებული სამუშაო ადგილები არ არის უცვლელი, რაც მიუთითებს იმაზე, რომ, თუ შეიცვალა ავტომატიზებული სამუშაო ადგილები, შესაბამისად შეიცვლება მათ მიერ შესრულებული სამუშაოები, ანუ მოხდება სამუშაოების გადანაწილება

კითხვები თვითშემოწმებისთვის

1. რა სამუშაოები სრულდება კომუნიკაციის თანამშრომლის ავტომატიზებულ სამუშაო ადგილზე?
2. რა სამუშაოები სრულდება დეპოზიტებთან მომუშავე თანამშრომლის ავტომატიზებულ სამუშაო ადგილზე?
3. რა სამუშაოები სრულდება კრედიტების განყოფილების თანამშრომლის ავტომატიზებულ სამუშაო ადგილზე?
4. რა სამუშაოები სრულდება მთავარი ბუღალტრის ავტომატიზებულ სამუშაო ადგილზე?
5. დაახასიათეთ ბანკის საინფორმაციო სისტემაში შემავალი ბლოკები.
6. რა სამუშაოები, სრულდება ბანკთაშორის ანგარიშსწორების განყოფილების თანამშრომლის ავტომატიზებულ სამუშაო ადგილზე?
7. რა სამუშაოები სრულდება მოლარის ავტომატიზებულ სამუშაო ადგილზე?

თავი 5. პლასტიკური ბარათები

5.1. პლასტიკური ბარათების ისტორია

საბანკო პლასტიკური ბარათები – ესაა ანგარიშსწორების თანამედროვე საშუალება, რომლის გამოყენებითაც შეგიძლიათ განახორციელოთ უნაღდო ანგარიშსწორება შეძენილ საქონელსა და მომსახურებაზე, ისარგებლოთ მთელ მსოფლიოში ნაღდი ფულის გაცემის პუნქტების ფართო სპექტრით, შეინახოთ საკუთარი სახსრები საბარათო ანგარიშზე და ა. შ. განასხვავებენ საკრედიტო ბარათებს და სადებეტო ბარათებს. საკრედიტო ბარათი არის პლასტიკური ბარათი, რომელზეც ბანკი კლიენტს გარკვეული ლიმიტით შემოსაზღვრულ საკრედიტო ხაზს უხსნის. სადებეტო ბარათი კი არის პლასტიკური ბარათი, რომელზეც კლიენტს დამოუკიდებლად შეაქვს ან გადარიცხავს ფულად სახსრებს შემდგომი გამოყენებისათვის.

პლასტიკური ბარათების ისტორია საკრედიტო ბარათების გამოშვებით იწყება. პირველი საკრედიტო ბარათები შეერთებულ შტატებში მე-20 საუკუნის დასაწყისში გამოჩნდა და სრულიად არ უკავშირდებოდა საბანკო სისტემას. მათ გარკვეული მაღაზიები და რესტორნები უშვებდნენ. ეს ბარათები მუყაოსგან მზადდებოდა და მდიდარი, შემოწმებული კლიენტებისთვის იყო გათვალისწინებული.

1950 წლიდან საკრედიტო და სხვა ბარათების წარმოებაში საგრძნობი აღმავლობა დაიწყო. ნიუ-იორკსა და ლოს-ანჯელესში ორმა მეწარმემ, ბლუმინგდელმა და მაკნამარამ, ერთდროულად ამოქმედეს თავიანთი საბარათე პროგრამები სახელწოდებით [25] „რომ ისადილებ, ხელი მოაწერე“. საინტერესოა, რომ მაკნამარას საქმე მაინცდამაინც სასურველი წარმატებით არ მისდიოდა მანამ, სანამ არ მოიფიქრა, როგორ მიეღო შემოსავალი კლიენტთა დაკრედიტების საშუალებით. ის მიზნობრივი აუდიტორია, რომელზეც მიმართვა გადაწყვიტა მაკნამარამ, მანჭეტენზე ასობით რესტორანი და ათასობით მათი კლიენტი იყო. მეწარმემ 5 000 დოლარის საწყისი კაპიტალით თავისი საბარათე პროგრამა ამოქმედა და პირველივე თვეში – 2000 დოლარი, ხოლო 4 თვის

შემდეგ უკვე 250 000 დოლარი მოგება ნახა. ლოს-ანჯელესში კი ანალოგიური კამპანიით ბლუმინგდელის მოგებამ 3 თვეში 150 000 დოლარი შეადგინა. ამჯერადაც ბარათები მუყაოსი იყო.

პირველი ლითონის ბარათები გამოჩნდა 1928 წელს, როდესაც კომპანია **Farrington Manufacturing**-მა საკრედიტო ბარათები ბენზინგასამართი სადგურების კლიენტებისთვის გამოუშვა. ყოველ ბარათს ენიჭებოდა თავისი იდენტიფიკატორი, რაც მისი გამოყენების პროცედურას აადვილებდა. გამყიდველი ჩეკ-ქვითარზე სპეციალური წნეხით აკეთებდა გარიგების შესახებ მონაცემთა ანაბეჭდს.

საბარათო ბაზარზე გამოსვლა თანდათანობით დაიწყო „კაპიტალიზმის ვეშაპებმა“ – **American Express**-მა და მსხვილმა ამერიკულმა ბანკებმა, რომლებიც შემდგომში გაერთიანდნენ მსხვილ საგადასახდლო სისტემებში, როგორიცაა **VISA, Europay, MasterCard**.

ლითონისა და მუყაოს ბარათებმა თავიანთი დრო მოჰამეს, აუცილებელი გახდა სხვა მასალების გამოყენება. ბარათისთვის მასალა უსაფრთხო, გამძლე და პლასტიკური უნდა ყოფილიყო, რათა შესაძლებელი გამხდარიყო მასზე იდენტიფიკაციისათვის საჭირო ინფორმაციის ამოტვიფრა. მაშინ გაჩნდა მსოფლიოში პირველი პლასტიკური ბარათი. უნდა აღინიშნოს, რომ ბარათი არა მხოლოდ პლასტიკის ნაჭერია, არამედ იგი არის მაღალი ტექნოლოგიის პროდუქტიც. დღეს პლასტიკური ბარათის გამოყენება გულისხმობს მონაცემთა გაცვლას არა მხოლოდ ერთი ქვეყნის ფარგლებში, არამედ სხვადასხვა სახელმწიფოებს შორისაც. არსებობს მაგნიტური პლასტიკური ბარათები და არსებობს ბარათები აგებული მიკროჩიპის საფუძველზე. მაგალითად, **VISA** ან **MasterCard** პლასტიკური ბარათებით თქვენ შეგიძლიათ შეძენილი საქონლის ან გაწეული მომსახურების ღირებულება გადაიხადოთ მსოფლიოს ნებისმიერ ქვეყანაში, სადაც გამოიყენება საბარათო გადახდის წესი. ევროპაში საკრედიტო და საბანკო ბარათებმა გავრცელება პოვეს გასული საუკუნის 50-იან წლებში, რასაც საფუძველი დაუდო ბრიტანულმა კორპორაციამ **British Hotel & Restaurant Association**, გამოუშვა რა საკრედიტო ბარათი

BHR. იმ დროს ევროპაში უკვე დომინირებდა ამერიკული კომპანია **Dinners Club**. 1972 წელს შეერთებულმა შტატებმა კიდევ ერთხელ სცადა პლასტიკური საკრედიტო ბარათების ევროპული ბაზრის დაპყრობა. **Americard**-მა 72 ქვეყანაში გამოაცხადა კამპანიის დაწყება, მაგრამ ევროპული ბანკები არ მიისწრაფოდნენ, დამორჩილებოდნენ ამერიკულ გიგანტს. ასეთ ვითარებაში **Interbank**-მა ხელი მოაწერა შეთანხმებას **EuriCard**-თან, ამჟამად ევროპაში არსებულ უნივერსალური პლასტიკური საბანკო ბარათების უმსხვილეს სისტემასთან.

დღეისათვის საბარათო ტექნოლოგიების შემუშავებასა და საბანკო პლასტიკური და საკრედიტო ბარათების წარმოებაში უპირობო ლიდერებს წარმოადგენენ: **VISA** – ამერიკული, **MasterCard** – ევროპული (გაერთიანდა **Maestro**-სთან) და **American Express** – ამერიკული კორპორაციები.

ყოფილ საბჭოთა კავშირში პლასტიკური ბარათების გამოყენება დაიწყო 1969 წლიდან. ამ ბარათების ემიტენტის როლში გამოდიოდნენ საზღვარგარეთის ფირმები. რუსეთში პირველი კომერციული ბანკი, რომელმაც პლასტიკური ბარათები გამოუშვა, იყო კრედო-ბანკი, 1991 წელს.

5.2. პლასტიკური ბარათების კლასიფიკაცია და სახეები

პლასტიკური ბარათების, როგორც შეძენილი საქონლისა და გაწეული მომსახურების გადახდის, ან პირადი ანგარიშიდან გარკვეული რაოდენობის ნაღდი ფულის მიღების საშუალების, კლასიფიკაცია შესაძლებელია სხვადასხვა ნიშნის მიხედვით: დასამზადებლად გამოყენებული მასალის, ანგარიშსწორების სახის, ბარათზე ინფორმაციის ჩანერის წესის, დაწესებულება ემიტენტისადმი კუთვნილების, გამოყენების სფეროს, ტერიტორიული კუთვნილების და გამოყენების დროის ხანგრძლივობის მიხედვით. ბარათები, დამზადებული მასალის მიხედვით, შეიძლება იყოს: მუყაოსი, ლითონის და პლასტმასის. ანგარიშსწორების მიხედვით: საკრედიტო, სადებეტო და საგადამხდელო. გამოყენე-

ბის მიხედვით: ინდივიდუალური, საოჯახო და კორპორაციული. ზოგჯერ ამ ჯგუფში ცალკე გამოყოფენ ტურიზმისა და გართობის ბარათებს.

ბარათებს მათზე ინფორმაციის ჩანერის ხერხის მიხედვით განასხვავებენ: გრაფიკული ჩანერის, ემბოსირებული, შტრიხკოდური, მაგნიტურ ზოლზე კოდირებული, ლაზერული (ოპტიკური ბარათები), და ბარათები მეხსიერებით [8].

ორგანიზაცია-ემიტენტის კუთვნილების მიხედვით განასხვავებენ: ბანკის ბარათებს, რომლის ემიტენტია ბანკი ან კონსორციუმი; კომერციული ბარათები, რომლებსაც უშვებენ არასაფინანსო დაწესებულებები, მაგალითად, კომერციული ფირმები.

გამოყენების სფეროს მიხედვით ასხვავებენ: უნივერსალურს, რომლითაც წარმოებს ნებისმიერი შეძენილი საქონლის ან განეული მომსახურების ანაზღაურება და კერძო კომერციული ბარათები, რომლებიც გამოიყენება რომელიმე განსაზღვრული მომსახურების ანაზღაურების მიზნით (მაგალითად, ავტოგასამართი სადგურების მომსახურების ანაზღაურება).

ტერიტორიული კუთვნილების მიხედვით განასხვავებენ: საერთაშორისო ბარათებს, რომლებიც ბევრ ქვეყნებში გამოიყენება; ნაციონალურ ბარათებს, რომლებიც ერთ რომელიმე სახელმწიფოში გამოიყენება; ლოკალურ ბარათებს, რომლებიც ქვეყნის ამა თუ იმ ნაწილში გამოიყენება; დაბოლოს, ბარათებს, რომლებიც გამოიყენება მხოლოდ ერთ რომელიმე დაწესებულებაში.

გამოყენების დროის მიხედვით განასხვავებენ უვადო და დროში შეზღუდულ ბარათებს.

ანგარიშსწორებისათვის გამოყენებული ბარათები შეიძლება იყოს ავტონომიური. მაგალითად, „ელექტრონული საფულე“ და „გასაღებ-ბარათები“, რომლებიც გამოიყენება ანგარიშების იდენტიფიკაციის მიზნით ან, როგორც სპეციალური საშვი ინფორმაციულ რესურსებთან ან კიდევ კომპიუტერთან მუშაობისათვის. უნაღდო ანგარიშსწორებისათვის გამოყენებული პლასტიკური ბარათებიდან დღეისათვის ყველაზე პერსპექტიულია ბარათები ჩაშენებული მიკროსქემებით – „ინტელექტუალური“ ბარათები, სმარტ-ბარათები (**Smart Card**). აღნიშნულ ბარათში ჩაშენებული მიკროპროცესორი, ფაქტობრივად, უდიდესი შესაძ-

ლებლობების (მეხსიერება, სხვადასხვა გაანგარიშებების შესაძლებლობა) მიკრო – კომპიუტერია. ამ ბარათების წინამორბედი პლასტიკური ბარათები გრაფიკული ჩანერით, ემბოსირებით, შტრიხკოდებით, მაგნიტური ზოლებით და ბარათები მეხსიერებით. საიმედოობის თვალსაზრისით ყველაზე პერსპექტიულია ბარათები ოპტიკური მეხსიერებით.

სმარტ-ბარათების გამოყენების საიმედოობა მაღალია. მაგალითად, თუ ვინმე შეეცდება მის არასანქცირებულ გამოყენებას, ამ შემთხვევაში ბარათი ან დროებით წყვეტს ფუნქციონირებას ან საერთოდ გამოდის მწყობრიდან. მათ აღსადგენად საჭიროა ბარათის გაგზვნა ბანკ-დამამზადებელთან. სმარტ-ბარათებს გააჩნია მაღალი საექსპლუატაციო მახასიათებლები, მაგალითად, ფრანგული ფირმა **Gemplus Card Ynternational**-ის მიერ დამზადებული ბარათისათვის დამახასიათებელია ინფორმაციის ხანგრძლივი ვადით შენახვა – 10 წელი; გადანერის მინიმალური რაოდენობა – 10000; ერთი ბაიტი ინფორმაციის ჩანერის დრო – 10 მიკროწამამდე; შენახვის ტემპერატურული რეჟიმი – 20 გრადუსიდან +55 გრადუსამდე; მუშა ტემპერატურული რეჟიმი – 0 გრადუსიდან +50-მდე. იგი საკმაოდ მდგრადია და მის გამოსაყენებლად საჭირო ტერმინალური მოწყობილობების ღირებულება დაბალია. სმარტბარათებზე აგებული სისტემების მომსახურება არ საჭიროებს დამატებით ხარჯებს, აქვს გამოყენების მაღალი საიმედოობა. ვაჭრობის ტერმინალის ავტონომიურობა უზრუნველყოფს მის ფართო გამოყენებას მობილურ პუნქტებსა და სავაჭრო ჯიხურებში. ამ ბარათების საშუალებით შეიძლება გადაიხადოთ ავტომატიდან შეძენილი სიგარეტის, სატელეფონო საუბრის, ავტომანქანების სადგომებზე გაჩერების ღირებულება და სხვ. აღნიშნული ბარათების გამოყენება ამარტივებს და აუმჯობესებს ურთიერთანგაროშსწორებას, ამცირებს სისტემით მოსარგებლე ყველა მომხმარებლის ხარჯებს, ამცირებს კრიმინალურ დანაშაულებებს.

სმარტ-ბარათებზე აგებული მრავალი სისტემა წარმატებით ფუნქციონირებს. ასეთ სისტემებს მიეკუთვნებიან: **Mondex, Proton, Visa-Cash** და სხვა. ყველა აღნიშნული სისტემა აგებულია ელექტრონული ფულის გამოყენებაზე.

სისტემა **Mondex** კავშირის არხებით ელექტრონული ფულის მოძრაობის სისტემაა. მსოფლიოს სხვადასხვა წერტილში მყოფ სუბიექტებს შორის შესაძლებელია ანგარიშსწორების მომენტალური განხორციელება. ბანკის ანგარიშიდან აღნიშნულ ბარათზე ფულის ჩასარიცხად ან ამ ბარათიდან ბანკში კლიენტის ანგარიშზე ფულის ჩასარიცხად გამოიყენება მონდექს ტელეფონი **Mondex phones**. ამრიგად, ელექტრონული ფულის გადაცემა ხდება სატელეფონო ხაზებით. ელექტრონული ფულის შენახვა შეიძლება ე.წ. საფულეში **Mondex Wallet**. მონდექს-საფულე პორტატიული მოწყობილობაა, რომელსაც შეუძლია ელექტრონული ფულის გადაგზავნა ბარათიდან ბარათზე, **PIN**-კოდის შეცვლა, კლიენტის ანგარიშიდან ბალანსის ნაკითხვა და სხვ. ამ მოწყობილობის მთავარი და ძირითადი ფუნქციაა ანგარიშიდან მოხსნილი ფულის შენახვა. შესაძლებელია, საფულიდან ელექტრონული ფულის გადაგზავნა მონდექს ბარათზე. ამავე სისტემით გათვალისწინებულია: ბანკომატიდან ნაღდი ფულის მიღება, სავაჭრო ტერმინალის საშუალებით მყიდველის ბარათიდან გამყიდველის ბარათზე ელექტრონული ფულის გადაგზავნა და შემდეგ მონდექს – ტელეფონის საშუალებით ფულის გადარიცხვა გამყიდველის ბარათიდან ბანკში, მის ანგარიშზე. აღნიშნული სისტემის აპრობაცია განხორციელდა ჯერ კიდევ 1995 წელს ინგლისში. 1996 წლისათვის ინგლისის პატარა ქალაქ სუიდონში აღნიშნული სისტემით სარგებლობდა ბარათის 10000 მფლობელი.

„ელექტრონული ფულის“ ერთ-ერთი სისტემაა 1995 წელს ბელგიის ფირმა **Banksis**-ის მიერ შემუშავებული სისტემა „ელექტრონული ფული“ – **Proton**-ი. აღნიშნული სისტემა „ელექტრონული საფულეა“, რომელიც წარმატებით გამოიყენება სხვადასხვა სფეროში: მაღაზიაში დაბალი ღირებულების საქონლის შესაძენად; სავაჭრო ავტომატებიდან საქონლის შესაძენად; ავტომანქანების სადგომებზე გაჩერების ღირებულების გადასახდელად; საზოგადოებრივი ტრანსპორტით მგზავრობის ღირებულების გადასახდელად; ტელეფონ-ავტომატით სარგებლობისათვის. **Proton** წარმოადგენს ბელგიის ნაციონალურ „ელექტრონულ ფულს“. იმისათვის, რომ „ელექტრონული ფულის“ გამოყენება

ისევე მარტივი და მოსახერხებელი იყოს, როგორც ჩვეულებრივი ნაღდი ფულის, მას უნდა გააჩნდეს უსაფრთხოების იგივე დონე, როგორიც ნაღდი ფულს და, ამავე დროს ქვეყნის ეკონომიკისათვის იყოს უსაფრთხო. იმისათვის, რომ „ელექტრონული ფულის“ მფლობელმა გაიგოს, თუ რა რაოდენობის ფული დარჩა საფულეში, ბარათის ფუტლიარში ჩამონტაჟებულია პორტატიული მონაცემების აღწერა, რომლის ღირებულება ხელის დაჭერით გამოჩნდება საფულეში დარჩენილი ნაშთი.

სისტემის უსაფრთხოება მიიღწევა აგრეთვე იმით, რომ „ელექტრონული ფულის“ ემიტენტი ბანკი ან საფინანსო დაწესებულება ახდენს კლიენტის ანგარიშის დეპეტირებას იმ მომენტში, როცა „ელექტრონულ საფულეში“ წარმოებს თანხის ჩატვირთვა. იმავედროულად, შესაბამისი თანხა ემიტენტის მიერ გაიგზავნება ქვეყნის ერთიან სარეზერვო ფონდში. დარეზერვირების აუცილებელი პროცედურა საშუალებას იძლევა, ერთი მხრივ კონტროლი გაუწიოთ „ელექტრონული ფულის“ ემისიას, მეორე მხრივ, იმ ორგანიზაციებისათვის თანხის ანაზღაურებას, რომლებმაც წარმოდგენილი ბარათის საფუძველზე თანხების ანაზღაურება განახორციელეს.

აღსანიშნავია, რომ დაკარგული საფულით შეუძლია ისარგებლოს ნებისმიერმა პირმა, რადგან „ელექტრონული საფულე“ ანონიმურია, ე.ი. არ არის საჭირო PIN-კოდის შეყვანა სისტემაში. ყველა სადებეტო ოპერაცია სრულდება **off-line** რეჟიმში. თუ იგი შეერთებულია ცენტრთან ტრანზაქციის შესახებ მონაცემები ტერმინალით გადაცემა საპროცესინგო ცენტრს, ან მონაცემების გადაცემა წარმოებს ოპერატორის მიერ კომპიუტერისა და მოდემის საშუალებით. სმარტ-ბარათით გაყიდული საქონლის ღირებულება გამყიდველის ანგარიშზე გადაიგზავნება ზემოთ აღნიშნული სარეზერვო ფონდიდან. „ელექტრონული ფული“ **Proton** და **Mondex** წარმატებით გამოიყენება ნიდერლანდებში, ავსტრალიაში, შვეიცარიაში, შვეციაში, კანადასა და ბრაზილიაში და სხვა ქვეყნებში.

„ელექტრონული ფულის“ ერთ-ერთი მსხვილი კორპორაციაა **VISA**. „ელექტრონული საფულე“ **Visa Cash** სისტემის დანიშნუ-

ლებაა მისი ღია სისტემაში გამოყენება. ამ სისტემის მონაწილეები: ემიტენტი, ეკვაირი და სავაჭრო მომსახურების სანარმო. ღია სისტემის ფარგლებში გამოშვებული ბარათების ანაზღაურება უნდა განახორციელოს სისტემაში გაერთიანებულმა ნებისმიერმა წევრმა.

გამოყენებაშია სამი სახის **Visa Cash**-ის „ელექტრონული საფულე“. პირველი „ელექტრონული საფულე“, რომელზედაც ერთხელ შეიტანება სანყისი თანხა. ამის შემდეგ აღნიშნულ ბარათზე აღარ წარმოებს დაფიქსირებული თანხის შეცვლა, ე. ი. შეუძლებელია მისი შემდგომი ახალი თანხით შევსება. ასეთი საფულე მოხერხებულია ბავშვებისათვის, ჯიბის ფულის ან საჩუქრებისათვის, საქმიანი ან ტურისტული მოგზაურობისათვის, როგორც სამგზავრო ფული, ბილეთების შესაძენად, ან სხვა ღონისძიებისათვის.

მეორე სახის „ელექტრონული საფულე“ გამოიყენება იმ შემთხვევაში, როცა ბარათზე არ არის დაფიქსირებული თანხის ნომინალური სიდიდე. კლიენტს შეუძლია ბანკომატის ან სპეციალური ტერმინალური მოწყობილობით მასზე შეიტანოს გარკვეული თანხა. შემდგომში ამ ბარათზე შეიძლება თანხის დამატება ტელეფონით ან ტერმინალური მოწყობილობით. ასეთ **VISA Cash**-ის ბარათებს შეუძლიათ შეასრულონ სადებეტო, საკრედიტო და ბანკომატის ბარათების ფუნქციები.

5.3. საქართველოს ბანკებში გამოყენებული პლასტიკური ბარათები

საქართველოში პლასტიკური ბარათების ბაზარი დინამიკურად ვითარდება. ჩვენს ქვეყანაში პლასტიკური ბარათების დანერგვა დაიწყო სახელმწიფოებრივი დამოუკიდებლობის აღდგენის შემდეგ. საქართველოს ეროვნული ბანკის ინფორმაციით, საქართველოში პლასტიკური ბარათების ბაზრის განვითარება დინამიკურობას ინარჩუნებს.

პლასტიკურ ბარათზე არსებული თანხა შეიძლება გავანაღდოთ არა მხოლოდ ბანკომატით, არამედ ტერმინალითაც. კერ-

ძოდ, მომსახურების ობიექტზე ან მაღაზიაში დადგმულ ტერმინალზე ბარათის გატარებით.

ბანკომატი დგას ძალიან ბევრ ადგილას. ყველა ბანკს აქვს თავისი ბანკომატი. თითოეული ბანკის ბანკომატში შესაძლებელია თანხის განაღდება, მომსახურების ტარიფები განსხვავებულია.

ტერმინალზე განაღდება თითქმის ყველა ბანკს აქვს 0%, ანუ რა ღირებულების მომსახურებას თუ საქონელსაც ყიდულობთ, ზუსტად ის თანხა ჩამოგვეჭრება ბარათიდან. ეს განსხვავებაა ბანკომატსა და ტერმინალს შორის.

ტერმინალები დგას როგორც მომსახურების ობიექტებში, ასევე ბანკებში. ამასთან, როდესაც ტერმინალი დგას მომსახურების ობიექტში, მასზე მხოლოდ და მხოლოდ ხდება ნაყიდი ნივთის ან მომსახურების ანაზღაურება ბარათიდან და როდესაც ტერმინალი დგას ბანკში, ხდება ბარათიდან თანხის მოხსნა.

საქართველოს მსხვილ კომერციულ ბანკებს გააჩნიათ საკუთარი პლასტიკური ბარათები. შექმნილია პლასტიკური ბარათების გამოყენების ერთიანი ქსელი.

დღეისათვის ძირითადი 3 ბრენდია: **VISA, MasterCard, Maestro**. თითოეული ტიპის ბრენდი იყოფა **Electron, Classic, Gold** და **Platinum** ბარათებად, რომლებიც სხვადასხვა სოციალურ ფენაზეა გათვლილი.

Electron-ი, ძირითადად, სახელფასო პროექტებისთვისაა გათვალისწინებული. ამ ბარათის ხარისხიც შედარებით დაბალია, ვიზუალურადაც ნაკლებად ეფექტურია, ფუნქციებიც უფრო ნაკლები აქვს (ზოგი ინტერნეტში არ მოქმედებს, ზოგიც – საზღვარგარეთ და სხვა).

Classic-ი უფრო მაღალი დონის ბარათია და საშუალო ფენაზეა გათვლილი. **Gold** და **Platinum** გათვლილია მაღალ ფენაზე და **VIP** კლიენტებზე.

როდესაც ორგანიზაცია ბანკში ხსნის სახელფასო პროექტს, როგორც წესი, რიგითი თანამშრომლებისთვის მზადდება ბარათები **Electron-ები**, საშუალო მენეჯმენტისთვის – **Classic-ები** და ღირექტორატისთვის – **Gold-ები**. **Gold** ბარათი მსოფლიოში ცნობილია,

როგორც საუკეთესო ბარათი, ვიზუალურადაც უფრო ლამაზია; ფუნქციებიც უფრო მეტი აქვს. მაგალითად, განაღდების დღიური ლიმიტი **Electron**-ზე არის უფრო ნაკლები; განაღდების დღიური ლიმიტი ბანკომატში შეიძლება – 1000 ერთეული იყოს და მაღაზიაში 2000. მაგრამ **VIP** კლიენტისთვის და დირექტორისთვის, რომელიც საზღვარგარეთ მიდის, ეს თანხა ძალიან მცირეა. იგივე ბიზნესმენი, რომელიც საზღვარგარეთ მიდის და ბარათიდან 10 ათასის მოხსნა სჭირდება, **Electron**-ით ნამდვილად ვერ წავა. ამავე დროს, **Gold**-ის მფლობელისთვის ბანკებში განსაზღვრულია სხვა შეთავაზებები, სხვა პირობები. თავის მხრივ, **Platinum** კიდევ უფრო მაღალი დონეა, ვიდრე **Gold**. **Platinum** ყველა ბანკს არა აქვს, ძირითადად, აქვთ **Electron**, **Classic** და **Gold**.

სადებეტო ბარათები არის ძირითადად **Electron**, **Classic** და **Gold**. საკრედიტო ბარათებს სხვადასხვა ბანკი სხვადასხვა სახელს არქმევს, მაგალითად, „საქართველოს ბანკის“ საკრედიტო ბარათს ჰქვია **Orange Card**-ი; „ბაზის ბანკისას“ – „**Geocell Visa Card** (რომელიც ერთობლივია „ჯეოსელთან“ ერთად) და „მეგობარი“; „ტაოპრივატბანკისას“ – „**აქცია**“, „**უბროცენტო**“ და ა. შ. ასევე ბანკებს აქვთ საკუთარი დიზაინის ბარათები. არიან ბანკები, რომლებსაც მხოლოდ და მხოლოდ **VISA** ტიპის ბარათი აქვთ და ასევე არიან ისეთებიც, რომლებსაც აქვთ როგორც **VISA** ტიპის, ასევე **MasterCard**-ის ბარათები.

საქართველოში პლასტიკური ბარათების კიდევ უფრო ფართოდ გავრცელებას ხელს უშლის:

- პლასტიკური ბარათების გამოყენების არასრულყოფილი საკანონმდებლო ბაზა;
- ხალხის ფართო მასების დაბალი კომპიუტერული განათლება;
- უნდობლობა ელექტრონული ანგარიშსწორების მიმართ.

ამიტომ საჭიროა მათი ფსიქოლოგიური მომზადება, მათთვის გარკვეული უნარ-ჩვევების გამომუშავება. აღნიშნულის განხორციელება უნდა მოხდეს სასწავლო დაწესებულებებში. უნდა შეიქმნას უფასო მოსამზადებელი საკონსულტაციო კურსები,

ამ საქმეში აქტიური როლი უნდა შეასრულოს ტელევიზიამ და პრესამ.

„თიბისი ბანკის“ პლასტიკური ბარათები. „თიბისი ბანკი“ კლიენტებს სთავაზობს შემდეგი სახის ბარათებს: საკრედიტო ბარათი **TBC Card**, განვადების ბარათები, სადებეტო ბარათები და **„TBC COSMO“**.

საკრედიტო ბარათს **TBC Card-ს** გააჩნია 55-დღიანი საშელავათო პერიოდი. მისი უპირატესობებია ის, რომ ეს არის უპროცენტო კრედიტი საქართველოში ყველაზე ხანგრძლივი პერიოდით, უვადო საკრედიტო ლიმიტით, კრედიტით უზრუნველყოფისა და თავდებობის გარეშე. **TBC Card-ის** მიღება მარტივია, თუ თქვენი ასაკი არის არანაკლებ 20 წელი, გაქვთ 6 თვის სამუშაო გამოცდილება და თქვენი ყოველთვიური შემოსავალი შეადგენს მინიმუმ 200 ლარს. **TBC Card-ის** დავალიანების დაფარვა შეგიძლიათ რამდენიმე გზით: „თიბისი ბანკის“ ნებისმიერ ფილიალში მისვლით, ტელეფონ ბანკით, ინტერნეტბანკით, სხვა ბანკიდან თანხის გადმორიცხვით.

განვადების ბარათი – ეს არის **VISA Electron-ის** ტიპის ბარათი რომელსაც გააჩნია შემდეგი უპირატესობები: სისწრაფე (ბარათი თქვენი გახდება განაცხადის შევსებისთანავე და მის მისაღებად ლოდინი საჭირო არ არის), კომფორტი (თქვენ თავისუფალი ხართ ბანკთან შეთანხმების და დამატებითი საბუთების მოძიებისაგან. მაღაზიაში შეგიძლიათ აირჩიოთ სასურველი საქონელი, საქონლის ღირებულება გადაიხადოთ განვადების ბარათით და განვადება ბანკში ავტომატურად რეგისტრირდება), მოქნილობა (შეგიძლიათ მრავალჯერ ისარგებლოთ წინასწარ განსაზღვრული განვადების ლიმიტით, მთლიანად ან ნაწილობრივ დაფაროთ და შემდეგ კვლავ გამოიყენოთ თანხა ნებისმიერ დროს, 2 წლის განმავლობაში), თავისუფლება (განვადების მენეჯერის ძებნა საჭირო აღარ არის), თქვენ თავისუფალი ხართ სავაჭრო ობიექტის შერჩევისას, ბარათი შეგიძლიათ გამოიყენოთ საქართველოს ნებისმიერ ობიექტში, რომელშიც შესაძლებელია **VISA** ბარათით ანგარიშსწორება).

ფასდაკლება 20%-მდე – განვადების ბარათით პარტნიორ ობიექტებში გადახდილი თანხის შესაბამისი პროცენტი ბონუსად დაგიბრუნდებათ ანგარიშზე.

განვადების მაქსიმალური ლიმიტია 3000 ლარი, განვადების ვადა – 10 თვე (განვადების დაფარვა ხდება 10 თვის განმავლობაში თანაბარი გადახდებით), ბარათის ღირებულება – 10 ლარი, ბარათის მოქმედების ხანგრძლივობა – 2 წელი, საქონლის ღირებულების გადახდა სავაჭრო ობიექტებში – 0%. განვადების ბარათით სარგებლობისას ერთჯერადი შენაძენის ღირებულება არ უნდა აღემატებოდეს 50 ლარს. საჭიროების შემთხვევაში, თანხის გამოტანა შესაძლებელია საქართველოს ტერიტორიაზე არსებული ნებისმიერი ბანკომატიდან ან ბანკიდან (არანაკლებ 50 ლარისა). განვადების ბარათით სარგებლობისთვის საკმარისია: იყოს საქართველოს სრულწლოვანი მოქალაქე და გქონდეთ სტაბილური შემოსავალი; მიმართოთ „თიბისი ბანკის“ ნებისმიერ ფილიალს ან სერვისცენტრს და წარადგინოთ პირადობის მოწმობა, შეავსოთ განაცხადი და მიიღოთ განვადების ბარათი 1 წუთში.

"TBC COSMO" VISA პლასტიკური ბარათი, რომელსაც გთავაზობთ „თიბისი ბანკი“ და ჟურნალი **COSMOPOLITA** შექმნილია ქალბატონებისთვის. ბარათების დიზაინი ქართველი ქალბატონების მოთხოვნების გათვალისწინებითაა შერჩეული და გააჩნია 5 ვარიანტი, საიდანაც 3 არის **Visa Electron-ი**, ხოლო 2-**Visa Classic-ი**. შესაძლებელია მათგან ნებისმიერის შერჩევა და შეძენა. **„TBC COSMO“** საშუალებას იძლევა უსაფრთხოდ და კომფორტულად განკარგოთ თანხები მსოფლიოს ნებისმიერ წერტილში. შეგიძლიათ აგრეთვე ისარგებლოთ სპეციალური ფასდაკლებებით (3%-დან 15%-მდე) საქართველოში არსებულ პარფიუმერიის, ტანსაცმლის, ფეხსაცმლის, სპორტული, საყოფაცხოვრებო ტექნიკის და სხვა მაღაზიებში, ასევე – რესტორნებში, სილამაზის სალონებში, გასართობ, სპორტულ-გამაჯანსაღებელ და სამედიცინო ცენტრებში. **„TBC COSMO“** ბარათი 4-წლიანია და წლიური მომსახურების საკომისიო: **Electron** ბარათის შემთხვევაში -15 ლარია, არ ითხოვს მინიმალურ

ნაშთს. წლიური მომსახურების საკომისიო **Classic** ბარათის შემთხვევაში 20 აშშ დოლარია, მინიმალური ნაშთი შეადგენს 20 აშშ დოლარს. ყველა დანარჩენი ტარიფი სტანდარტული **VISA** ბარათების ანალოგიურია.

TBC COSMO-ს მფლობელები შეღავათებს მიიღებენ „თიბისი ბანკის“ სხვადასხვა მომსახურებაზე და ისარგებლებენ ექსკლუზიური პირობებით „ჯიპიაი ჰოლდინგისგან“.

Mobile Card არის „თიბისი ბანკისა“ და მაგთიკომის ერთობლივი ჩიპური ტექნოლოგიის საერთაშორისო ბარათი, უნიკალური საბონუსე სისტემა ახალგაზრდებისათვის, რომელსაც გააჩნია მთელი რიგი უპირატესობები.

„თიბისი ბანკისა“ და „ლუკოილ ჯორჯიას“ ერთობლივი **VISA** ბარათი – თიბისი ლუკოილი, ჩიპური ტექნოლოგიის, **VISA Electron**-ის საკრედიტო ბარათია, რომლითაც კრედიტი ხელმისაწვდომია 24 საათის განმავლობაში. მისი მთავარი უპირატესობებია:

- უფასო სანავის მიღების შესაძლებლობა ლუკოილის ავტოგასამართ სადგურებზე და საქართველოს ტერიტორიაზე ნებისმიერ სავაჭრო ობიექტში ბარათის მოხმარებით დაგროვილი ბონუსქულების სანაცვლოდ;
- ბარათით გადახდისას 5%-დან 10%-მდე ფასდაკლება ავტომობილებთან დაკავშირებულ სხვადასხვა სავაჭრო ობიექტში და GMC ჯგუფის რესტორნებში;
- ფასდაკლება საბანკო მომსახურებაზე „თიბისი ბანკისაგან“;
- ავტოდაზღვევის პოლისი უფასოდ „ჯიპიაი ჰოლდინგისაგან“.

თიბისი ბანკის **VISA/MasterCard** ბარათები მოქმედებს მსოფლიოს ნებისმიერ წერტილში, რომელიც აღჭურვილია **VISA/MasterCard** ნიშნით.

საქართველოს ბანკის პლასტიკური ბარათები. საქართველოს ბანკის მიერ ემიტირებული პლასტიკური ბარათი გამოიყენება მსოფლიოს ნებისმიერ ქვეყანაში ყველგან, სადაც კი **VISA** ან **MasterCard** საფირმო ნიშანია გამოსახული [9].

სადეპეტო ბარათები **VISA Electron, Cirrus/Maestro** ხელმი-საწვდომია ყველასათვის, ვისაც სურვილი აქვს, საკუთარი თანხა მიიღოს ან ხარჯოს პლასტიკური ბარათების მეშვეობით. **VISA Electron, Cirrus /Maestro** ბარათები საშუალებას იძლევა დახარ-ჯოთ თანხის ზუსტად ის რაოდენობა, რამდენიც საბარათე ანგარიშზეა განთავსებული.

VISA Classic და **Master Card Standard**-ი არის ბარათები საქ-მიანი ადამიანებისათვის.

VISA Classic და **MasterCard Standard** სახის საკრედიტო ბარათები-სათვის არ არსებობს არანაირი დაბრკოლება. თქვენი ბარათი გაძლევთ საშუალებას, დახარჯოთ დეპოზიტზე განთავსებულ თანხაზე მეტი, ანუ თქვენს საბარათე ანგარიშზე თანხების დროებითი უკმარისობა არ შეა-ფერხებს თქვენივე სურვილების რეალიზებას.

ოქროს ბარათები – **VISA Gold** და **MasterCard Gold** – მთელ მსო-ფლიოში თქვენი პრესტიჟის ნიშანია, იმის ნიშანი, რომ თქვენ კარგი საკრედიტო ისტორიის მფლობელი ხართ და ამის შესახებ იციან არა მხოლოდ თქვენს ქვეყანაში, არამედ მთელ მსოფლიოში, რის საფუძველზეც იღებთ ფინანსურ სტაბილურობას განურჩევლად იმისა, თუ საზღვარგარეთის რომელ ქვეყანაში იმყოფებით. **VISA Platinum** და **MasterCard Platinum** ბარათები კი იმის ნიშანია, რომ თქვენ მსოფლიო ელიტის ნევრი ხართ.

პლატინის და **OneCard** ბარათები შექმნილია ყველაზე პრივ-ილეგირებული ადამიანებისათვის. „საქართველოს ბანკი“ პირვე-ლი სთავაზობს თავის კლიენტებს მსგავს ბარათებს. თუ თქვენ სარგებლობთ კერძო ბანკირების მომსახურებით, პლატინის და **OneCard** ბარათები თქვენი მუდმივი თანამგზავრი გახდება. მათი მეშვეობით შესაძლებელია თითქმის ნებისმიერი სურვილის ას-რულება, **VIP** მომსახურება მსოფლიოს ნებისმიერ ქვეყანაში – აეროპორტებში, სასტუმროებში, რესტორნებში, მაღაზიებში, 10%-იანი ფასდაკლება **British Airways**-ის ავიაბილეთებზე.

Orange Card – ეს არის საბანკო კრედიტი, რომელიც შეგიძ-ლიათ გამოიყენოთ ნებისმიერი მიზნისთვის. **Orange Card**-ით სარგებლობისთვის სესხის უზრუნველყოფა არ მოგეთხოვებათ. **Orange Card**-ის გამოყენება შესაძლებელია მთელ მსოფლიოში.

ყოველთვიურად შეგიძლიათ ისარგებლოთ 30-დღიანი 0%-იანი კრედიტით. ყოველთვიურად, დადგენილ თარიღამდე დავალთანების სრულად დაფარვის შემთხვევაში თქვენ არ მოგეთხოვებათ პროცენტის გადახდა.

Orange Card-ით სარგებლობისას პროცენტის დარიცხვა ხდება მხოლოდ ათვისებულ თანხაზე, ათვისებელ ლიმიტზე კი პროცენტი არ დაგერიცხებათ.

გარდა ამისა, „საქართველოს ბანკის“ მიერ ემიტირებულია სპეციალური სერიის ბარათები: **ArtCard** გამოშვებულია ახალგაზრდა ქართველი მხატვრებისა და ალტერნატიული სამხატვრო ხელოვნების მხარდასაჭერად.

ICard გამოშვებულია პროექტ MeloMoney-ს ფარგლებში. შეიძინეთ Apple-ის ციფრული მუსიკალური ფლეიერი iPod-ი თვეში მხოლოდ 50 ლარად და „საქართველოს ბანკისგან“ მიიღეთ სპეციალური დიზაინის პლასტიკური ბარათი **ICard**.

„ჩემები“ – „ავერსი ფარმა“ – „საქართველოს ბანკის“, მისი შვილობილი კომპანიის „ბი სი აი“-ის პროექტის „ჩემები“ და „ავერსი ფარმას“ ერთობლივი სადებეტო ბარათია. ამ ბარათს ავტომატურად მიიღებს „ჩემების“ ყველა კლიენტი. მისი მეშვეობით შესაძლებელია 10%-იანი ფასდაკლების მიღება „ავერსი ფარმას“ ნებისმიერ აფთიაქში მედიკამენტების შეძენისას.

GeocellCard წარმოადგენს **Cirrus/Maestro** პლასტიკურ ბარათს. ეს ბარათი შეგიძლიათ გამოიყენოთ პროდუქციის და მომსახურების შესაძენად როგორც საქართველოში, ისე მსოფლიოს ნებისმიერ ქვეყანაში და მიიღოთ ბონუსები ჯეოსელში.

Bali Card „საქართველოს ბანკისა“ და ბალის ერთობლივი სტუდენტური ბარათია.

ელექტრონულ ფულს ქალაქის ფულთან შედარებით გააჩნია შემდეგი უპირატესობები:

1. მსოფლიოს მასშტაბით შესაძლებელია უნაღდო ანგარიშსწორების ორგანიზება.
2. მნიშვნელოვნად მცირდება კლიენტებს შორის ანგარიშსწორების დრო.

3. მარტივდება ფულის ემისის პროცესი.
4. მარტივდება ფულის ინკასაცია.
5. იზრდება ფულის მფლობელის უსაფრთხოება.
6. ფულის შესანახად აღარ იქნება საჭირო დიდი ფართობის საცავები.
7. განადგურებას გადაურჩება მილიონობით ჰექტარი ტყე.
8. აღარ იწება საჭირო ფულის გადასაზიდად სპეციალური სატრანსპორტო საშუალებები და პერსონალი.
9. აღარ იქნება საჭირო იმ უზარმაზარი თანხების გაღება, რომელიც დაკავშირებულია ქალაქის ფულის მოჭრასთან.
10. შესაძლებელია, თავიდან იქნეს აცილებული დაუსაბუთებელი ემისია.
11. მარტივდება ფულის დახურდავების პროცესი.
12. ელექტრონული ფულის შემოღება საფუძველს ჩაუყრის ერთიანი ინფორმაციულ-ფიჭური საზოგადოების აშენებას და ქვეყნებს შორის ეკონომიკური საზღვრების წაშლას.

კითხვები თვითშემოწმებისთვის

- განახორციელეთ პლასტიკური ბარათების კლასიფიკაცია სხვადასხვა ნიშნის მიხედვით.
- როდის დაიწყეს პლასტიკური ბარათების გამოყენება?
- დაახასიათეთ საქართველოს ბანკებში გამოყენებული პლასტიკური ბარათები.
- რას გამოიწვევს ელექტრონული ფულის შემოღება?

თავი 6. გადახდის სისტემები. საქონლის მიწოდებისა და გადახდის სახეები

6.1. საქონლის ტრანსპორტირებისა და გადახდის ხერხები

შეძენილი საქონლის ღირებულების გადახდის ვარიანტი დამოკიდებულია საქონლის მიწოდების ისეთ ხერხებზე როგორიცაა: ანაზღაურება ნაღდი ფულით კურიერისათვის საქონლის მიწოდების შემდეგ ან მყიდველის მიერ რეალურ მაღაზიაში საქონლის შეძენისას; ანაზღაურება საბანკო გზავნილით, ე. ი. ფულის გადარიცხვა ელექტრონული მაღაზიის ანგარიშზე; ფასდადებით ანაზღაურება წარმოებს ფოსტაში საქონლის მიღებისას, მოქმედი საფოსტო წესების მიხედვით; საფოსტო გზავნილით (ტელეგრაფით); საკრედიტო ბარათების **VISA, EuroCard/masterCard, DinersClub, cyberPlat** და **SSIST** სისტემის საშუალებით და ა.შ.

საქონლის მიწოდების ხერხებია:

- საერთაშორისო საკურიერო სამსახურით;
- მაღაზიის საკურიერო სამსახურით ან პროფესიული საკურიერო სამსახურით;
- ფოსტით (წინასწარი ანაზღაურებით ან ფასდადებით);
- მაგისტრალური ტრანსპორტის გამოყენებით;
- საერთაშორისო საფოსტო სამსახურით;
- კლიენტის ტრანსპორტით, ანუ თვითმომსახურებით;
- ინფორმაციული შინაარსის მქონე საქონლის შემთხვევაში, ტელესაკომუნიკაციო საშუალებებით.

6.2. ანაზღაურება ნაღდი ფულით. ინტერნეტში ანაზღაურების ხერხები.

ტრადიციული ანაზღაურების მეთოდები, ნაღდი ფულის ჩათვლით, საბანკო გზავნილები, ჩეკები და პლასტიკური ბარათები, გამოგონებული იყო ელექტრონული კომერციის აღმოცენებამდე. ფიზიკური საქონლის შეძენისას ფულის მიღება მყიდველისაგან შეიძლება საქონლის მიწოდების შემდეგ. თუ ყიდვა წარმოებს ციფრული სახით წარმოდგენილი საქონლის, ანუ ინფორმაციის, მაშინ საქონლის ღირებულების ანაზღაურება უნდა მოხდეს პირდაპირ ადგილზე, ანუ გამყიდველის საიტზე. ინტერნეტში ელექტრონული გზით შეძენილი საქონლის ღირებულების ანაზღაურება შესაძლებელია:

- მობილური ტელეფონის ანგარიშიდან (**Mcommerce**);
- წინასწარი ანაზღაურების ბარათების (სკრეტი-ბარათის) მეშვეობით;
- ანაზღაურება ელექტრონული ფულით;
- ანაზღაურება საგადამხდელო ბარათებით.

6.3. ანაზღაურება წინასწარ ანაზღაურების ბარათებით (სკრეტი-ბარათები)

სკრეტი-ბარათები ესაა ბარათები წინასწარი გადახდით, რაც იმას ნიშნავს, რომ, ყიდულობთ რა საქონელს, თქვენ წინასწარ ფარავთ იმ მომსახურების ან შეძენილი საქონლის ღირებულებას, რომლის შესაძენად დაკვეთა მიეცით. ასეთი სახელწოდება ამ ბარათებმა მიიღეს ინგლისური სიტყვიდან „**scratch**“. ბარათზე განსაკუთრებული დამცავი ფენა ფარავს ალფაბეტურ-ციფრულ ანანწყობს. იგი წარმოადგენს წინასწარი ანაზღაურების განსაკუთრებულ განმასხვავებელ ნიშანს. უნდა აღვნიშნოთ, რომ თითოეულ წინასწარი ანაზღაურების ბარათს გააჩნია თავისი უნიკალური ნომერი, რომელიც გამოიყენება მომსახურების ანაზღაურებისათვის. წინასწარი ანაზღაურების ბარათებს უშვებენ

სხვადასხვა ფირმები. ეს ბარათები სხვადასხვა ნომინალისა და სხვადასხვა დანიშნულებისაა. როგორც წესი, მათ გააჩნიათ შეზღუდული მოქმედების ვადა, რომელიც იცვლება ბარათის ნომინალური ღირებულებიდან, ან სხვა პირობებიდან გამომდინარე. თვით ბარათი პლასტიკურია და მასზე მითითებულია: დამამზადებელი ფირმა, გამოყენების სფერო და მოქმედების ვადა. ნინასნარი ანაზღაურების ბარათებმა ფართო გავრცელება პოვა, რადგან მომსახურების ან შეძენილი საქონლის ღირებულების გადახდის მოხერხებული ფორმაა. ასეთ ბარათებს ფართოდ იყენებენ ფიჭური კავშირებითა და ინტერნეტ-პროვაიდერების მომსახურებით დაკავებული კომპანიები, რომლებიც დაკავებული არიან ფიჭური კავშირებით და ენევიან ინტერნეტ-პროვაიდერების მომსახურებას.

საკრედიტო ბარათები. საკრედიტო ბარათი არის სახელდებული საგადამხდელო-საანგარიშსწორებო დოკუმენტი, პლასტიკური ბარათის სახით, რომელსაც გასცემს ბანკი თავის მეანაბრებზე განეული მომსახურების ან შეძენილი საქონლის ღირებულების ასანაზღაურებლად საცალო ვაჭრობის ქსელში, სადაც ფუნქციონირებს კომპიუტერული მონეობილობები, რომლებიც გადაიცემა მოთხოვნა ბანკში საქონლის ღირებულების გადასახდელად. საკრედიტო ბარათი ადასტურებს ბანკში მისი მფლობელის მიმდინარე ანგარიშის არსებობას. სხვადასხვა ქვეყანაში გამოყენებაშია აშშ-ის საფინანსო-საკრედიტო **VISA, MasterCard, American Express** და სხვა ჯგუფის პლასტიკური ბარათები.

სადებეტო ბარათები. სადებეტო ბარათები შეიძლება გამოყენებულ იქნეს ინტერნეტის საშუალებით ონლაინრეჟიმში შეძენილი საქონლის ან განეული მომსახურებისათვის ფულის გადასახდელად ან ბანკომატიდან ნაღდი ფულის გამოსატანად. ფულის გამოსატანად ბარათის მფლობელმა ბანკომატში უნდა შეიტანოს PIN-კოდი.

ვირტუალური ბარათები. რადგან კლასიკური საკრედიტო ბარათებით ინტერნეტის მეშვეობით ანგარიშსწორება არ არის უსაფრთხო, ამიტომ შეიმუშავეს ვირტუალური ბარათები – **VI-SAE-c@rd** და **VISA Master Card**, რომელთა დანიშნულებაა მთელ

მსოფლიოში ინტერნეტის მეშვეობით ანგარიშსწორების განხორციელება. საერთაშორისო საგადასახდელო სისტემები – ეს ისეთი სისტემებია, რომლითაც მთელ მსოფლიოში სარგებლობს მილიონობით ადამიანი. ასეთი სისტემებისათვის არ არსებობს სახელმწიფო საზღვრები – ამ ბარათებით შეიძლება გადახდა განხორციელდეს მსოფლიოს, მილიონობით სავაჭრო წერტილში, ნაღდი ფულის მიღება კი შესაძლებელია მსოფლიოში მოქმედი ასობით ათასი ბანკომატიდან. დღეისათვის მსოფლიოში ყველაზე ცნობილ საგადასახდელო სისტემებს მიეკუთვნებიან: **VISA, MasterCard-ი, American Express-ი, DinersClub-ი** და სხვ.

სისტემა **VISA** ყველაზე პოპულარულია მთელ მსოფლიოში. ამ სისტემით 72-ზე მეტ ქვეყანაში სარგებლობს მილიონობით მომხმარებელი. კლიენტებს მომსახურებას უწევს 20 ათასზე მეტი ბანკი. საქართველოში ამ სისტემის გამოყენება დაიწყო 17 წლის წინ. **VISA**-ს სხვადასხვა კატეგორიის მომხმარებლისათვის შემუშავებული აქვს მთელი რიგი საგადასახდელო ბარათები. **VISA** არის გადახდისა და ნაღდი ფულის მიღების ყველაზე მოხერხებული და საიმედო, როგორც ყოველდღიური გამოყენების, ასევე მგზავრობისათვის.

VISA-ას დანიშნულებაა ინტერნეტის მეშვეობით მსოფლიოს ნებისმიერ ელექტრონულ მაღაზიაში შეძენილი საქონლის ღირებულების ან მომსახურების გადახდა. მისი საშუალებით შესაძლებელია მობილური ოპერატორის, ინტერნეტპროვაიდერის, ტურისტული კომპანიების, სასტუმრო ბიზნესის მომსახურების საფასურის გადახდა.

EuroCard/MasterCard-ი ბარათები ორიენტირებულია საშუალოდ უზრუნველყოფილი მოქალაქეებისათვის, რომლებიც პერიოდულად მიემგზავრებიან საზღვარგარეთ, იძენენ საქონელს, იხდიან სასტუმროს ან რესტორანის მომსახურების ხარჯებს. აღნიშნული ბარათები გადახდის თანამედროვე მოხერხებული საშუალებაა, იგი მსოფლიოში სარგებლობს დიდი პოპულარობით, უზრუნველყოფს ფულადი საშუალებების უსაფრთხო შენახვის მაღალ ხარისხს.

6.4. ინტერნეტგადახდის სისტემა

საკრედიტო გადახდის სისტემის საფუძველს წარმოადგენს საკრედიტო ბარათების გამოყენება. „ელექტრონულ ბაზარზე“ ერთჯერადი ყიდვის განხორციელებისათვის, ბარათი მოქმედებს ისე, როგორც ჩვეულებრივ მაღაზიაში საქონლის შეძენისას. კლიენტი იძენს საქონელს ან მომსახურებას, აწვდის თავის საკრედიტო ბარათის ნომერს გამყიდველს. ყველაფერი ხდება ინტერნეტის მეშვეობით. მონაცემების ასეთი წესით გადაცემა აუცილებელს ხდის, გავატაროთ უსაფრთხოების დამატებითი ღონისძიებები (შეტყობინების დაშიფრვა, ციფრული ხელმოწერა და ა.შ.). ინტერნეტის მეშვეობით გადახდის სქემას აქვს შემდეგი სახე:

- მყიდველი „ელექტრონული მაღაზიის“ მთავარ გვერდზე ირჩევს სასურველ საქონელს ან მომსახურებას და გზავნის მას „კალათაში“, ირჩევს ანაზღაურების სახეს – „საკრედიტო ბარათი“;

- ავტორიზაციის მიზნით, ბარათის რეკვიზიტები (ნომერი, მფლობელის სახელი, მოქმედების ბოლო ვადა) გადაეცემა ინტერნეტის საგადამხდელო სისტემას. ამ დროს ხდება საკრედიტო ბარათის მონაცემების შეტანა მაღაზიის საიტზე, რომელიც შემდეგ გადაეცემა საგადამხდელო სისტემის სერვერს; აგრეთვე შესაძლებელია ამ მონაცემების შეტანა საგადამხდელო სისტემის სერვერზე. მყიდველისათვის მეორე ხერხით მონაცემების შეტანა უფრო უსაფრთხოა, რადგანაც მცირდება ბარათის შესახებ მონაცემების „გადინების“ რისკი;

- ინტერნეტსაგადამხდელო სისტემა ავტორიზაციის მიზნით დაკვეთას გადასცემს საპროცესინგო ცენტრს, ავტორიზაციის შედეგი გადაეცემა ინტერნეტ-საგადასახადო სისტემას, გამყიდველი და მყიდველი ღებულობენ ავტორიზაციის შედეგს. ავტორიზაციის დადებითი პასუხის შემთხვევაში მაღაზია მყიდველს მოემსახურება ან გადატვირთავს საქონელს. საპროცესინგო ცენტრი შესრულებული ტრანზაქციის მონაცემებს გადასცემს საანგარიშსწორებო ბანკს. ფული მყიდველის ანგარიშიდან გადაირიცხება მაღაზიის ანგარიშზე.

6.5. ინტერნეტგადახდის სისტემები: სადებეტო სქემები

ინტერნეტის მეშვეობით სადებეტო გადახდის სისტემა ონლაინრეჟიმში ისევე მუშაობს, როგორც მისი წინამორბედი ოფლაინური – ჩეკებითა და ნაღდი ფულით ანგარიშსწორების სისტემები. ანგარიშსწორებაში მონაწილეობენ ემიტენტი და მომხმარებელი. ემიტენტი უშვებს საფულეს რალაც ელექტრონულ ერთეულს, ბანკში ანგარიშზე ან ჩეკზე არსებული ფულის ციფრულ ეკვივალენტს. მომხმარებელი გადახდას ახორციელებს ინტერნეტის მეშვეობით, იყენებს რა მოცემულ საფულეს ელექტრონულ ერთეულებს.

ელექტრონული ჩეკები ჩვეულებრივი ქალაქის ჩეკების ანალოგია. ეს არის მომხმარებლის მიწერილობა ბანკისათვის თანხის გადარიცხვის შესახებ მისი ანგარიშიდან ფულის მიმღების ანგარიშზე. ელექტრონული ჩეკის წიგნის მფლობელი ელექტრონულ ჩეკზე დაფიქსირებულ თანხაზე ანერს ხელს, ელექტრონული ფორმით, ასეთი სახით გაფორმებული ელექტრონული ჩეკი მიმღებს გადაეცემა ნებისმიერი სახით. მიმღები მას ნარაღგენს სისტემაში ასანაზღაურებლად. თუ შემომწმების შედეგად დადასტურდა ჩეკის ნამდვილობა, მაშინ გადამხდელს მიეცემა საქონელი ან გაენწევა მომსახურება, ფულის გადარიცხვა მოხდება მყიდველის ანგარიშიდან გამყიდველის ანგარიშზე. ასეთი გადახდის სისტემებია: **NetCash-ი, NetChex-ი, NetCheque.**

6.6. კლიენტის კომპიუტერის „ელექტრონულ საფულეზე“ მომუშავე სისტემები

იმისათვის, რომ ქსელის საშუალებით თავისუფლად განხორციელდეს ელექტრონული ფულის გაცვლა, ამ სისტემის მონაწილენი თავიანთ კომპიუტერებზე აყენებენ განსაკუთრებულ პროგრამას – „ელექტრონულ საფულეს“, რომელიც უზრუნველყოფს ელექტრონული ფულის აღრიცხვას, გადაცემას და ნამდვილობის კონტროლს. „ანგარიშის“ შევსება შესაძლებელია ან წინასწარი ანაზღაურების ბარათით, ან კიდევ ბანკის მეშვეობით,

გადარიცხვის წესით. თუ კლიენტი თავისი ელექტრონული საფულედან „ნაღდი“ ელექტრონული ფულით იხდის, მაშინ ამის განხორციელება წარმოებს შემდეგნაირად: კლიენტი რეგისტრირდება იმ სისტემაში, რომელიც მუშაობს ციფრულ ფულთან, თავის კომპიუტერზე აყენებს შესაბამის პროგრამულ უზრუნველყოფას და ააქტიურებს „ელექტრონულ საფულეს“ კლიენტი საქონლის შესაძენად გამყიდველის სერვერზე გადარიცხავს ელექტრონულ ფულს; ელექტრონული კუპიურები წარედგინება ემიტენტს, რომელიც ამოწმებს მის ნამდვილობას, შემდეგ გამყიდველის ანგარიშზე ჩაირიცხება შესაძენი საქონლის ღირებულება, მყიდველს კი გაეგზავნება შეძენილი საქონელი ან გაენევა მომსახურება.

ელექტრონული ფულის თავისებურება ისაა, რომ შესაძლებელია მისი კონვერტირება რეალურ ფულში. ელექტრონული ფულით სარგებლობას, სხვა გადახდის სისტემებთან შედარებით გააჩნია ბევრი დადებითი თვისება. კერძოდ: გამოყენების სიმარტივე; უსაფრთხოების მაღალი დონე; მიკრო-გადახდების შესაძლებლობა; განხორციელებული ტრანზაქციის სიიაფე. ელექტრონული ფულით სარგებლობისას მის მფლობელს არ მოეთხოვება პიროვნების და კრედიტუნარიანობის დადასტურება. ამ სისტემის უარყოფით მხარეს წარმოადგენს „ელექტრონული საფულეს“ წინასწარი შევსების აუცილებლობა.

6.7. სმარტ-ბარათებზე მომუშავე სისტემები

სმარტ-ბარათი (**smart-card**) – ეს არის პლასტიკური ბარათი ჩაშენებული მიკროპროცესორით. სმარტ-ბარათებს უშვებენ ბანკები. ბარათის ჩიპზე ინახება მყიდველის საბანკო ანგარიშის შესახებ ინფორმაცია (ანგარიშის ნომერი, თანხა და ინფორმაცია ემიტენტის, მყიდველის შესახებ). ბანკის მიერ მყიდველის ანგარიშ-ბარათიდან თანხა ჩამოინერება საქონლის შეძენის ან მომსახურების განევის შემდეგ. შესაბამისი თანხა გადაირიცხება გამყიდველის ანგარიშზე. შესყიდვის ოპერაციის განხორციელებისას შესაბამისი ცვლილებები მოხდება სმარტ-ბარათზე.

სმარტ-ბარათის ბალანსის შევსება ხდება შემდეგნაირად: ემიტენტბანკში მფლობელის ანგარიშბარათზე წარმოებს თანხის ჩანერა, რომელიც ჩამოინერება სმარტ-ბარათის მფლობელის ჩვეულებრივი ანგარიშიდან ან თანხა შემოდის ნაღდი ფულის სახით. ბარათი შეიძლება გამოყენებულ იქნეს, როგორც გადახდის საშუალება როგორც ინტერნეტში, ასევე ავტონომიური მოწყობილობის მიერ.

სმარტ-ბარათებს გააჩნიათ დაცულობის უფრო მაღალი ხარისხი და მოხერხებულია მომხმარებლისათვის უფრო ვიდრე ჩვეულებრივი პლასტიკური ბარათები მაგნიტური ზოლით. მათი ფართოდ გავრცელება ჯერჯერობით ფერხდება მაღალი თვითღირებულების გამო. დღეისათვის საზღვარგარეთ ყველაზე გავრცელებულია **Mondex**-ის სისტემის ბარათები. ინტერნეტის მეშვეობით სმარტ-ბარათით გადახდისათვის მომხმარებელს ინფორმაციის წასაკითხად და მასზე ცვლილებების შესატანად უნდა ჰქონდეს სპეციალური მოწყობილობა.

6.8. უნივერსალური ელექტრონული ბარათები

უნივერსალური ელექტრონული ბარათები (უებ) – ანუ მულტიპლიკაციური ბარათები, რომელთა დანიშნულებაა სხვადასხვა ელექტრონული მომსახურების გაწევა ონლაინრეჟიმში. ამ ბარათს შეუძლია შეითავსოს ისეთი დოკუმენტების ფუნქციები, როგორიცაა: პასპორტი და მართვის მოწმობა; მისი საშუალებით შესაძლებელია დისტანციური დაკავშირება სახელმწიფო და კომერციულ სტრუქტურებთან; გამოიყენება, როგორც სადებეტო და საკრედიტო ბარათები; ბანკომატიდან ნაღდი ფულის მიღების საშუალება; საყოფაცხოვრებო მომსახურებისათვის საჭირო თანხების გადახდა; ქალაქის ტრანსპორტით მგზავრობის ღირებულების ანაზღაურება; ინტერნეტვაჭრობა; ვაჭრობის წერტილებში საქონლის შეძენა და სხვ.

დღეისათვის მსოფლიოს მრავალ ქვეყანაში გამოყენებულია **უებ**-ის სხვადასხვა მოდიფიკაცია. ამის კარგი მაგალითია ფინეთში სმარტ-ბარათების საფუძველზე აგებული სისტემა **FinEIDD**-ი, რომლის დახმარებითაც შესაძლებელია ელექტრო-

ნული ხელმონერის, სახელმწიფო და კომერციულ სტრუქტურებთან ონლაინრეჟიმში კავშირის განხორციელება.

მაღაზიაში **უებ**-ის დანერგვა დაიწყო 1999 წლიდან. აღნიშნული **უებ**-ის სახელწოდებაა **MyKad**-ი. იგი ცვლის პირადობის და ტრანსპორტის მართვის მოწმობებს, მისი გამოყენება ამარტივებს მოქალაქეების საზღვარგარეთ გასვლისა და შემოსვლის კონტროლს აღნიშნულ ქვეყანაში. **MyKad** საშუალებას აძლევს მოქალაქეებს, ონლაინრეჟიმში დაუკავშირდნენ სახელმწიფო და კომერციულ სტრუქტურებს. იგი გამოიყენება, როგორც საგადამხდელო დოკუმენტი, ტრანსპორტით მგზავრობისათვის ღირებულების გადახდის საშუალება, ავტოტრანსპორტის პარკირებისათვის გადახდის საშუალება და ბანკომატიდან ნაღდი ფულის მისაღებად. მასზე აგრეთვე ინახება მოქალაქის სამედიცინო მონაცემები.

1999 წლიდან დიდ ბრიტანეთში ფართოდ გამოიყენება ფირმა **Smartex**-ის მიერ შემუშავებული **უებ – Citizens Card**. იგი გამოიყენება როგორც მკითხველის ბარათი, როგორც ბილეთი სხვადასხვა სახის ტრანსპორტზე, საქონლის შესაძენად და განეული მომსახურების ანაზღაურებისათვის.

სამხრეთ კორეაში 2000 წლიდან დაიწყო სმარტ-ბარათ **Mifare Pro**-ს გამოყენება. მისი საშუალებით შესაძლებელია ელექტრონული ხელმონერის განხორციელება, მაღაზიაში შეძენილი საქონლის ღირებულების ანაზღაურება. იგი ასრულებს საკრედიტო და სადებეტო ბარათების ფუნქციას. მისი დახმარებით შესაძლებელია ინტერნეტვაჭრობის განხორციელება, მუნიციპალურ ტრანსპორტზე ბილეთების შეძენა და სხვ.

ჰონგკონგში 1994 წლიდან დაიწყო **უებ – Octopus**-ი. იგი გამოიყენება ქალაქის ყველა სახის ტრანსპორტით მგზავრობის ღირებულების ასანაზღაურებლად, როგორც „ელექტრონული საფულე“ მაღაზიაში საქონლის შესაძენად, სასაუზმეებში და კაფეებში მომსახურების ასანაზღაურებლად.

იტალიაში, რომში, **უებ – Metro bus**-ი – გამოიყენება ყველა სახის მუნიციპალური ტრანსპორტით მგზავრობის ღირებულების ასანაზღაურებლად.

კითხვები თვითშემოწმებისთვის

1. ინტერნეტგადახდის რა სახებია ცნობილი?
2. როგორ ხდება წინასწარი ანაზღაურება სკრეი-ბარათით?
3. როგორ ხდება შეძენილი საქონლის ელექტრონული ფულით გადახდა?
4. რას წარმოადგენს საკრედიტო ბარათები?
5. რას წარმოადგენს სადებეტო ბარათები?
6. დაახასიათეთ ინტერნეტგადახდის სისტემა.
8. დაახასიათეთ კლიენტის კომპიუტერის „ელექტრონულ საფულეზე“ მომუშავე სისტემები.
9. რას წარმოადგენს სმარტ-ბარათებზე მომუშავე სისტემები?
10. დაახასიათეთ მსოფლიოს სხვადასხვა ქვეყანაში გამოყენებული უნივერსალური ელექტრონული ბარათები.

თავი 7. ელექტრონული ფული

7.1. ციფრული ფულის ცნება და ინტერნეტში ციფრული ფულით გადახდები

ციფრულ ფულში იგულისხმება ქალაქის ბანკნოტების ანალოგი. ციფრული „კუპიურა“ (შემდეგში კუპიურა) წარმოადგენს ციფრების (ბიტების) კრებულს, რომელიც ჩანერილია მონაცემების ელექტრონულ მატარებლებზე. თითოეული კუპიურა შეიცავს მონაცემებს კუპიურის ნომინალისა და ემიტენტის შესახებ. ციფრული ნაღდი ფულის ემიტენტის როლში, როგორც წესი, გვევლინება კომერციული ბანკი, თუმცა ეს ფუნქცია შეიძლება შეასრულოს ციფრული ნაღდი ფულით ანგარიშსწორების ორგანიზატორმაც. ემიტენტს შეუძლია თვითონ შექმნას ციფრული კუპიურები, მასზე ელექტრონული ხელმოწერით და კავშირის არხებით გაუგზავნოს ანგარიშსწორებაში მონაწილეებს. კუპიურების ემისია შესაძლებელია სხვა ხერხითაც. ბანკის კლიენტი (ანგარიშსწორების სისტემის მონაწილე) თვითონ ქმნის საჭირო კუპიურის ციფრულ ნომინალს, გადაუგზავნის ბანკს ან ორგანიზატორ ემიტენტს, სადაც წარმოებს კლიენტის ანგარიშის შემოწმება და ემიტენტის ელექტრონული ციფრული ხელმოწერა. კლიენტისთვის დაბრუნებული ციფრული ხელმოწერილი კუპიურა შეიძლება გამოყენებულ იქნეს ანგარიშსწორებისთვის ან გადაეგზავნოს საქონლის/მომსახურების გამყიდველს, ან ფულადი საშუალებების სხვა მიმღებს. ციფრული ფულის შენახვა შესაძლებელია ორი წესით:

პირველი, ციფრული ფული ინახება სმარტ-ბარათებზე. ასეთ სისტემაში ანგარიშსწორებისთვის გადამხდელსაც და მიმღებსაც უნდა ჰქონდეს სპეციალური მონყობილობა, რომელიც განახორციელებს ციფრული ფულის ჩანერას სმარტ-ბარათზე ან გაატანას სმარტ-ბარათიდან სხვა მონყობილობაზე. მონყობილობას, რომლის საშუალებითაც შესაძლებელია სმარტ-ბარათზე შენახული ციფრული ფულის დათვალიერება, ეწოდება „ელექტრონული საფულე“. სისტემის სახედან გამომდინარე, „ელექ-

ტრონულ საფულეს“ შეუძლია ციფრული კუპიურების გადატანა ერთი სმარტ-ბარათიდან მეორეზე.

არსებობს სისტემები, რომლებიც ითვალისწინებენ ციფრული ფულის შენახვას ფაილის სახით სტანდარტულ მაგნიტურ დამგროვებელზე (მყარი დისკი, დისკეტა, ფლემ-ბარათი და ა.შ.). ასეთი სისტემებით მუშაობისას არ არის საჭირო, მყიდველსა და გამყიდველს ჰქონდეს სპეციალური ტექნიკური საშუალება, გარდა პერსონალური კომპიუტერისა.

დღეისათვის არსებობს სისტემები, რომელთა საშუალებითაც შესაძლებელია ისეთი მოწყობილობის გამოყენება როგორიცაა ბარათ-რიდერი მიერთებული პერსონალურ კომპიუტერთან. აღნიშნულ მოწყობილობას შეუძლია სმარტ-ბარათიდან ნაიკითხოს მონაცემები და გადასცეს ქსელის საშუალებით. თუმცა ციფრული ფულით ანგარიშსწორების ყველა სისტემას არ შეუძლია განახორციელოს ქალაქის ფულის მიერ შესრულებული ყველა ტექნოლოგია.

საგადამხდელო სისტემის ორგანიზატორი (საპროცესინგო ქვესისტემაში) ან სმარტ-ბარათზე ინახავს მონაცემებს იმის შესახებ, რომ სისტემის თითოეულ მომხმარებელს რა რაოდენობის თანხის ფარგლებში შეუძლია გადახდა. ამ შემთხვევაში მომხმარებელში იგულისხმება ცალკეული იდენტიფიკატორი. კონკრეტულ მომხმარებელს შეიძლება ეკუთვნოდეს რამდენიმე ასეთი იდენტიფიკატორი. გადამხდელი გადახდის მომენტში ახორციელებს ციფრული ფულის გენერაციას მისთვის საჭირო ნომინალში. ასეთი სახით წარმოებს ბანკნოტების დახურდავება. ამით იგი განსხვავდება ქალაქის ფულით ანგარიშსწორებისაგან. ე.ი. გადამხდელისთვის არ არის აუცილებელი, წინასწარ იქონიოს კუპიურა ან კუპიურების ნაკრები, რომლითაც განახორციელებს ანგარიშსწორებას, ფულის მიმღები კი თავისუფლდება ვალდებულებისაგან ჰქონდეს დასახურდავებლად საჭირო კუპიურები.

მხედველობაში უნდა მივიღოთ, რომ ანგარიშსწორების განხილული სისტემების მონაწილენი თავიანთ მფლობელობაში ღებულობენ, მართალია „ციფრულ“, მაგრამ ნაღდ ფულს, რომელიც, როგორც ქალაქის ნაღდი ფული, შეიძლება დაიკარგოს. მაგ., თუ კომპიუტერის ინფორმაციის დამგროვებელი (ვინ-

ჩესტერი ან მეხსიერების სხვა მონყობილობა, გამოვა მწყობრიდან ან მას ვინმე მოიპარვს, მაშინ მისი მფლობელი დაკარგავს ფულს მთლიანად, რომელიც მან გადაიყვანა თავის კომპიუტერში და ვერ მოასწრო გამოყენება. უფრო მეტიც, აღარ ექნება სმარტ-ბარათი, მეორე მხრივ, ემიტენტს არ შეეძლება ხელი შეუშალოს სმარტ-ბარათზე განთავსებული ფულის გამოყენებას. აღნიშნული შესაძლებელია მხოლოდ მაშინ, თუ ანგარიშსწორების სისტემა შეწყვეტს ფუნქციონირებას. ეს უკანასკნელი მიმზიდველია იმით, რომ, თუ სასამართლო დაბლოკავს ბანკში სმარტ-ბარათის მფლობელის ანგარიშს, სმარტ-ბარათის მფლობელი მაინც შეძლებს მასზე განთავსებული ფულის დახარჯვას¹.

ციფრული ფულით ანგარიშსწორების სქემა შემდეგია: იმისათვის, რომ მომხმარებელს მიეცეს შესაძლებლობა, გადაიხადოს ან მიიღოს ციფრული ფული, აუცილებელია დარეგისტრირდეს ანგარიშსწორების მოცემულ სისტემაში და მიიღოს სპეციალური მონყობილობა სმარტ-ბარათებთან სამუშაოდ ან ჰქონდეს სპეციალური პროგრამული უზრუნველყოფა. ისეთ სისტემებში, რომელიც იყენებს პერსონალურ კომპიუტერს და ინტერნეტს, ციფრული ფულით ანგარიშსწორება შეუძლიათ მხოლოდ იმ პირებს, რომლებიც დარეგისტრირებული არიან კონკრეტულ საგადამხდელო სისტემაში. შემდეგ წარმოებს ციფრული ფულის მიღება, რაც მიიღწევა ნაღდი ქაღალდის ფულის ციფრულ ფულში კონვერტაციის საფუძველზე. სხვადასხვა საგადამხდელო სისტემაში სხვადასხვაა კონვერტაციის ხერხი. მაგრამ, როგორც წესი, ყველგან არის გათვალისწინებული სისტემის ორგანიზატორის ანგარიშზე ფულადი საშუალებების გადაყვანა ციფრულ ფულში, რომლის დროსაც მიეთითება კლიენტის იდენტიფიკატორი. გადაყვანილი ციფრული ფული შემდეგ განთავსდება სმარტ-ბარათზე ან კომპიუტერში.

ციფრული ფულით ანგარიშსწორება უცხო ქვეყნის ტერიტორიაზე წარმოებს ქაღალდის ნაღდი ფულის ანალოგიურად. ამ შემთხვევაში აუცილებელია მისი წინასწარი კონვერტაცია (ნაღ-

¹ Бафинковские информационные ситемы: Учебник./ Под редакцией профессора В. В. Дика. М: Маркет ДС, 2006.გვ. 455.

დი ან უნაღდო ფორმით). ხდება ფულის გადაყვანა ერთი ვალუტიდან მეორე ვალუტაში. იგი დროებით ხდება უცხოური ნაღდი ფულით ანგარიშსწორების სისტემის მონაწილე. მას შემდეგ, რაც მყიდველი და გამყიდველი შეთანხმდებიან ანაზღაურების წესზე, სმარტ-ბარათიდან ან კომპიუტერიდან ციფრული ფული გადაადგილდება მიმღების ანალოგურ მატარებელზე. ციფრული ნაღდი ფულის გადაადგილების ხერხი დამოკიდებულია კონკრეტულ სისტემაზე. ციფრული ფულით ანგარიშსწორების პროცედურა შეიძლება რამდენიმეჯერ გავიმეოროთ. თუ ანგარიშსწორებაში მონაწილე ერთ-ერთი მხარე გადაწყვეტს შეწყვიტოს ანგარიშსწორება ციფრული ფულით ან თუ მას გაუჩნდება სურვილი, ციფრული ფულის ნაწილი გადაიყვანოს ქალაქის ნაღდი ფულში, წარმოებს ციფრული ფულის კონვერტაცია. აღნიშნული პროცედურა ქალაქის ნაღდი ფულის ციფრულ ფულში კონვერტაციის საპირისპიროა, რომელიც შეიძლება განხორციელდეს მხოლოდ სისტემასთან მიერთების შემთხვევაში. აქაც შეიძლება ადგილი ჰქონდეს რამდენიმე ვარიანტს. ჩვეულებრივ, ციფრული ფულის ჩამონერა წარმოებს სმარტ-ბარათიდან ან კომპიუტერიდან და რეალური ფულის ჩარიცხვა ხდება სისტემის მონაწილის მიერ მითითებულ ანგარიშზე. ანგარიშის მფლობელს შეუძლია ამ ანგარიშიდან ნაღდი ფულის მიღება ან უნაღდო ანგარიშსწორების განხორციელება (მაგალითად, საგადასხდელო დავალების დახმარებით).

სმარტ-ბარათს, რომელზედაც ციფრული ფული ინახება ეწოდება „ელექტრონული საფულე“ (როგორც წესი, სმარტ-ბარათზე ფულის ჩანერა წარმოებს სპეციალური ტერმინალის (ბანკომატის) საშუალებით, რომლის მფლობელიცაა ანგარიშსწორების სისტემის ორგანიზატორი. სისტემის კლიენტი იმ ბანკში, რომელიც ემსახურება საგადასხდელო სისტემას ხსნის ანგარიშსწორების ანგარიშს, რომელზედაც ჩარიცხავს ფულს. შემდეგ სპეციალური საბანკო ტერმინალის საშუალებით, რომელიც წარმოადგენს ბანკომატის ნაირსახეობას, ანგარიშსწორების ანგარიშიდან ციფრულ ფულს გადაიტანს სმარტ-ბარათზე. აღნიშნული პროცედურის შესრულება აგრეთვე შესაძლებელია სპეციალური ტელეფონის საშუალებით, რომლის შემადგენლო-

ბაშიც შედის ბარათ-რიდერი. სმარტ-ბარათზე არსებული ნაშთის გაზრდა ან ჩამოწერა შესაძლებელია რამდენიმეჯერ.

აღნიშნული ბანკომატის საშუალებით აგრეთვე შესაძლებელია ქალაქის ნაღდი ფულის მიღებაც და სმარტ-ბარათიდან საბანკო ანგარიშზე თანხის გადატანა. რადგან ინფორმაცია ციფრული ფულის რაოდენობის შესახებ ინახება მხოლოდ სმარტ-ბარათზე, ეს თანხა არ ექვემდებარება ბლოკირებას, ანუ სმარტ-ბარათის დაკარგვის შემთხვევაში თქვენ კარგავთ მასზე განთავსებულ ფულად საშუალებებს. ციფრული ფულის ეს თვისება საშუალებას იძლევა, უზრუნველყოფილ იქნეს ანგარიშსწორების ანონიმურობა. ანაზღაურების მომენტისთვის სმარტ-ბარათის მფლობელს შეუძლია გადახდა, თუ მან იცის ბარათის მექანიერებაში შესვლის პირადი კოდი, ამ შემთხვევაში ინფორმაციის დაცვის სხვა საშუალება არ არსებობს.

სმარტ-ბარათებით ანგარიშსწორებისთვის აუცილებელია, გაგვაჩნდეს სპეციალური ტექნიკური მოწყობილობა, რომელშიც იდება სმარტ-ბარათები. გადამხდელისა და მიმღების პირადი კოდისა და გადასაცემი თანხის შეყვანის შემდეგ გადაგზავნილი თანხის ოდენობით მცირდება გადამხდელის სმარტ-ბარათზე არსებული თანხა და იმავე თანხით იზრდება მიმღების სმარტ-ბარათზე არსებული ნაშთი.

მაღაზიაში დაყენებული **POS**-ტერმინალის, საშუალებითაც შესაძლებელია მხოლოდ გადამხდელის სმარტ-ბარათიდან ციფრული ნაღდი ფულის შეტანა **POS**-ტერმინალის მექანიერებაში. მოგვიანებით შესაძლებელია **POS**-ტერმინალში შენახული ციფრული ფულის გადანერა სმარტბარათზე, ან სხვა სახის მაგნიტურ დამაგროვებელზე, ან მთლიანად გადაცემა ბანკში, რათა ის გადაიცვალოს ქალაქის ნაღდი ფულზე, რომელსაც ბანკი ჩაურიცხავს გამყიდველს ანგარიშსწორების ანგარიშზე. ბარათ-რიდერის გამოყენებით გაფართოვდა სმარტ-ბარათების გამოყენების საგადამხდელო სისტემა. ამ შემთხვევაში პერსონალური კომპიუტერი ცვლის ტერმინალ-ბანკომატს ციფრული ფულის ჩაწერის ან ჩამოწერის ოპერაციების შესრულებისას. სმარტ-ბარათების საფუძველზე აგებული საგადამხდელო სისტემებისაგან განსხვავებით ინტერნეტსაგადამხდელო სისტემებს

ინტერნეტის გარემოში შეუძლიათ მხოლოდ ფინანსური ოპერაციების შესრულება. მსგავს სისტემებში ყველა კლიენტი თანასწორუფლებიანია. ეს იმას ნიშნავს, რომ, თუ გინდა ფულადი საშუალებების გაგზავნა ან ანაზღაურების მიღება, არ არის საჭირო სტატუსის წინასწარი მიღება. ანგარიშსწორებისთვის მყიდველიც და გამყიდველიც სარგებლობს სპეციალური პროგრამული უზრუნველყოფით, რომელსაც ზოგიერთ სისტემაში „ელექტრონულ საფულეს“ უწოდებენ.

პროგრამის ფუნქციებია: ციფრული კუპიურების გენერაცია და მასზე ციფრული ელექტრონული ხელმოწერის განხორციელება; ციფრული კუპიურის გაგზავნა მიმღებთან; გადამხდელისგან ციფრული კუპიურის მიღება და მისი გადაგზავნა სისტემის ორგანიზატორის სერვერზე, კუპიურის ნამდვილობის დასადაგენად ციფრული კუპიურის ნამდვილობის შესახებ ინფორმაციის მიღება; ციფრული ფულის მფლობელის კომპიუტერზე ნაშთის შენახვა და შეცვლა; მომხმარებლის მოთხოვნის მიხედვით ციფრულ ფულზე შესრულებული ოპერაციების შესახებ ანგარიშგების მიღება.

7.2. ჩეკებით ანგარიშსწორება

საბანკო პლასტიკური ბარათებით ანგარიშსწორების საფუძველს წარმოადგენს ჩეკებით უნაღდო ანგარიშსწორება. მოკლედ აღვწეროთ ჩეკებით ანგარიშსწორების ტექნოლოგია.

კლიენტი კომერციულ ბანკთან დებს ხელშეკრულებას ჩეკების გამოყენებით ანგარიშსწორების შესახებ. ამისთვის კლიენტს უხსნიან ანგარიშსწორების ანგარიშს, კლიენტი ღებულობს ჩეკების წიგნაკს – მკაცრი ანგარიშსწორების დოკუმენტს. შინაარსობრივად ეს წიგნაკი წარმოადგენს საბრუნავ-საღებურ უწყისს. ბრუნვა ატარებს მხოლოდ გასავლის ოპერაციის სახეს. ყოველი შესრულებული ოპერაციის შემდეგ საღებო ფიქსირდება ჩეკის ყუაზე. შემოსავლის ოპერაციას ადგილი აქვს კლიენტის მიერ ანგარიშზე ფულის შეტანისას. რამდენადაც ჩეკების საფუძველზე განხორციელებული ანგარიშსწორება წარმოადგენს საბარათო ანგარიშსწორების საფუძველს, მის ანალოგს, ხელშეკრულებაში

დამატებით მიეთითება ანგარიშიდან ერთჯერადად ან დღე-ღამის განმავლობაში თანხის მოხსნის ლიმიტი, რაც ამცირებს კლიენტის ანგარიშიდან არასანქცირებული ფულადი სახსრების მოხსნის რისკს.

კლიენტი საქონლის შეძენისას ჩეკზე აფიქსირებს გადასახდელი თანხის რაოდენობას, ოპერაციის შესრულების თარიღს და ხელმოწერას. ანგარიშსწორება ჩეკებით ნიშნავს კლიენტის მიერ სასაქონლო ფორმით სესხის მიღებას, ანუ ადგილი აქვს განსაზღვრული სახით საკრედიტო რისკის აღმოცენებას. სწორედ ამის გამო გახდა აუცილებელი ავტორიზაციის განხორციელება, გამყიდველის დაკავშირება იმ ბანკთან, სადაც კლიენტს გახსნილი აქვს ანგარიშსწორების ანგარიში.

გამყიდველს შეუძლია გაყიდვის ოპერაციის განმავლობაში მოახდინოს მყიდველის იდენტიფიკაცია და ავტორიზაცია. შემდეგ გამყიდველი ჩეკს გადასცემს ბანკ – ემიტენტს (ახდენს ინკასაციას). ეს უკანასკნელი, გამყიდველის თხოვნის საფუძველზე, ინკასოს მოთხოვნას წარადგენს მყიდველის ბანკში (ემიტენტის ან მყიდველის ბანკში). ფული გადაირიცხება ბანკ-მყიდველის ანგარიშიდან ბანკ-ემიტენტის ანგარიშზე და ჩაირიცხება გამყიდველის ანგარიშზე.

7.3. ვირტუალურ ანგარიშებზე დაფუძნებული საგადამხდელო ინტერნეტის სისტემები

ვირტუალურ ანგარიშში იგულისხმება ინტერნეტ-საგადამხდელო სისტემის ორგანიზატორის სერვერზე სააღრიცხვო ჩანაწერი (აქაუნთი). ეს სააღრიცხვო ჩანაწერი მოიცავს მონაცემებს კლიენტისა და ფულადი საშუალებების ეკვივალენტის შესახებ, რომლის ფარგლებშიც კლიენტს შეუძლია განახორციელოს გადახდები. შინაარსობრივად ვირტუალური ანგარიში ძალიან ჰგავს საბანკო ანგარიშს, მაგრამ მისი გახსნა და მომსახურება წარმოებს არასაბანკო ორგანიზაციების მიერ. აღრიცხვის ერთეულის როლში გამოდის არა ფულადი ერთეულები, არამედ პირობითი ერთეულები. ვირტუალური ანგარიშის გახსნა ნიშნავს სა-

აღრიცხვო ჩანაწერის შექმნას და მისთვის იდენტიფიკატორის მინიჭებას. მომსახურებაში კი იგულისხმება: ფულადი საშუალებების ნაშთის ცვლილება შესრულებული ოპერაციის შენახვა, ანგარიშის მიხედვით ნაშთის შეცვლა, ვირტუალური ანგარიშის მიხედვით განხორციელებული ოპერაციების შესახებ კლიენტისთვის ამონაწერის მიწოდება და სხვ. ფულადი საშუალებების გადამხდელის ან მიმღების თვალსაზრისით აღნიშნულ სისტემაში მუშაობა ჰგავს (ანალოგიურია) ინტერნეტბანკინგის დახმარებით განხორციელებულ ანგარიშსწორების პროცესს. ანგარიშსწორებაში მომავალი მონაწილე (გადამხდელი) დარეგისტრირდება სისტემაში და მასზე გაიხსნება ანგარიში, რომელზედაც უნდა ჩაირიცხოს რაღაც თანხა. რეგისტრაციის პროცესის თავისებურებაზე დამოკიდებულებით მსგავს სისტემებში ვირტუალური ანგარიშების გახსნა ნიშნავს თანხის შეტანისთანავე (ე.ი. ფულადი საშუალებების საწყის შეტანას, სააღრიცხვო ჩანაწერის შექმნას). შემდეგ სპეციალურად გაფორმებული დავალების დახმარებით შეიძლება განხორციელდეს გადახდები, მაგრამ თავისებურება გამოიხატება იმაში, რომ ასეთი სისტემები არის დახურული, ე. ი. გადახდა შეიძლება განხორციელდეს წინასწარ ამ სისტემაში დარეგისტრირებული მიმღების სასარგებლოდ (მსგავსია ელექტრონული ნაღდი ფულის სისტემის). დარეგისტრირებული ნიშნავს, რომ მას ამ საგადამხდელო სისტემაში გააჩნია ვირტუალური ანგარიში. სავაჭრო დანესებულება დაინტერესებულია, მონაწილეობა მიიღოს ასეთ სისტემაში, რაც მას საშუალებას აძლევს, ოპერატიულად მიიღოს ინფორმაცია ვირტუალურ ანგარიშზე განხორციელებული ცალკეული ოპერაციის მიხედვით.

ამრიგად, გამყიდველს შეუძლია სწრაფად განსაზღვროს გადაიხადა თუ არა მყიდველმა შეძენილი საქონლისთვის თანხა და ამის შემდეგ მოახდინოს საქონლის გადატვირთვა ან გაუწიოს მომსახურება. შემდეგ გამყიდველს შეუძლია პირველი, სისტემიდან გამომუშავებული თანხის გამოტანა – სისტემის ორგანიზატორისათვის მიცემული სპეციალური დავალების შემდეგ. ამ შემთხვევაში სრულდება საბანკო გზავნილება სისტემის ორგანიზატორის ანგარიშსწორების ანგარიშიდან გამყიდველის ანგარიშსწორების ანგარიშზე. საერთოდ ვირტუალური ანგარიშების

სისტემის დახმარებით ჩქარდება მყიდველსა და გამყიდველს შორის ურთიერთქმედების პროცესი. თუმცა ამ დროს ფინანსური ოპერაციების რეალური დაჩქარება არ ხდება (საჭიროა გარკვეული დრო მყიდველის მხრიდან სისტემაში რეალური ფულის თანხის შესატანად და მის გადასაგზავნად გამყიდველის ანგარიშზე). ციფრული ფულით და ვირტუალური ანგარიშებით ანგარიშსწორების სისტემებს უწოდებენ წინასწარ ანაზღაურებულს. რაც იმაში გამოიხატება, რომ, სანამ მოხდება საქონლის შეძენა ან მომსახურების გაწევა, საჭიროა სისტემის ორგანიზატორის ანგარიშზე ფულის ჩარიცხვა, ანუ უნდა მოხდეს რეალური ფულის კონვერტაცია ვირტუალურში. თანაც გადახდა შეიძლება განხორციელდეს წინასწარ შეტანილი თანხის ფარგლებში.

ამრიგად, ელექტრონული ფულით და ვირტუალური ანგარიშებით ანგარიშსწორების სისტემები ფუნქციონირებენ გადახდის სადებეტო სისტემის სქემით. აღნიშნულ სისტემებს მიეკუთვნებიან: რაპიდა, კრედიტ-პილოტი, **Ciberpilot-ი, Assist-ი, Яндекс деньги, Web-Money Transfer-ი** და სხვ.

7.4. ინტერნეტბანკინგი

ინტერნეტბანკინგი ეწოდება ინტერნეტის საშუალებით საბანკო ანგარიშების მართვას. ინტერნეტმომსახურებებს შორის ის ყველაზე დინამიური მიმართულებაა და, ამავდროულად, საფუძველი ფასიან ქალაქდებთან ინტერაქტიულ რეჟიმში მუშაობის, ინტერნეტაზღვევის ორგანიზაციის. ინტერნეტბანკინგის კლასიკური ვარიანტი მომხმარებელს საშუალებას აძლევს, სახლიდან ან ოფისიდან გაუსვლელად მიიღოს ყველა საბანკო მომსახურება, გარდა ნაღდი ფულის გაცემისა. ბევრი ბანკი და საბროკერო კომპანია დაინტერესებულია, აქციების, ობლიგაციების, ოპციონებისა და ფიუჩერსების ყიდვა-გაყიდვა მოხდეს ინტერაქტიული ვაჭრობის მეშვეობით. პოტენციურ ინვესტორს, პირველ რიგში, ქსელში ტრეიდინგი იზიდავს გარიგების დადების სიმარტივეთა და ონლაინბროკერის მომსახურების დაბალი ტარიფით [10].

პერსონალური კომპიუტერ ბანკინგი არის პერსონალურ კომპიუტერთან მიერთებული მოდემის საშუალებით ბანკის ქსელთან მიერთება.

ტელეფონბანკინგი კი ანგარიშების მომსახურება ტელეფონით.

ვიდეობანკინგი – ბანკის პერსონალთან ინტერაქტიულ რეჟიმში ურთიერთობის დამყარება.

ზოგადად ინტერნეტბანკინგი მოიცავს ოფისებში ფიზიკური და იურიდიული პირებისადმი დისტანციურ კომპლექსურ საბანკო მომსახურებას.

ინტერნეტბანკინგის სისტემის დახმარებით შეიძლება უზრუნველყოფილი იქნეს: უნაღდო ყიდვა-გაყიდვა, მომსახურების ანაზღაურება, ბანკის შიდა და ბანკთაშორისი უნაღდო ანგარიშსწორება, ფულადი საშუალებების გადაგზავნა ანგარიშზე, სახლიდან და ოფისიდან გაუსვლელად დღე-ღამის განმავლობაში ანგარიშზე სახსრების მოძრაობის კონტროლი.

დღესდღეობით არსებობს ინტერნეტბანკინგის მომსახურების ორი ვარიანტი: პასიური და აქტიური.

პირველის შემთხვევაში ონლაინრეჟიმში შესაძლებელია შემდეგი ოპერაციების შესრულება: ანგარიშის დათვალიერება, ანგარიშიდან ამონაწერის ამობეჭდვა, ვალუტის კურსის გაცნობა და ა.შ.

აქტიური ოპერაციების შესრულებისას ზემოთ ჩამოთვლილ პასიურ ოპერაციებს ემატება ანგარიშებზე ფულის გადარიცხვა, კონვერტაცია, დეპოზიტის გახსნა, კომუნალური გადასახადების გადახდა, სესხის დაფარვა და ა. შ.

დღეისათვის ინტერნეტბანკინგი დანერგილია საქართველოს ბანკებში: „საქართველოს ბანკი“, „თიბისი ბანკი“, „ინტელექტბანკინგი“, „ბაზისბანკი“, „აგრობიზნესბანკი“, „გაერთიანებული ქართული ბანკი“ და სხვ.

ინტერნეტბანკინგის გამოყენებას გააჩნია მთელი რიგი უპირატესობები:

დროის ეკონომია. ფიზიკურად კლიენტს არ სჭირდება ბანკში მისვლა;

ფულის დაზოგვა. ინტერნეტბანკინგით სარგებლობისას მომსახურების გადასახადი გაცილებით ნაკლებია, ვიდრე დანახარჯები, რომლის გადახდაც მოუწევს კლიენტს ბანკში უშუალოდ მისვლისას;

კლიენტს შესაძლებლობა ეძლევა, 24 საათის განმავლობაში აკონტროლოს თავისი ანგარიში, მოახდინოს ოპერატიული რეაგირება ფინანსურ ბაზარზე შექმნილ სიტუაციაზე.

ინტერნეტბანკინგის დანერგვით წარმოებს ბანკის ოფისების განტვირთვა.

ინტერნეტბანკინგის სისტემაში ფინანსური ოპერაციების უსაფრთხოებას უზრუნველყოფს პროგრამულ-ტექნიკური დაცვის თანამედროვე ტექნოლოგია. შესრულებული ოპერაციების კონფიდენციალობის თითქმის 100%-იან გარანტიას იძლევა დაცვის მეთოდების კვალიფიცირებული გამოყენება.

1995 წლამდე, როცა ჯერ კიდევ, კარგად არ იყო განვითარებული ინტერნეტი, ბანკები კლიენტებს ემსახურებოდნენ „კლიენტბანკის“ რეჟიმში. ამ შემთხვევაში კლიენტის პერსონალურ კომპიუტერზე დაყენებული იყო სპეციალური პროგრამული უზრუნველყოფა, მოდემის საშუალებით ხორციელდებოდა ინფორმაციის გაცვლა ბანკთან. 1995-2000 წლებში აშშ-სა და ევროპაში დაიწყო ეგრეთ წოდებული „ვირტუალური ბანკების“ გახსნა, რომლებსაც არ გააჩნდათ არც ერთი ოფისი. ანგარიშის გახსნა, მისი მართვა და კრედიტის მიღება ხორციელდებოდა ინტერნეტის მეშვეობით. დღეს, ინტერნეტბანკინგი გავრცელებულია თითქმის ყველა ქვეყანაში.

ინტერნეტით განხორციელებული ბიზნესის ერთ-ერთ პერსპექტიულ მიმართულებას წარმოადგენს **on-line** კრედიტების გაცემა, რომელსაც ახორციელებს სპეციალიზებული სასესხო კომპანიები მაგ., **LendingTre.com-ი** და **E-Loan Inc-ი** კომპანია.

მსოფლიოში დაიწყო მობილური ტელეფონებით WAP-ბანკინგით ანგარიშების დისტანციური მართვა, რომელიც ეფუძნება მონაცემების უსადენო გადაცემას. მობილური ტელეფონების მფლობელებს ბანკები სთავაზობენ კიდევ ერთი სახის მომსახურებას – **SMS-ბანკინგს**. მოკლე შეტყობინების საფუძველზე კლიენტს შეუძლია მიიღოს ინფორმაცია ანგარიშსწორების ანგარი-

შის მდგომარეობის (ნაშთი ანგარიშზე, ამონაწერი ანგარიშიდან) შესახებ. სპეციალისტები **SMS**-ბანკინგის განვითარებას **WAP**-ბანკინგთან შედარებით დიდ პერსპექტივას უწინასწარმეტყველებენ.

7.5. ანაზღაურება მობილური ტელეფონის ანგარიშიდან

მობილური კომერცია ეს არის მობილური პორტატიული მონეობილობის გამოყენება ურთიერთობის, გართობის, ინფორმაციის გადაცემისა და მიღებისათვის, ტრანზაქციის შესრულებისათვის საზოგადოებრივი ან კერძო ქსელის მეშვეობით.

დღეისათვის შეძენილი საქონლის ან გაწეული მომსახურების ღირებულების გადახდა შესაძლებელია მობილური ტელეფონის საშუალებით. მობილური ტელეფონით შეიძლება ელექტრონულ მაღაზიაში საქონლის შეძენა ან კომუნალური გადასახადების გადახდა, საბანკო რეკვიზიტების გაგზავნა. ზოგიერთი მობილური კომპანიები ამ სახის მომსახურებას უფასოდ ეწევიან, როგორც მობილური მომხმარებლის ჩვეულებრივი პაკეტი. ფული, რომელიც უნდა გადაიხადოს მობილური ტელეფონის მფლობელმა შეძენილი საქონლის ან გაწეული მომსახურებისათვის, მოიხსნება ტელეფონის მფლობელის ანგარიშიდან ან სპეციალური ბარათიდან, რომელიც უნდა შეიძინოს ტელეფონის მფლობელმა და შემდეგ გაააქტიუროს.

გაწეული მომსახურების ან შეძენილი საქონლის ღირებულების ანაზღაურება წარმოებს საიდუმლო შეტყობინების (SMS) გაგზავნით. ეს უკანასკნელი მოიცავს: ტელეფონის მფლობელის ანგარიშის ნომერს, გადასახდელ თანხას, საქონლის ან მომსახურების კოდურ ნომერს და გამყიდველის ანგარიშის ნომერს. თუ გადასახდელი თანხა აღემატება მყიდველის ანგარიშზე არსებულ თანხას, მაშინ საჭიროა ახალი ბარათის გააქტიურება. ამ დროს გამოუყენებელი ნაშთი წინა ბარათიდან დაემატება გააქტიურებულ ბარათზე მითითებულ ნომინალურ რაოდენობას. აღნიშნული ფუნქციის შესასრულებლად საჭიროა, რომ მყიდველის ტელეფონი აღჭურვილი იყოს ან **Wap** ფუნქციით, ან საკუთარი მიკროპრაუზერით. მობილური კომერცია სულ უფრო და უფრო და-

მოუკიდებელს ხდის მომხმარებელს სტაციონარული მოწყობილობებისაგან, აძლევს რა მას შესაძლებლობას, განახორციელოს ყველა ზემოთ ჩამოთვლილი ოპერაცია მობილური ტელეფონით, ან ჯიბის კომპიუტერით.

7.6. რეალური დროის რეჟიმში მომუშავე გზავნილების საზღვარგარეთული ეროვნული სისტემები

აშშ-ში ონლაინრეჟიმში ფუნქციონირებს რეგიონალური, რეგიონალთშორისი და ბანკთაშორისი ელექტრონული სისტემები: **CHIPS-ი**, **Fedwire-ი** და **Bankwire-ი**. ამ სისტემების მუშაობა ეყრდნობა საკომუნიკაციო სისტემებს, რომლებიც იყენებენ საერთო-ეროვნულ და ცალკეული ბანკების ქსელებს. **CHIPS-ი** და **Fedwire-ი** ძირითადი სისტემებია, რომლებიც უზრუნველყოფენ საკომუნიკაციო, ანგარიშსწორებების და გზავნილების მომსახურების განხორციელებას. სისტემა **Fed-wire-ი** წარმოადგენს დიდი თანხებისა და ფასიანი ქაღალდების გზავნილების სისტემას. იგი ეკუთვნის აშშ-ის ფედერალურ სარეზერვო სისტემას და მოიცავს საერთო ქსელში გაერთიანებულ 12 ფედერალურ სარეზერვო ბანკს. მასში გაერთიანებულია ფედერალური სარეზერვო სისტემის მთავარი ოფისები და განყოფილებები, ფედერალური სარეზერვო სისტემის 500-ზე მეტი ბანკი-წევრი. ფედერალური სარეზერვო სისტემის საკომუნიკაციო ცენტრი მდებარეობს ვირჯინიის შტატის ქალაქ კალპენტერში.

CHIPS (Clearing Hous Interbank Payment System) ნიუ-იორკის ერთ-ერთი ონლაინკრილინგური სისტემაა, რომელიც უზრუნველყოფს ბანკთაშორის გადახდებს.

ამ სისტემით განხორციელებული გადახდები მოიცავს უცხოურ ვალუტაში განხორციელებულ გარიგებებს და ევრო-დოლარებში განთავსებულ ფასიან ქაღალდებს. ეს სისტემა დაფუძნებულია 1970 წელს ნიუ-იორკის საკრილინგო პალატის ასოციაციის მიერ, ჩეკებით ანგარიშსწორებიდან ელექტრონულ ანგარიშსწორებაზე გადასვლის მიზნით, და უზრუნველყოფს აშშ-ის მიერ განხორციელებული საერთაშორისო ანგარიშსწორებების

90%-ს. მასში გაერთიანებულია ნიუ-იორკის 11 მსხვილი ბანკი. ესაა ელექტრონული სისტემა, რომელმაც შეცვალა ქალაქის მატარებლებზე აგებული სისტემები, წარმოადგენს საკრედიტო გზავნილების სისტემას. ამ სისტემის მონაწილე შეიძლება გახდეს ბანკი, რომლის კაპიტალის მოცულობაც ნაკლები არ უნდა იყოს 250 მილიონ დოლარზე. ამ სისტემაში ასოცირებული წევრის სტატუსით მონაწილისთვის აუცილებელი პირობაა თანხმობა სისტემის წესების დაცვაზე.

საკომუნიკაციო მომსახურების მიზნით გამოიყენება 14 ქსელური პროცესორი. მათგან 12 ემსახურება ფედერალურ სარეზერვო ბანკს, ერთი – მმართველ საბჭოს და ერთიც – ცენტრს. არ არსებობს მთავარი საკომუნიკაციო ცენტრი. კოორდინაცია ხორციელდება კალპენტერის ცენტრიდან.

CHIPS-ში გაერთიანებულია მოთავე ბანკები, საანგარიშსწორებო ბანკები და ბანკი-მონაწილენი. ბანკ-მონაწილის როლში შეიძლება გამოვიდეს კომერციული ბანკები, კორპორაციები და საინვესტიციო კომპანიები. განვიხილოთ ზოგიერთ ქვეყანაში მოქმედი საკრილინგო სისტემები.

დიდი ბრიტანეთი. დიდი ბრიტანეთში გამოიყენება ელექტრონული გზავნილებისა და კრილინგის ორი სისტემა – **BACS**-ი და **CHAPS**-ი.

BACS (Bankers Automated Clearing Services) დაარსდა 1968 წელს მსხვილი და წვრილი საწარმოების კომერციული უნაღდო ანგარიშსწორებისთვის. ამ სისტემის წამყვანი ელემენტებია: საკრილინგო ანგარიშსწორების ცენტრები და ტელესაკომუნიკაციო სისტემა **Bacstelecom**-ი. სისტემის კლიენტები, სარგებლობენ რა **EDI**-ი სტანდარტებით, **Bacsnet**-ი ქსელის საშუალებით გადასცემენ საგადამხდელო დოკუმენტებს. საკრილინგო ცენტრი უზრუნველყოფს საგადამხდელო პაკეტის ფორმირებას და გადასცემს მას **Chcaps**-ის მეშვეობით. შეტყობინებების გადაცემა და მიღება წარმოებს სატელეფონო არხების საშუალებით. სისტემის ძირითადი ელემენტებია: საკრილინგო-საანგარიშსწორებო ცენტრები და ტელესაკომუნიკაციო სისტემა **BACStel**-ი. საკრილინგო ცენტრებში კლიენტების საგადამხდელო დავალებების

გადაცემა ხორციელდება სატელეფონო არხებით ან მაგნიტური მატარებლებით. **BACS**-ი, მიიღებს რა ფაილს, ყველა ტრანზაქციას ახარისხებს იმ ბანკების ქრილში, რომელთათვისაც ეს ტრანზაქციებია განკუთვნილი; ამ ბანკებისთვის ფორმირდება ფაილი, რომელშიც ასახულია ნაერთი ინფორმაცია. ბანკს საკრილინგო ცენტრიდან მიღებული საგადამხდელო პაკეტის საფუძველზე შეუძლია განახორციელოს გადახდები **CHIPS**-ი ბანკთაშორის სისტემით. სისტემაში დოკუმენტების დამუშავება წარმოებს 3 დღის განმავლობაში. დამამთავრებელ ეტაპზე წარმოებს ბანკის თითოეული განყოფილების მიხედვით სადებეტო და საკრედიტო ოპერაციების ურთიერთჩათვლები. სისტემაში ანგარიშსწორება დაფუძნებულია ერთი სამუშაო დღის განმავლობაში გადახდების გადაგზავნის გარანტიის პრინციპზე. სისტემაში გამოყოფილია მონაცემების გადაცემის სამი დონე. ბანკი-მონაწილენი ელექტრონულ საგადამხდელო დავალებას გადასცემენ მეორე დონის ერთ-ერთ საანგარიშსწორებო ცენტრს, რომელიც აღჭურვილია პროგრამულ-აპარატურული კომპლექსით – **GATEWAY**. თავის მხრივ ეს ცენტრები დაკავშირებული არიან ერთმანეთთან და ცენტრალურ ბანკთან მაღალ სიჩქარიანი ქსელით – **BRI-TICH TELE-COM**-ით.

საკრილინგო ცენტრების ფუნქციებია: შეტყობინების დამუშავება, ვერიფიკაცია და მონაწილე ბანკის აუცილებელი ინფორმაციით უზრუნველყოფა. 1985 წლის ბოლოს საერთაშორისო საბანკო ჯგუფში – **HonKong bank Group** – დაინერგა კომპიუტერული სისტემა – **Hexagen Electronic Banking Sistem**, რომელიც უზრუნველყოფს:

- კლიენტის ანგარიშის მდგომარეობის შესახებ ინფორმაციის გაცემას;
- ანგარიშებიდან ამონაწერის მიღებას;
- გადახდების განხორციელებას;
- ფულადი საშუალებების გადაგზავნას;
- აკრედიტივების გახსნას და სხვ.

შვეიცარია. შვეიცარიის ბანკთაშორისი საკრილინგო სისტემა **SIC (Swiss Interbank Clearing)** შემუშავებულია 1981-1986

წლებში, კომპანია „**Телекүрс АГ**“-ის მიერ, კომერციულ ბანკებთან თანამშრომლობით. ამ სისტემის ექსპლუატაცია დაიწყო 1987 წლიდან. თითოეული ბანკი სისტემასთან მიერთებულია „**Телекүрс АГ**“-ის მიერ გამოყენებული ქსელის საშუალებით. ეს ქსელი გამოიყენება არა მარტო სისტემის საჭიროებისთვის, არამედ სხვა ქსელური მომსახურებისთვის, რომელსაც ეს სისტემა მომხმარებელს სთავაზობს. „**Телекүрс АГ**“ სისტემასთან მიერთება წარმოებს ბანკ **Front-Office** კომპიუტერის მეშვეობით.

შვეიცარიული ბანკთაშორისი საკრილინგო ანგარიშსწორების სისტემა დღე-ღამის განმავლობაში ახორციელებს საბოლოო გადახდებს შვეიცარიის ეროვნულ ბანკში მაკორესპოდენტირებელი ანგარიშების მეშვეობით. გადახდების მოცულობა შეუზღუდავია. შვეიცარიაში ეს ერთადერთი სისტემაა, რომელიც ახორციელებს შვეიცარიის ბანკთაშორის მთლიან (საერთო) გადახდებს. ამ დროს წარმოებს ბანკი-გადამხდელის ანგარიშების დებეტირება. ბანკ-მიმღების ანგარიშების დაკრედიტებასთან ანგარიშსწორება შეიძლება განხორციელდეს მხოლოდ იმ გზავნილებით, რომელთა ინიცირება ხდება ბანკ-გადამხდელის მიერ. სისტემას შეუძლია აწარმოოს ბანკის კლიენტების ფულის გადარიცხვა რომელიმე საბანკო ანგარიშზე, შეასრულოს საგადამხდელო დავალება მესამე მხარის სასარგებლოდ, განახორციელოს ბანკთაშორისი გადახდები.

სისტემაში მუშაობის განსახორციელებლად, მისი მონაწილენი მიერთებული უნდა იყვნენ სისტემის ცენტრალურ კომპიუტერთან, რათა შეძლონ ონლაინრეჟიმში მუშაობა. საგადამხდელო დოკუმენტები უნდა შეიცავდეს მითითებებს ფულადი საშუალებების იმავე დღეს გადარიცხვის შესახებ (დოკუმენტების წარდგენის დღეს), ან ანგარიშსწორება უნდა განხორციელდეს მომავალში (10 სამუშაო დღის განმავლობაში). ანგარიშსწორება შეიძლება განხორციელდეს მხოლოდ იმ შემთხვევაში, თუ ფულის გამგზავნი ბანკის ანგარიშზე არსებობს საკმარისი თანხა. ამ შემთხვევაში ანგარიშსწორება არის საბოლოო, საგადამხდელო ტრანზაქციის მიღების მომენტისთვის გამგზავნი ბანკის ანგარიშზე არ არის საკმარისი საშუალებები, მაშინ გადახდა დგება რიგში (მოლოდინის ფაილში). მოსალოდნელი გადახდები შეიძლება გაუქმდეს, ბანკი-გამგზავ-

ნის მიერ ნებისმიერ მომენტში. ამ შემთხვევაში ბანკ-მიმღებს გაეგზავნება შეტყობინება ტრანზაქციის გაუქმების შესახებ.

სისტემის მონაწილეებს შეუძლიათ ნებისმიერ დროს მოითხოვონ ინფორმაცია მათი ანგარიშების მდგომარეობის შესახებ, აგრეთვე, ინფორმაცია შემოსული გადახდებისა და ფაილში შეტანილი გადახდების შესახებ. ბანკის სამუშაო დღეებში სისტემა ფუნქციონირებს დღე-ღამის განმავლობაში.

მონაცემების დასამუშავებლად სისტემის გამოთვლით ცენტრში გამოიყენება აქტიური და პასიური კომპიუტერები. მესამე კომპიუტერი ჩვეულებრივ გამოიყენება სისტემის შესამუშავებლად. საჭიროების შემთხვევაში, მისი, როგორც მუშა მანქანის გამოყენება შეიძლება სისტემის გამოთვლით ცენტრში.

გერმანია. გერმანიაში ადრე ჩატარებულმა დოკუმენტების ფორმებისა და შინაარსის სტანდარტიზაციამ ხელი შეუწყო ოპტიკური ნაკითხვის სისტემის გაფართოებას, რამაც საბოლოოდ გამოიწვია სისტემაში ინფორმაციის შეტანის გაიოლება, ინფორმაციის დამუშავებისა და გადაგზავნის ღირებულების შემცირება.

გერმანიაში გავრცელებულია ჟიროანგარიშსწორების სისტემა. შემნახველი ბანკების ჟიროქსელი წარმოადგენს ურთიერთდახმარების საზოგადოებებისა და კოპერატივების ქსელს. ბანკის განყოფილებებს, ასევე, მოთავე ოფისსა და საანგარიშსწორებო ცენტრებს შორის მონაცემების გადასაცემად იყენებენ ტელესაკომუნიკაციო საშუალებებს. დოიჩე ბუნდესბანკის ჟიროქსელის თითოეულ ფედერალურ მიწას გააჩნია 11 კომპიუტერული ცენტრი, რომლებიც ერთმანეთთან დაკავშირებულია მონაცემების გადაცემის ტელესაკომუნიკაციო სისტემით. ამუშავებენ როგორც ოპტიკურად წამკითხავ დოკუმენტებს, ასევე, ელექტრონული ფორმით წარმოდგენილ ინფორმაციას. გადახდების სისტემებისაგან განსხვავებით, ჟიროქსელებს არ გააჩნიათ მფლობელი და მართვის შესახებ შეთანხმება. კომერციული ბანკების ჟიროქსელი შეიძლება განხილულ იქნეს, როგორც შიდა ქსელი. ამ ქსელების ევოლუცია ხდებოდა წლების განმავლობაში – ერთი მხრივ, გადახდების დამუშავების ღირებულების შემცირების, მეორე მხრივ, საკრედიტო ორგანიზაციის ან საბანკო ჯგუფის შიგნით ლიკვიდურობისთვის.

კომერციული ბანკების ჟიროქსელი. კომერციული ბანკების ჟიროქსელის ძირითადი მონაწილენი არიან ორი მსხვილი ბანკი და გერმანული საფოსტო ბანკი. თითოეული ეს ბანკი გადახდების დამუშავების მართვას ახორციელებს საკუთარი შიდა ქსელით. ეს ქსელი ეფუძნება ბანკის ფილიალებს და შვილობილ კომპანიებს. მთავარი კანტორა, ბანკის ფილიალები ან, ზოგჯერ შვილობილი კომპანიები დაკავშირებული არიან კონკრეტულ დამამუშავებელ სამეურნეო ორგანიზაციებთან (მომსახურების პროვაიდერები), ან კიდევ იმ კომპიუტერულ ქსელებთან, რომლებიც ტრანზაქციების დამუშავებასა და საბუღალტრო აღრიცხვას ახორციელებენ. 1990 წელს გერმანიის ცენტრალურმა ბანკმა დაიწყო ერთი დღის განმავლობაში ყველაზე დიდი გადახდების ანგარიშსწორების ავტომატიზებული სისტემის დანერგვა, რომელიც აშშ-ის **CHIPS**-ის ანალოგიურია. ეს სისტემაა **EAF (Elekt-ronische Abrechnung Fran-kruf)**. საკრილინგო სისტემა **EAF-ი** (ინგლისური **Euro Access Furt**) დღეისათვის ევროპაში უმსხვილესი საკრილინგო სისტემაა. ყოველდღიურად მისი მეშვეობით ხორციელდება 160 000 გადახდა. **EAF**-ში ანგარიშსწორების პროცედურა ხორციელდება ორ ეტაპად. **EAF**-ის არაპირდაპირი მონაწილეებისთვის მთავარ უპირატესობას წარმოადგენს ის, რომ ყველა ევროტრანზაქციისთვის ფულადი საშუალების გადასაგზავნად მათ გააჩნიათ ცენტრალური მისამართი. მათ შეუძლიათ თავიანთი ლიკვიდობის კონცენტრაცია და რეზერვების სხვადასხვა ანგარიშებს შორის განაწილებაზე უარის თქმა.

პირველ ეტაპზე ორმხრივი შემხვედრი გადახდები ექვემდებარება ურთიერთჩათვლას და საბოლოოდ გადადის ბანკ-მიმღების განკარგულებაში. დავალების შესრულება აგრეთვე ხდება ლიმიტის ფარგლებში. მეორე ეტაპზე გახსნილი პოზიციების მიხედვით წარმოებს გადახდების რეგულირება. სისტემა არ ღებულობს დარჩენილ სადებეტო პოზიციებს. ეს გადახდები შემდეგში შეიძლება შეტანილ იქნეს მთლიან ანგარიშსწორების სისტემაში და დამუშავდეს იმავე დღეს. აღნიშნული ინვესს სისტემური და საკრედიტო რისკების შემცირებას, მნიშვნელოვნად ამცირებს ლიკვიდურ რესურსებზე მოთხოვნებს.

დოიჩე ბუნდესბანკი მხარს უჭერს ორ ბანკთაშორის საფონდო საკრილინგო ბანკს და ანგარიშსწორების ევროგადახდების სისტემას. ორივე სისტემა საზღვარგარეთიდან მათთან წვდომას უზრუნველყოფს, გერმანიის ბანკების ფილიალებთან მიმართვის გარეშე. EAF-ში გაერთიანებულია 68 პირდაპირი და 600 არაპირდაპირი მონაწილე, 100 ქვეყნიდან. ტრანზაქციის ღირებულებაა 0.15 ევრო, ყოველთვიური საწევრო შენატანი შეადგენს 256 ევროს, სისტემაში შესვლა უფასოა.

ELS სისტემაში ინდივიდუალური გადახდები ხორციელდება მთლიანობის საფუძველზე. ეს სისტემა ასევე გერმანიის მეშვეობით უზრუნველყოფს TAR-GET სისტემასთან წვდომას და საზღვარგარეთის ქვეყნებიდან გადახდების განხორციელებას. **ELS** სისტემაში მონაწილეობს კომერციული ბანკების 3500 ფილიალი. პირველი ერთჯერადი გადახდის ღირებულება შეადგენს 0,26 ევროს. საჭირო არაა საწევრო შენატანების გადახდა. **ELS** სისტემა ინარჩუნებს შესაძლებლობას, შიდა გადახდებისათვის გამოიყენოს ევროგადახდები, ამასთან ერთად, უზრუნველყოს ევრო და საერთაშორისო გადახდებს მესამე ვალუტაში (მაგ., **USD**, **GBP** და სხვ.). **EAF** და **ELS** სისტემებთან დაშორებული წვდომა შესაძლებელია **S.W.I.F.T**-ის მეშვეობით. ბუნდეს-ბანკი უზრუნველყოფს მონაწილეების დაშორებულ წვდომას. საბოლოოდ ეს უზრუნველყოფს **EAF** და **ELS** სისტემების სრულ ფუნქციონირებას და ევროგადახდისთვის მონაწილეებს აძლევს შესაძლებლობას, განახორციელონ დაშორებული წვდომა **S.W.I.F.T**-ის სტანდარტების შეტყობინების საფუძველზე. ეს გადაწყვეტილება დაფუძნებულია **stat-of-the-art** ბრაუზერის ტექნოლოგიაზე და იყენებს მაღალგანვითარებულ **S.W.I.F.T**-სერვისს. გადახდების მართვა ხორციელდება **S.W.I.F.T-FIN** სერვისის მეშვეობით. ბევრ შემთხვევაში **S.W.I.F.T**-ის ინტერფეისი ადვილად მისაწვდომია. საგადამხდელო განკარგულების გასაგზავნად **EAF** და **ELS** სისტემებში დაშორებულმა მონაწილემ თავისი ინტერფეისის მეშვეობით უნდა განახორციელოს ორი ახალი BIC-კოდის ადრესაცია.

ევროში ელექტრონული ანგარიშსწორების საერთაშორისო სისტემა. ერთიანი ევროპული ვალუტის შემოღებამ, პირველ

რიგში, ზემოქმედება იქონია ბანკთაშორისი და კომერციული გადახდების ბაზარზე. კომერციულ ბანკებს შორის გაიზარდა კონკურენცია, ახალი კრილინგური ანგარიშსწორების სისტემის დაწერვამ შეავიწროვა ტრადიციული საგადახდელო სისტემები.

ევროში კრილინგური ელექტრონული სისტემა აერთიანებს 49 მსხვილ ბანკს. ასოციაციის მონაწილენი, მოქმედებენ რა თავიანთი სახელით და სხვა კომერციული ბანკების დავალებით, საკრილინგო სისტემაში აგზავნიან **S.W.I.F.T.**-შეტყობინებას. აღნიშნული სისტემა მდებარეობს მაინის ფრანკფურტში და სამუშაო დღის დამთავრების შემდეგ აწარმოებს ავტომატურ შედარებებს და გადახდების ურთიერთჩათვლას. ამ საგადახდელო სისტემის უპირატესობაა მიწოდებული მომსახურების შედარებით სიიფე (0,16 ევრო თითოეული შესრულებული ოპერაციისთვის). თუმცა უნდა აღვნიშნოთ, რომ, შეიძლება ადგილი ჰქონდეს ყოველდღიური გადახდების რაოდენობის გაზრდის გამო აღმოცენებულ ტექნიკურ პრობლემებს. ცენტრალური ბანკების ევროპულმა სისტემამ მუშაობა დაიწყო 1999 წლიდან და აერთიანებს ევროპის ცენტრალურ ბანკს, რომლის შტაბბინა მდებარეობს ფრანკფურტში.

ESCB-ი – არის ორგანიზაცია, რომელიც შექმნილია სტაბილური ფასების შენარჩუნებისა და ევროს მხარდასაჭერად. ევროკავშირის ცენტრალური ბანკების ძირითადი ამოცანებია:

- ევროკავშირის მონეტარული პოლიტიკის განსაზღვრა და ცხოვრებაში გატარება;
- გაცვლითი ოპერაციების ჩატარების კონტროლი;
- საგადახდელო სისტემის საქმიანობის სტიმულირება და მართვა;
- ევროკავშირის წევრი ქვეყნების ოფიციალური რეზერვების მხარდაჭერა და მართვა.

ევროკავშირის ქვეყნების ეროვნული ცენტრალური ბანკების ძირითადი მიმართულება მდგომარეობს ევროკავშირის მონეტარული პოლიტიკის განსაზღვრასა და განვითარებაში. გარდა პორტფელის სტანდარტული მართვის, კრედიტების წინააღმდეგობისა და საბაზრო რისკების მართვა. ევროკავშირის ცენტრალუ-

რი ბანკი საკუთარი რეზერვების მართვისთვის აყალიბებს პორტფელების მართვის მოთხოვნებს.

1999 წლის 1 იანვრიდან ევროკავშირის ქვეყნების ცენტრალური ბანკები ყველა საერთაშორისო გადახდებს **S.W.I.F.T**-თან მიმართებაში ახორციელებენ სხვადასხვა ალტერნატიული არხებით.

საგადამხდელო სისტემა TARGET (Ttrans European Real-time Cross Settlement Expres Transfere System) შედგება ევროკავშირის ქვეყნების მთლიანი ანგარიშსწორებების რეალური დროის რეჟიმში მომუშავე სისტემებისაგან. **Target** სისტემა რეალური დროის რეჟიმში მომუშავე ტრანსევროპული, ავტომატური ანგარიშსწორების ექსპრეს-სისტემაა, რომელიც შექმნილია ევროპის ცენტრალური ბანკისა და მონაწილე ქვეყნების ეროვნული ბანკების მიერ – დეცენტრალიზებული სისტემა, რომელიც შედგება 15 **RTCS** ეროვნული სისტემისაგან. **Target** სისტემების შექმნის შესახებ გადაწყვეტილება მიიღო ევროპის სავალუტო ინსტიტუტის საბჭომ 1995 წლის მარტში, სამი ძირითადი მიზნის მისაღწევად:

- ფულის ევრობაზრის ინტეგრაციის ხელშესაწყობად;
- ერთიანი ფულად-საკრედიტო პოლიტიკის პირობების შესაქმნელად;
- გადახდის საიმედოობისა და ეფექტიანობის უზრუნველსაყოფად.

მოცემული სისტემის მეშვეობით კომერციული ოპერაციების განხორციელება, გადახდების ოპერაციების მაღალი ღირებულების გამო, მნიშვნელოვნად შემოფარგლულია. აღნიშნული სისტემა მოითხოვს, რომ სალიკვიდო საშუალებების მნიშვნელოვანი მოცულობა აუცილებლად არსებობდეს ეროვნული ცენტრალური ბანკების სპეციალურ ანგარიშებზე. ფინანსური ბაზრების მოთხოვნების და კერძოდ მისი კლიენტების დასაკმაყოფილებლად. **Target** სისტემის სამუშაო დღის ხანგრძლივობა დიდია. – მუშაობას იწყებს 07.00 საათზე და ამთავრებს 18.00 საათზე. იმისთვის, რომ მონაწილეებმა კარგად მართონ თავიანთი ლიკვიდობა, კლიენტების გადახდები უნდა დამთავრდეს 17.00 საათზე.

Target-ის ყველაზე მნიშვნელოვან უპირატესობას წარმოადგენს ისიც, რომ ანგარიშების მიხედვით საკრედიტო გატარებები წყდება დაუყოვნებლივ, გადახდები ხორციელდება მხოლოდ მაშინ, თუ ბანკ-გადამხდელის მიერ წარდგენილი ფულადი საშუალებები საკმარისია. სისტემის სტრუქტურა ითვალისწინებს ევროპული სისტემის ცენტრალური ბანკების სტრუქტურას, რომელშიაც თითოეული ბანკი წარმოდგენილია, როგორც დამოუკიდებელი იურიდიული პირი, ხოლო საერთო ფუნქციების მართვის განხორციელება წარმოებს ევროკავშირის ცენტრალური ბანკის მიერ. ანგარიშსწორებები **Target**-ში ხორციელდება რეალური დროის რეჟიმში, მთლიანი ანგარიშსწორებების გამოყენების საფუძველზე, ევროკავშირის ცენტრალურ ბანკთან ორმხრივი შეთანხმების საფუძველზე. საკომუნიკაციო ქსელის სახით გამოიყენება **S.W.I.F.T.-FIN** სერვისი. ეროვნული ცენტრალური ბანკები და ევროკავშირის ცენტრალური ბანკი ერთმანეთთან პირდაპირ არ არიან შეერთებული. ამ კავშირის დამყარება ხდება მესამე მხარის – **S.W.I.F.T.**-ის მეშვეობით. ეროვნული ცენტრალური ბანკები და ევროკავშირის ცენტრალური ბანკი **S.W.I.F.T.**-თან შეტყობინების გაცვლისას პასუხისმგებლობას იღებენ გამოყენებულ მონეობილობებზე და ინსტრუმენტებზე. **S.W.I.F.T.**-ი ქვეყნებს შორის გადახდების განხორციელებისთვის უზრუნველყოფს საკომუნიკაციო კავშირს **Target**-სა და **RTGS** სისტემებს შორის. აგრეთვე, უზრუნველყოფს შემდეგი ტიპის ტრანზაქციებს:

- გადახდებს, რომელიც უშუალოდ არის დაკავშირებული ცენტრალური ბანკის ოპერაციებთან, რომელშიც ევროსისტემა მონაწილეობს ან, როგორც მიმღები, ან, როგორც გადამცემი;
- ევროში დიდი თანხების ვალდებულებების ურთიერთჩათვლის ანგარიშსწორების ოპერაციებს;
- ბანკთაშორის და კომერციული გადახდებს ევროში.

ქვეყნებს შორის გადახდების შესასრულებლად **RTGS** სისტემის მეშვეობით ბანკი-გამგზავნი საგადამხდელო დავალებას უგზავნის თავის ეროვნულ ცენტრალურ ბანკს. ეროვნული ცენტრალური ბანკი ამონმებს გადახდის შესაბამისობას მოთხოვნებთან, გამოთქვამს თანხმობას, ან უარს ამბობს ოპერაციის

შესრულების შესაძლებლობაზე. ავტორიზაციის წარმატებით დასრულების შემთხვევაში გადასახდელი თანხა ბანკი-გამგზავნის ანგარიშიდან ეროვნული **RTGS** სისტემის მეშვეობით გადაიგზავნება ბანკი-მიმღების ანგარიშზე. ბანკი-გამგზავნის ეროვნული ცენტრალური ბანკი საგადამხდელო დავალებისთვის აყალიბებს სტანდარტულ შეტყობინებას, რომელიც მოიცავს ეროვნულ ბანკებს შორის სეანსის კავშირის პერიოდში შეტყობინების დაცვის დამატებით საშუალებებს. ამის შემდეგ ბანკი-მიმღების ეროვნული ცენტრალური ბანკი ამონმებს საგადამხდელო დავალებაში მითითებული შეტყობინების დაცვის საშუალებების მთლიანობას. თუ ბანკი-მიმღები არ არის **RTGS**-ის სისტემის მონაწილე, მაშინ ეროვნული ცენტრალური ბანკი უარს ამბობს გადახდაზე და სთხოვს გამგზავნი ბანკის ეროვნულ ცენტრალურ ბანკს, ჩაურიცხოს ეს თანხა ბანკ-გამგზავნის ანგარიშზე. თუ ბანკი – მიმღები **RTGS** სისტემის მონაწილეა, მაშინ მიმღები ბანკის ეროვნული ცენტრალური ბანკი საინფორმაციო სისტემის ცენტრალური სტანდარტიდან გადაიყვანს შეტყობინებას ეროვნულ სტანდარტში და განახორციელებს გამგზავნი ბანკის ეროვნული ცენტრალური ბანკის ანგარიშის დებეტირებას, ჩარიცხავს თანხას ბანკი-მიმღების ანგარიშზე, **RTGS** ეროვნული სისტემის მეშვეობით. შემდეგ მიმღების ეროვნული ცენტრალური ბანკი საგადამხდელო დავალებას გადაუგზავნის ბანკ-მიმღებს. **S.W.I.F.T.-FIN**-ის სერვისის გამოყენება საკომუტაციო ქსელად საშუალებას იძლევა, გავაერთიანოთ სხვადასხვა ტექნოლოგიების **RTGS** ეროვნული სისტემები და უზრუნველყოთ შეტყობინების სწრაფი და საიმედო გაცვლა **TARGET** სისტემის მონაწილეებს შორის.

კითხვები თვითშემოწმებისთვის

1. რა არის ციფრული ფული?
2. როგორ ხდება ინტერნეტში ციფრული ფულით გადახდები?
3. როგორ ხდება ჩეკებით ანგარიშსწორება?
4. როგორ ხდება ინტერნეტ-ბანკინგით მომსახურება?
5. როგორ ხდება ინტერნეტ-ტელეფონით მომსახურება?

6. დაახასიათეთ აშშ-ის ელექტრონულ გადახდების სისტემა.
7. დაახასიათეთ ელექტრონული გადახდების სისტემა.
8. დაახასიათეთ გერმანიის ელექტრონული გადახდების სისტემა.
9. დაახასიათეთ ელექტრონული საგადამხდელო **TARGET** სისტემა.
10. დაახასიათეთ ევროში ელექტრონული ანგარიშსწორების საერთაშორისო სისტემა.

თემა 8. კრიპტოვალუტა

8.1. კრიპტოვალუტის მაინინგი

ელექტრონული ფული არის ვირტუალური ფულის ერთეული, გადახდის საშუალება, რომელიც არსებობს მხოლოდ ელექტრონულად სპეციალურ ელექტრონულ სისტემაში ჩანანერის სახით.

ელექტრონული ფულის გამოყენების პოპულარობა განისაზღვრება მისი ისეთი უპირატესობებით, როგორიცაა: მოხერხებულობა, ოპერაციების შესრულების მაღალი სისწრაფე, მიმოქცევის სიმარტივე, განაღდების კონტროლის უზრუნველყოფა, უსაფრთხოება, ანონიმურობა, სხვა პირისთვის გადაცემის შესაძლებლობა და სხვ.

ელექტრონული ფული მნიშვნელოვნად აფართოებს საქონლით ვაჭრობის პირობებს, რაც დაკავშირებულია ნაღდი ფულის მიმოქცევის ოპერაციების, მისი ტრანსპორტირებისა და შენახვის ხარჯების შემცირებასთან. ინტერნეტის გამოყენება აღნიშნულ საქმეში მნიშვნელოვნად ამცირებს ასევე საქონლით ვაჭრობის დანახარჯებს.

ელექტრონული ფულის მიმოქცევის პროცესი მუდმივად ვითარდება. ამის მაგალითია ფულად-საკრედიტო სისტემაში ელექტრონული ფულის ისეთი სახის გამოჩენა, როგორიცაა კრიპტოვალუტა [11].

კრიპტოვალუტა ელექტრონული ფულის ნაირსახეობაა, რომლის აღმოცენება და გამოყენება განაპირობა ფულის უნაღდო ანგარიშსწორების განვითარების საჭიროებამ თანამედროვე ინფორმაციულ ტექნოლოგიებზე დაყრდნობით [12]. იგი ემყარება დაცვის კრიპტოლოგიურ მეთოდებს და საუცხოოდ ასრულებს ფულის ყველა ფუნქციას მიმოქცევისათვის შეზღუდულ სივრცეში [13].

2024 წლის 20 მარტის მონაცემებით მსოფლიოში კრიპტოვალუტების რაოდენობამ 9168 შეადგინა [13]. 2025 წლის 22 მაისის მონაცემებით კრიპტოვალუტების საერთო კაპიტალიზაციამ შეადგინა 3 466 814 690 529 დოლარი [15].

კრიპტოვალუტის შექმნის პროცესი ზრდის ტენდენციით ხასიათდება, რაც უაღრესად დადებითი მოვლენაა ელექტრონული ფულის განვითარების საქმეში, ვინაიდან იგი აუცილებლად დასავამს ერთიან მსოფლიო კრიპტოვალუტაზე გადასვლის საჭიროებას.

კრიპტოვალუტის უპირველესი და ძირითადი სახეობაა ბიტკოინი. ერთ-ერთი ყველაზე გავრცელებული ვერსიის მიხედვით, ბიტკოინის შემქმნელი სატოში ნაკამოტო, რომელმაც 2008 წლის მიწურულს საჯაროდ განაცხადა საკუთარი გამოგონების შესახებ და გამოაქვეყნა ამის დამადასტურებელ დოკუმენტი, ხოლო 2009 წლიდან კომპიუტერულ ქსელში ჩაუშვა შესაბამისი სისტემა [16].

სატოში ნაკამოტო, როგორც ცნობილია, ფსევდონიმია, რომლის უკანაც დგას ორი პიროვნება – ავსტრიელი ბიზნესმენი კრეიგ რაიტი და ამერიკელი პროგრამისტი დევიდ კლეიმანი, თუმცა 2016 წლის მაისში თავად რაიტმა განაცხადა, რომ სწორედ ისაა ბიტკოინის შემქმნელი და რომ სატოში ნაკამოტო მხოლოდ მისი ფსევდონიმია. ამის დასამტკიცებლად მან გამომცემლობებს Go, Bi Bi Si და The Economist გადასცა მონაცემები ბიტკოინის შექმნის შესახებ და ჟურნალისტებს განუცხადა, რომ ბიტკოინის შექმნაში მას ეხმარებოდა დევიდ კლეიმანი.

ბიტკოინის დამახასიათებელი მთავარი ნიშანია ის, რომ იგი რომელიმე ცენტრალური საფინანსო ინსტიტუტის ან ორგანიზაციის მიერ არ გაიცემა, რაც გარკვეულწილად აფერხებს მისი გაუფასურების პროცესს.

დღეისათვის მსოფლიოს არაერთ ქვეყანაში ანგარიშსწორება უკვე ბიტკოინის საშუალებით მიმდინარეობს.

ბიტკოინს გააჩნია შემდეგი უმცირესი ერთეული (სატოში)*.

კრიპტოვალუტის მოპოვებას მაინინგი ეწოდება. ტერმინი – „მაინინგი“ (Mining) წარმოდგება ინგლისური სიტყვისგან mine,

* 1 სატოში = 0.00000001 ბიტკოინი; 10 სატოში = 0.0000001 ბიტკოინი; 100 სატოში = 0.000001 ბიტკოინი; 1,000 სატოში = 0.00001 ბიტკოინი; 10,000 სატოში = 0.0001 ბიტკოინი; 100,000 სატოში = 0.001 ბიტკოინი; 100,000,000 სატოში = 1 ბიტკოინი.

რაც სიტყვასიტყვით ნიშნავს მაღაროს (შახტას). შესაბამისად, წიაღისეულის მოპოვების ანალოგიით, კრიპტოვალუტის შექმნის პროცესსაც მეცნიერებაში მაინინგი შეერქვა. ხოლო მის მომპოვებელს – მაინერი (Miner).

ბლოკების მოპოვებისთვის მაინერები ჯილდოს სახით ღებულობენ გარკვეული რაოდენობის ბიტკოინის მონეტას (ჯილდოს რაოდენობა ყოველ ოთხ წელიწადში ნახევრდება. მაგალითად, 2009 წელს ერთი ბლოკის მოპოვებისთვის ჯილდო ტოლი იყო 50 ბიტკოინი, 2013 წლისთვის 25 ბიტკოინი, 2017 წლისთვის 12,5 ბიტკოინი, 2023 წლისთვის 6,25 ბიტკოინი. დღეისთვის ის ტოლია 3.125 და ა.შ. ბიტკოინების ემისია დასრულდება 2140 წელს. ხოლო 2140 წლის შემდეგ მოხდება ბიტკოინების მხოლოდ მიმოქცევა და მათი ტრანზაქციისათვის საკომისიოს გადახდა. თუმცა ზოგიერთ მკვლევარს ეჭვი ეპარება ამ რიცხვის სიზუსტეში. რამდენადაც ახალი ტექნიკისა და ტექნოლოგიების შემუშავებამ შეიძლება გამოიწვიოს ამ რიცხვის ცვლილება.

დღეს მსოფლიოში კრიპტოვალუტის გამოშვებისა და გამოყენების ნამდვილი ბუმი, მათ შორის, საქართველოშიც.

კრიპტოვალუტის მაინინგი დაიწყო საფრანგეთში, ისლანდიაში და საქართველოში 2014 წელს, საკუთარი მოწყობილობების ბაზაზე.

ცნობილია კრიპტოვალუტის მოპოვების (მაინინგის) ორი ხერხი: საკუთარი (სოლო) აპარატურული მაინინგი და ღრუბლოვანი მაინინგი.

პირველის შემთხვევაში, კრიპტოვალუტის მოპოვება ხდება საკუთარი აპარატურული მოწყობილობების საშუალებით, ხოლო მეორე შემთხვევაში, სხვისი აპარატურული საშუალებების დაქირავებით.

საკუთარ კომპიუტერზე ბიტკოინის მოპოვების დადებითი მხარეა: გამოყენებული ვიდეოკარტების ხელმეორედ გამოყენება შეიძლება ნებისმიერი კრიპტოვალუტის მოსაპოვებლად, შესაძლებელია მოწყობილობის დისკონტით გაყიდვა. ხოლო უარყოფითი მხარეა: მოწყობილობის მწყობრიდან გამოსვლის ალბათობა, მოწყობილობის მუშაობასთან დაკავშირებული ხმაური, ელექტროენერგიის მოხმარების სიდიდე (ბიტკოინის ღირებულებ-

ბის 90%-ი ელექტროენერგიის ხარჯია) და სხვ. მაინინგის მეორე ხერხი, ღრუბლოვანი მაინინგი დავახასიათოთ ქვემოთ.

კრიპტოვალუტის მოპოვების ანუ მაინინგისათვის საჭიროა გარკვეული რესურსები. ესაა, უზნარეს ყოვლისა, მძლავრი კომპიუტერული ტექნიკა, რომელიც აღჭურვილი იქნება კრიპტოვალუტის მოსაპოვებლად საჭირო სხვადასხვა მაკომპლექტებული ელემენტით, როგორიცაა: დედაპლატა რომელზედაც შესაძლებელი იქნება რამდენიმე გრაფიკული ადაპტერის მიერთება; მყარი დისკი; 4-8 გიგა ბაიტი ოპერატიული მეხსიერება; მაღალი სიხშირის პროცესორი; 5-8 ვიდეო ბარათი; 2 გიგა ბაიტის მოცულობის ვიდეობარათი; 750 W-ის სიმძლავრის კვების ბლოკი; რაიზერები (დამაგრძელებლები) დედაპლატასთან მისაერთებლად; გამაგრილებელი მოწყობილობები და სხვ.

თუ მსგავსი „ფერმის“ გასაცევებლად საკმარისი არ აღმოჩნდება ბუნებრივი ვენტილაცია, მაშინ მასზე უნდა დაყენდეს კონდიციონერი. წინააღმდეგ შემთხვევაში ადგილი ექნება მოწყობილობათა მუშაობის ხშირ შეფერხებებს, ან მათ გამოსვლას მწყობრიდან, რაც საბოლოოდ გამოიწვევს მაინინგის არარენტაბელურ ფუნქციონირებას.

დღეისათვის მაინინგისათვის გამოიყენება ორი სახის კომპიუტერული მოწყობილობა: ვიდეობარათები (GPU – graphics processing unit – გრაფიკული პროცესორები) და ბევრად უფრო სრულყოფილი მოწყობილობა, სახელწოდებით ASIC (Application Specific Integrated Circuit) სპეციალური დანიშნულების ინტეგრალური სქემა). აღნიშნული მოწყობილობა შეიქმნა ჩინეთში 2016 წელს. იგი წარმოადგენს ბიტკოინის მაინინგის სპეციალურ მოწყობილობას.

კრიპტოვალუტის მიმოქცევის სფეროში ხშირ შემთხვევაში ერთი და იგივე მნიშვნელობით გამოიყენება ტერმინები მოპოვება (მაინინგი) და გამომუშავება, რაც არამართებულია. ამიტომ მიზანშეწონილად მიგვაჩნია გავმიჯნოთ ამ ტერმინების მნიშვნელობები.

კრიპტოვალუტის **მოპოვება** გულისხმობს ახალი ვირტუალური მონეტის მაინინგს. ხოლო **გამომუშავების** დროს ხდება არსებული ვირტუალური მონეტების გადაცემა ერთი ფიზიკური ან

იურიდიული პირიდან მეორესადმი, ვაჭრობის ან კრანის [17] გზით.

კრიპტოვალუტის მოპოვება (მაინინგი) და გამომუშავება ხორციელდება ისეთი ხერხებით, როგორიცაა: ვიდეო ბარათების გამოყენება და ღრუბლოვანი მაინინგი, კრიპტოვალუტის გამომუშავება ხორციელდება კრიპტოვალუტის კურსის ცვლილების საფუძველზე და კრანის გამოყენებით.

ღრუბლოვანი მაინინგი არის ციფრული ფულის გამოშვების ახალი მოდელი, რომელსაც ქმნიან მაინინგ – ჯგუფები (მაინინგ პულები*) დიდი შემოსავლების მიღების მიზნით, მეიჯარის მონეობილობების გამოყენებით. ამ შემთხვევაში მეიჯარე წყვეტს ყველა წარმოქმნილ პრობლემას, დაკავშირებულს ტექნიკურ და პროგრამულ უზრუნველყოფასთან. მეიჯარე კომპანია თვითონ აწარმოებს ან შეიძენს კრიპტოვალუტის მოსაპოვებლად საჭირო მონეობილობებს და შემდეგ ახდენს მათ გაცემას იჯარით საბოლოო კლიენტებზე. ღრუბლოვანი მაინინგის შემთხვევაში ისეთი დანახარჯების ანაზღაურება, როგორიცაა: ელექტროენერგია, ინტერნეტში ჩართვა და მონეობილობებისა და პროგრამული საშუალებების გამართვა წარმოებს მეიჯარე კომპანიის მიერ. ღრუბლოვანი მაინინგი კლიენტს ათავისუფლებს კრიპტოვალუტის მაინინგის პროცესში წარმოქმნილი პრობლემებისაგან, როგორიცაა: შეფერხებები ინტერნეტის ქსელში, ელექტრომომარაგებაში, მონეობილობების მოცდენები და სხვ.

როგორც ზემოთ აღვნიშნეთ ღრუბლოვანი მაინინგის დადებითი მხარეა ის, რომ ტექნიკურ და პროგრამულ უზრუნველყოფასთან დაკავშირებულ ყველა პრობლემას წყვეტს მეიჯარე. იგი წარმოადგენს ბიტკოინებისა და ალტკოინების გამართივებულ მაინინგს, რომელიც ათავისუფლებს მაინერებს ელექტროენერ-

* მაინინგ პული – ეს არის კომპანია, რომელიც ერთმანეთთან აერთიანებენ მაინერების ჯგუფს და ამით კოორდინირებას უწევენ ყველა მომხმარებლის სიმძლავრეს. ათასობით მომხმარებელი ერთიანდება მაინინგ პულზე, რათა საერთო სიმძლავრე მიმართონ ბლოკის გამოსათვლელად, ხოლო გამოთვლის შემდეგ იღებენ ჯილდოს. რაც უფრო დიდია პულის სიმძლავრე, მით მეტია გამომუშავებული კრიპტოვალუტა.

გიის დანახარჯებისგან და საკუთარ მოწყობილობებზე პროგრამული უზრუნველყოფის დაყენებისაგან.

ღრუბლოვანი მაინინგის უარყოფითი მხარეა ის, რომ შეიძლება შემოგვთავაზონ არარსებული სიმძლავრეები, გართულებულია გამომუშავებული საშუალებების კონტროლი, შეუძლებელია ერთი სახის ვალუტიდან მეორეზე გადასვლა და სხვ.

კრიპტოვალუტისთვის დამახასიათებელია კურსის მაღალი ცვლილება. ამიტომ შესაძლებელია კრიპტოვალუტის გამომუშავება მისი კურსის ცვლილების საფუძველზეც, რაც კრიპტოვალუტის მაინინგის ერთერთი ხერხია.

კრიპტოვალუტის მოპოვება კრანის გამოყენებით მისი ყველაზე მარტივი ხერხია და არ მოითხოვს კლიენტისაგან (მომხმარებლისაგან) სპეციალურ ცოდნას, მომზადებასა და კაპიტალდაბანდებას. ამისთვის საჭიროა მხოლოდ კლიენტის სურვილი და დრო. კრანი – ეს არის სპეციალური სერვისი (საიტი), რომელიც კრიპტოვალუტის მაინინგში მონაწილეს გადაურიცხავს კრიპტოვალუტას ისეთი მარტივი მოქმედებების შესრულებისთვის, როგორიცაა: კაპტაჩა*, ვიდეოროლიკების დათვალიერება, რეკლამაზე დაკლიკება, გადასვლა სხვა საიტებზე და სხვ.

კრანის გამოყენებით კრიპტოვალუტის მოპოვების დადებითი მხარეებია ის, რომ არაა საჭირო წინასწარი ინვესტიცია, კრიპტოვალუტის გამომუშავება შეუძლია ყველა მსურველს და მომხმარებელი თვითონ ირჩევს ბიტკოინის მოპოვების ხერხს.

ინტერნეტში განთავსებულია სხვადასხვა გემოვნების ასობით კრანი.

კრანებით მაინინგის უარყოფითი მხარეებია: მისი მეშვეობით შეუძლებელია დიდი თანხის გამომუშავება, აღნიშნული ნესით კრიპტოვალუტის მოპოვება მისაღებია იმ ადამიანებისთვის, ვისაც აქვს დიდი თავისუფალი დრო და არ გააჩნია საწყისი კაპიტალი. შემოსავალი დამოკიდებულია მაინერის აქტივობაზე.

კრიპტოვალუტის მაინინგისათვის საჭიროა: გამომუშავებული კრიპტოვალუტისთვის საფულეს შექმნა, თუმცა, შესაძლებელია

* კაპჩა არის ავტომატურად გენერირებული ტესტი, რომელიც ამოწმებს, მომხმარებელი ადამიანია თუ კომპიუტერი.

ლია გასამრჯელოს მაშინვე გამოტანა, მაგრამ ამისთვის საჭიროა გარკვეული საკომისიო გადასახადის გადახდა, რაც არც ისე მცირეა. არსებობს საფულეს რამდენიმე სახეობა: საფულე სტაციონალური კომპიუტერისთვის, საფულე მობილური მონეებისთვის და ინტერნეტსაფულე.

კრიპტოვალუტის მაინინგისათვის უნდა იქნეს არჩეული კრიპტოვალუტის რომელიმე სახეობა და პული. კრიპტოვალუტის არჩეულ სახეობაზეა დამოკიდებული მისი მოპოვების ხერხის გამოყენებაც.

პული მაინერების თანასაზოგადოებაა. დღეს კრიპტოვალუტას ინდივიდუალურად თითქმის აღარავენ მოიპოვებს. პულები ანაწილებენ გამოსათვლელ ამოცანებს მონაწილეებს შორის და ამით ამცირებენ შემთხვევითობებს ამ პროცესში. ამ შემთხვევაში ორიენტაცია კეთდება საკომისიო გადასახადის რაოდენობაზე, მაინინგის პროგრამის სირთულეზე და თანასაზოგადოების წევრებზე გასამრჯელოს განაწილებაზე.

იზადება კითხვა – აქვს თუ არა მომავალი კრიპტოვალუტის მაინინგს? დასმულ კითხვაზე პასუხის გაცემა საკმაოდ რთულია. მოვიყვანოთ ცნობილი ექსპერტების პროგნოზები აღნიშნულ საკითხზე.

კიბერუსაფრთხოების პიონერის, ანტივირუსული პროგრამული უზრუნველყოფის დამფუძნებლის – ჯონ მაკაფის (McAfee) აზრით, კრიპტოვალუტა ბიტკოინის შეჩერება არავის შეუძლია. იგი გავრცელდება ყველგან და ამიტომ მას მხარი უნდა აუბას მთელმა მსოფლიომ. იგი ამბობს, რომ 100 წლის წინათ ურთიერთანგარიშსწორებისთვის ქვეყნები იყენებდნენ ოქროს. მხოლოდ მე-20 საუკუნის შუა ნახევარში დაიწყეს ვალუტის მიბმა დოლართან. მოგვიანებით შემოიტანეს ისეთი ცნება, როგორიცაა „მცოცავი“ კურსი. ოქრომ შეცვალა სასაქონლო ბარტერი, ქალაქის ფულმა შეცვალა ოქრო. სახელმწიფოთაშორის ვაჭრობის სწრაფი რეგულირების პროცესში ბიტკოინის შეუძლია შეცვალოს ქალაქის ფული და შეიძლება გამოვიდეს „კრიპტოვალუტის სტანდარტის“ სახით. არაა აუცილებელი, რომ იგი აღიაროს მთელმა მსოფლიომ. საკმარისია იგი აღიაროს რამოდენიმე ლიდერმა სახელმწიფომ, რომლებსაც მიუერთდებიან მათთან დამოკიდებული სახელმწიფოები. ამის შემდეგ დოლარის თანაბრად

დაიწყებენ ბიტკოინის და შესაძლოა სხვა ვალუტების გამოყენებას ფიქსირებული კურსით.

რატომ უნდა იყოს აღიარებული კრიპტოვალუტების სტანდარტად საკუთრივ ბიტკოინი? იმიტომ, რომ ის იყო პირველი კრიპტოვალუტა მსოფლიოში. მისი მოპოვება ისევე რთულია, როგორც ოქროსი, მოიპოვება განსაზღვრული რაოდენობით და მისი მოპოვებისათვის საჭიროა დიდი რაოდენობით ენერგია.

ამერიკელი ჰედჟ-ფონდის მენეჯერი და ინვესტორი ჯეიმს ალტუშერის აზრით, კრიპტოვალუტას შეუძლია ჩამოართვას სახელმწიფოს ფულის გამოშვების მონოპოლიის უფლება. ისევე, როგორც ინტერნეტმა ჩამოართვა კავშირგაბმულობის მონოპოლიის უფლება სატელეფონო ინდუსტრიას.

დღეისათვის ინვესტიციების ჩადება ძირითადად ხდება კრიპტოვალუტაში.

იზადება კითხვა: რა მოხდება მას შემდეგ, როდესაც ამოიწურება ცალკეული სახის კრიპტოვალუტის ემისიის რესურსი? სავარაუდოდ, გაგრძელდება მხოლოდ მისი მიმოქცევის პროცესი. არ არის გამორიცხული, რომ იგი გახდეს ფულის ერთადერთი ერთეული ქვეყანაში, რომლის დროსაც მას დაარეგულირებს მხოლოდ სახელმწიფო თავის განკარგულებაში არსებული ოქროს მარაგების შესაბამისად [16].

უახლოეს მომავალში კრიპტოვალუტის ბაზარზე, სავარაუდოდ, დარჩება მხოლოდ და მხოლოდ რამდენიმე ათეული სახის კრიპტოვალუტა. მაგ., ევროკავშირის ქვეყნებს ექნებათ კრიტოვალტის ერთი სახეობა, სხვა ქვეყნებს – მეორე და ა. შ., რაც კაცობრიობას, ალბათ, ერთიანი კრიპტოვალუტის მიმოქცევამდე მიიყვანს.

8.2. ბლოკჩეინტექნოლოგია, კრიპტოვალუტა და ციფრული ვალუტა

თანამედროვე ტექნოლოგიური ევოლუციის ეპოქაში დღეისათვის არსებული ფუნდამენტური ეკონომიკური სისტემები განიცდიან მნიშვნელოვან ტრანსფორმაციას. ერთ-ერთი ასეთი ყველაზე დამაჯერებელი ცვლილებაა მომხდარი ფინანსების

სფეროში. ამის მკაფიო მაგალითია ციფრული ვალუტების რიცხოვნობის სწრაფი ზრდა, რამაც მსოფლიო საზოგადოების ყურადღება მიიპყრო.

მთავრობის მიერ მხარდაჭერილი ციფრული ვალუტები ეფუძნებიან ციფრული ტექნოლოგიების გამოყენებას. ისინი ორიენტირებული არიან ეროვნული ეკონომიკის მართვის სტაბილურობასა და პროგრესზე და ამით, ფაქტობრივად, წამოადგენენ ასევე ტრადიციული ფიატური ფულისთვის თანამედროვე ალტერნატივასაც. ქართული ციფრული ლარის გამოჩენა ახალი საუკუნის ამ ფინანსური ცვლილებების ეტაპის დასტურია. რამდენადაც ცნობილია, საქართველო ამ ინოვაციების წინა პლანზე გამოდის. ამიტომ მნიშვნელოვანია სათანადოდ იყოს გაგებული და გაცნობიერებული ასეთი წამოწყების დინამიკა, სარგებელი და გამოწვევები. ამ თვალსაზრისით საგულისხმოა ის ფაქტიც, რომ 2017 წელს საქართველო მესამე ადგილზე იყო მსოფლიოში კრიპტოვალუტის მოპოვების მხრივ ჩინეთისა და აშშ-ის შემდეგ. წინამდებარე პარაგრაფის ძირითადი მიზანია ციფრული ვალუტების სამყაროს სიღრმისეული შესწავლა და მასთან ასოცირებული ხარჯების შედარება ტრადიციული ფიატური ფულის ხარჯებთან, სადაც მთავარი კოორდინატორი იქნება ქართული ლარი.

ციფრული ვალუტის შემოღების მთავარი ამოცანაა: ტრანზაქციების დაჩქარება და სიიაფე, შუამავლების ჩამოცილება, გამჭვირვალობა, მოსახლეობის ფინანსური უსაფრთხოების დაცვა და სხვ.

ციფრული ვალუტა. ციფრული ანუ ელექტრონული ფორმით ფულის მიმოქცევა არაა ახალი მოვლენა მსოფლიოში [11]. ქვეყნის მასშტაბით უნაღდო ანგარიშსწორების ავტომატიზებული სისტემების შექმნის თეორიული კვლევები დაიწყო გასული საუკუნის 70-ანი წლებიდან [12].

ციფრული ვალუტა არის ნებისმიერი ვალუტა, რომელიც არსებობს და მიმოქცევა მხოლოდ ელექტრონული ფორმით. იგი არ არსებობს კომპიუტერული ქსელის გარეშე. დღეისათვის ციფრული ვალუტის უმეტესობა იმავდროულად კრიპტოვალუტაცაა. კრიპტოვალუტა არის ციფრული ვალუტა, რომელიც და-

ფუძნებულია ბლოკჩეინტექნოლოგიაზე (ბლოკჩეინი, ინგლ. **Bloc-chain** – ბლოკების ჯაჭვი – მუდმივად მზარდი ჩანაწერების სია, სახელწოდებით „ბლოკები“, რომლებიც დაცულია კრიპტოგრაფიულად (ბერძ. *kryptó*-ს – საიდუმლო, დამალული), რომლის საფუძველზეც სატოში ნაკამოტომ 2008 წელს შექმნა პირველი კრიპტოვალუტა ბიტკოინი.

თვით ბლოკჩეინის შექმნის ისტორია იწყება 1982 წლიდან. ამერიკელმა კრიპტოგრაფმა დევიდ ჩაუმმა თავის დისერტაციაში პირველად წარმოადგინა ბლოკჩეინის მსგავსი პროტოკოლი [18], რომელიც შემდგომ განავითარეს პროგრამისტმა სტიუარტ ჰაბერტმა და ფიზიკოსმა სკოტ შტორნემმა. მათ გამოიგონეს დეცენტრალიზებული განაწილებული რეესტრი [19].

ელექტრონული ფულის მიმოქცევის პროცესის მუდმივი განვითარების კლასიკური მაგალითია ფულად-საკრედიტო სისტემაში მისი ისეთი სახეობის გამოჩენა, როგორიცაა კრიპტოვალუტა.

როგორც ზემოთ აღვნიშნეთ კრიპტოვალუტი უმეტესობა აგებულია ბლოკჩეინ-ტექნოლოგიის საფუძველზე. ის მომავლის ტექნოლოგიაა და შექმნილია ინფორმაციის უსაფრთხოდ შენახვის, ტრანზაქციების დაჩქარების და შუამავალი რგოლების (ბანკები, ნოტარიუსები, სხვადასხვა საგადამხდელო სისტემები და ა.შ.) ჩამოსაცილებლად. დღეისათვის მისი ფუნქციონირება ხორციელდება დეცენტრალიზებულად. მასში ინფორმაცია ინახება ბლოკების სახით და უზრუნველყოფილია მათი დაცვის მაღალი დონე. ტრანზაქციების განხორციელებისას მონაცემები ხვდება ერთდროულად კრიპტოვალუტის ქსელში ჩართულ ყველა კომპიუტერში და ხდება მათი კოპირება. ტრანზაქცია ჩაითვლება შესრულებულად მხოლოდ მაშინ, როცა მას დამოწმებს ქსელში ჩართული ყველა მომხმარებელი. დამოწმება გულისხმობს ბლოკჩეინში ტრანზაქციის დამატების შემდეგ შექმნილი ბლოკების რაოდენობას. როგორც ნესი ბიტკოინ ტრანზაქციები დაცულად ჩაითვლება მინიმუმ ექვსზე მეტი დამოწმების შემდეგ. ასეთი სისტემა საშუალებას იძლევა უარი ითქვას შუამავლებზე და გამორიცხავს რომელიმე ბლოკიდან ინფორმაციის მოპარვის ან შეცვლის შესაძლებლობას, რადგან ამისთვის საჭიროა კრიპტო-

ვალუტის ქსელში ჩართული ყველა კომპიუტერის გატეხვა. ეს კი პრაქტიკულად შეუძლებელია და მიუღწეველიც, ვინაიდან სისტემა ავტომატურად ავლენს მონაცემების გაყალბების ან მოპარვის მცდელობას. ვინაიდან ეს ხდება ბლოკჩეინტექნოლოგიაში ინფორმაციის კრიპტოგრაფიული დაშიფრვისა და ჰეშირების (ჰეში – არის მათემატიკური ალგორითმი, რომელიც ნებისმიერი მოცულობის მონაცემთა მასივს გარდაქმნის ასოებისა და ციფრებისაგან შემდგარ ფიქსირებული სიგრძის სტრიქონად) ალგორითმების გამოყენებით [20].

ბლოკჩეინის სისტემა ერთდროულად გახსნილიცაა და ანონიმიურიც. ტრანზაქციის განხორციელებისთვის მომხმარებელს ენიჭება სპეციალური პერსონალური კოდი, რომლითაც მას შეუძლია სისტემაში შესვლა და მისი გამოყენება.

ბლოკჩეინის სისტემა ღიაა ასევე იმ თვალსაზრისით, რომ ნებისმიერ მომხმარებელს შეუძლია დააკვირდეს სისტემის განვითარებას და გაეცნოს გარიგებების არქივს. მომხმარებლის ინფორმაცია დაცულია არასანქცირებული შეღწევისაგან. ბლოკჩეინის მეშვეობით ტრანზაქციების განხორციელებისას არ ხდება მესამე პირისადმი საკომისიო გადასახადის გადახდა. მისი ოდენობა სხვა შემთხვევებში საკმაოდ დიდია [20].

ცნობილია, რომ ბლოკჩეინტექნოლოგიას საფუძვლად უდევს განაწილებული რეესტრის ტექნოლოგია – DLT (Distributed ledger technology). მიუხედავად იმისა, რომ ბლოკჩეინი არის განაწილებული რეესტრის ტექნოლოგია, ყველა განაწილებული რეესტრის ტექნოლოგია არ არის ბლოკჩეინი. განაწილებული რეესტრის ტექნოლოგია ცენტრალური უფლებამოსილების გარეშე ერთდროულად მრავალ მხარეს აძლევს საშუალებას ჰქონდეს წვდომა მუდმივად სინქრონიზებულ და განახლებულ ციფრულ სისტემაზე. ამ ტექნოლოგიას ეფუძნება ყველა სახის კრიპტოვალუტა, რაც უზრუნველყოფს მათ გამჭვირვალობასა და უსაფრთხოებას.

ციფრული ვალუტის სახეები. კურსის სტაბილურობის მიხედვით შეიძლება გამოიყოს სამი ძირითადი სახის ციფრული ვალუტა: არასტაბილური კრიპტოვალუტა (ბიტკოინი, ეთერიუმი და სხვ.), სტაბილური კრიპტოვალუტა ანუ სტეიბლკოინი და ცენტრალური ბანკის ციფრული ვალუტა.

არასტაბილური კრიპტოვალუტა არის ციფრული ვალუტა, რომელიც არაა უზრუნველყოფილი რაიმე სახის ნატურალური სიმდიდრით. რის გამოც მისი კურსი მუდმივად მერყეობს. დღეისათვის მისი მართვა არ ხდება მსოფლიოს რომელიმე ერთი ცენტრალური ორგანოს ან კერძო სტრუქტურის მიერ და, ამდენად, იგი ფუნქციონირებს დეცენტრალიზებულად.

ბიტკოინის აღმოცენების შემდეგ კრიპტოვალუტის ბაზარზე მრავალი ალტკოინი (გამოჩნდა. 2023 წელს ყველაზე პოპულარული ალტკოინებია: ეთერიუმი, ეოსი, ლაიტკოინი, სტელარი და მონერო. რომელთა მიზანი იყო ბიტკოინისთვის კონკურენციის გაწევა ან მისგან განსხვავებული ფუნქციების შესრულება.

როგორც ცნობილია, ბიტკოინის ფასი არასტაბილურია, რაზედაც მეტყველებს შემდეგი სტატისტიკა: 2010 წელს მისი ფასი იყო – 0,39 დოლარი; 2017 წლის აგვისტოში – 3000 დოლარი; 2017 წლის სექტემბერში – 5000 დოლარი; 2017 წლის ბოლოს – 20 000 დოლარი; 2021 წლის ბოლოს კი – 62 000-ზე მეტი დოლარი; დღეისათვის (21.05.25) ბიტკოინის ფასი არის – 108,960.36 დოლარი.

ბიტკოინის ფასის ცვლილებაზე მოქმედებს შემდეგი ფაქტორები: მოთხოვნა-მიწოდება, ინფორმაციის მასობრივ საშუალებებში გაკეთებული დადებითი ან უარყოფითი შეფასებები, ინფრასტრუქტურა, ცნობილი ადამიანების განცხადებები, სახელმწიფოების დამოკიდებულება კრიპტოვალუტის მიმართ.

ციფრული ვალუტის არასტაბილურობის თავიდან ასაცილებლად ზოგიერთმა ქვეყანამ შემოიღო კრიპტოვალუტის ისეთი სახეობა, როგორიცაა სტეიბლკოინი.

სტეიბლკოინი არის ფიქსირებული ანუ მდგრადი კურსის მქონე ციფრული ვალუტა. კრიპტოინდუსტრიაში მეტად გავრცელებული სტეიბლკოინები მიბმულია დოლარის ფასთან. ასეთი სტეიბლკოინია – Tether (USDT). 1 USDT ტოლია 1 დოლარის და გააჩნია მინიმალური გადახრა დოლარის ფასიდან. არსებობს ისეთი სტეიბლკოინი, რომელიც მიბმულია ევროსთან. მაგალითად, Stasis Euro (EURS). აგრეთვე არის ისეთი სტეიბლკოინები, რომლებიც მიბმულია ოქროსთან. კერძოდ – PAX Gold (PAXG) და Tether Gold (XAUT) [21].

2023 წელს საგადახდელო სისტემამ PayPal-მა (აშშ) გამოუშვა საკუთარი სტეიბლკოინი PYUSD, რომლითაც შესაძლებელია სხვადასხვა გადახდების, ასევე ქვეყნის შიდა და საერთაშორისო გზავნილების განხორციელება. იგი გაშვებულია ეთერიუმის ქსელში ERK-20-ის ფორმატით. მისი ემიტენტია Paxos [22].

ცენტრალური ბანკის ციფრული ვალუტა (ცბცვ). ცენტრალური ბანკის ციფრული ვალუტა იგივე კრიპტოვალუტაა.

როგორც ცნობილია, ფიატური ფული არსებობს ბანკნოტების ან მონეტების სახით, ხოლო ციფრული ვალუტა მხოლოდ ციფრული ფორმით. თავისი არსით ციფრული ვალუტა არის ჩანაწერი, რომელიც ინახება ელექტრონულად. ცენტრალური ბანკის ციფრული ვალუტა მხარდაჭერილია სახელმწიფოს ცენტრალური ბანკის მიერ და წარმოადგენს ფიატური ფულის ანალოგს [23], განსხვავებით კრიპტოვალუტებისგან, როგორიცაა: ბიტკოინი, ეთერიუმი და სხვ., რომელნიც ფუნქციონირებენ დეცენტრალიზებულად და არ არიან მიბმული რომელიმე სახელმწიფო მარეგულირებელ ორგანოსთან.

კრიპტოვალუტები საქართველოში არ წარმოადგენს გადახდის კანონიერ საშუალებას. მასთან დაკავშირებული საქმიანობა არ რეგულირდება საქართველოს კანონმდებლობით და, შესაბამისად, ვირტუალური ვალუტა არ წარმოადგენს ეროვნული ბანკის რეგულირების სფეროს.

დღეისათვის მსოფლიოს 87 ქვეყანა მუშაობს cbcv-ზე. მათ შორის არის საქართველოც.

ფულის ადრეულმა ვერსიებმა გზა გაუხსნა დღევანდელ დახვეწილ ციფრულ ვალუტას, როგორიცაა ბიტკოინი. 2008 წელს ბიტკოინის ჩაშვებამ მიმოქცევაში გარდამტეხი როლი შეასრულა აღნიშნულ სფეროში. ამგვარმა დეცენტრალიზებულმა კრიპტოვალუტამ გამოიწვია გლობალური ინტერესი ბლოკჩეინის ტექნოლოგიისა და დეცენტრალიზებული სისტემების პოტენციალის მიმართ. ამიტომ მსოფლიოს არაერთმა ქვეყანამ მალევე გააცნობიერა კრიპტოვალუტების გამოყენების პოტენციური სარგებელი და დაიწყო მთავრობის მიერ მხარდაჭერილი ციფრული ვალუტების შემუშავება. მიუხედავად ციფრულ ვალუტებს შორის

რიგი განსხვავებისა, მათი უმეტესობის ძირითადი ფუნდამენტური პრინციპები ერთნაირია.

ციფრული ვალუტის მუშაობის სპეციფიკა. ციფრული ვალუტების მუშაობის სპეციფიკა რთულია. ისინი ეფუძნებიან ეკონომიკას, კომპიუტერულ ტექნოლოგიასა და კრიპტოგრაფიას.

ციფრული ვალუტების გამოყენებისას მნიშვნელოვანია ციფრული საფულებების გახსნა და ტრანზაქციების განხორციელება. ციფრული ვალუტების შესანახად და სამართავად მომხმარებლები იყენებენ ციფრულ საფულებებს. ეს შეიძლება იყოს აპარატურა, ან პროგრამული უზრუნველყოფა. როდესაც მომხმარებელს სურს ციფრული ვალუტის გაგზავნა, ის ტრანზაქციისთვის იყენებს თავის ციფრულ საფულეს. ეს ტრანზაქცია შემდეგ გადაეცემა ქსელს და ელოდება დამოწმებას. დამოწმების შემდეგ ტრანზაქცია ემატება რეესტრში არსებულ მონაცემებს და ციფრული ვალუტა გადადის ერთი მომხმარებლის საფულედან მეორე მომხმარებლის საფულეში. ტრანზაქციების დასაცავად და ახალი ერთეულების შექმნის გასაკონტროლებლად ციფრული ვალუტები იყენებენ კრიპტოგრაფიულ მეთოდებს.

ციფრულ საფულებებს გააჩნიათ ორი გასაღები: საჯარო ანუ ღია, რომელიც ხელმისაწვდომია ყველასთვის და პირადი ანუ დახურული, საიდუმლო, რომელიც ცნობილია მხოლოდ მისი მფლობელისთვის. უაღრესად მნიშვნელოვანია პირადი გასაღების უსაფრთხოების უზრუნველყოფა, რადგან მისი დაკარგვა ნიშნავს საფულეში არსებული ციფრული ვალუტის დაკარგვას.

ციფრული ვალუტის დადებითი მხარეები და ნაკლოვანებები. ციფრულ ვალუტებს, ტრადიციულ ფიატურ ვალუტებთან შედარებით, გააჩნიათ როგორც უნიკალური უპირატესობები, ასევე ნაკლოვანებები. ციფრულ ვალუტებს, განსაკუთრებით ბლოკჩეინ ტექნოლოგიის მხარდაჭერით, შეუძლიათ შუამავლების გარეშე, ხელი შეუწყონ უფრო სწრაფ ტრანსსასაზღვრო ტრანზაქციებს, შეამცირონ გადარიცხვის დრო დღეებიდან წამებამდე. შუამავლების საჭიროების აღმოფხვრა ან შემცირება ასევე იწვევს ტრანზაქციის საკომისიო გადასახადის შემცირებას, რაც განსაკუთრებით მომგებიანი შეიძლება გახდეს საერთაშორისო ფულადი გზავნილების დროს.

ციფრული საფულის ფუნქციონირებისთვის აუცილებელია ინტერნეტთან წვდომა, რითაც ციფრულ ვალუტებს შეუძლიათ მიანოდონ ფინანსური სერვისები მოსახლეობის უზარმაზარ სეგმენტებს, რომლებსაც არა აქვთ ბანკებთან ახლო ფიზიკური ურთიერთობა ან საკმარისი მომსახურება. როგორც ევროკავშირის ბლოკჩეინისა და ხელოვნური ინტელექტის მრჩეველი ლევან ბოძაშვილი აღნიშნავს, საქართველოში ციფრული ვალუტის გამოშვება მოსახლეობას სხვადასხვა სახის გადასახადების გადახდისას ყოველწლიურად დააზოგვინებს 600-700 მილიონ ლარს. აღარ იქნება საჭირო შუამავალი ბანკები და სხვა საგადასახადო სისტემები. მომხმარებელი ციფრული ლარით პირდაპირ გადაუხდის გადასახადს ელექტროენერგიის მომწოდებელ კომპანიებს, ბანკის გარეშე [24].

ციფრულ ვალუტას შეუძლია ასევე აღმოფხვრას საერთაშორისო ანგარიშსწორებაში არსებული ისეთი ნაკლოვანებები როგორცაა: სიძვირე, შენელებული ტრანზაქციები, შეზღუდული წვდომა, გაუმჭირვალობა და სხვ. საერთაშორისო გადარიცხვების დრო შემცირდება სტანდარტული 3-5 დღიდან 2-10 წამამდე [25].

ცენტრალური ბანკის ციფრული ვალუტა უზრუნველყოფს ფინანსურ სერვისებთან თანაბარ წვდომას.

ცბცვ-ს შემოღების შემთხვევაში ქვეყნის ცენტრალურ ბანკს შეუძლია განახორციელოს ფულის მასის რეგულირების უფრო ეფექტიანი მონეტარული პოლიტიკა და კონტროლი, რაც საბოლოოდ ნიშნავს ბანკის მხრიდან ეკონომიკაში პირდაპირ და სწრაფ ჩარევას. ციფრული ვალუტების შემოღებისას ერთ-ერთი მთავარი ამოცანაა ფასების სტაბილურობის მაღალი დონის უზრუნველყოფა. სწორედ ამისთვის იქნა შემოღებულ სტიმულები.

ცბცვ-ის დანერგვას შესაძლოა თან ახლდეს ტექნოლოგიური ბარიერები. ამ მხრივ პირველ რიგში საჭიროა ფართო საზოგადოების მიერ ციფრული ვალუტის გამოყენების ელემენტარული ცოდნა, მისდამი ნდობის გამოცხადება და მხარდაჭერა. განსაკუთრებით მოსახლეობის ხანდაზმულ და ტექნიკურად ნაკლებად გაცნობიერებულ ნაწილს ესაჭიროება ცბცვ-ის თავისებუ-

რებებისა და გამოყენების შესახებ ახსნა-განმარტება, ტრენინგების ორგანიზება.

ბანკის მიერ ციფრული ვალუტის გამოყენებისას განსაკუთრებული ყურადღება ექცევა კონფიდენციალურობის დაცვას, ვინაიდან მთავრობას შეუძლია ციფრულ ვალუტაზე ზედამხედველობის განხორციელება. მიუხედავად იმისა, რომ ბლოკჩეინის ტრანზაქციები გამჭვირვალეა, მათზე დაკვირვება შესაძლებელია ინდივიდების დონემდე. ეს იწვევს პირადი ფინანსური კონფიდენციალურობის დარღვევასა და, შესაბამისად, საზოგადოების შემფოთებასაც, განსაკუთრებით ბანკის ციფრული ვალუტის გამოყენებასთან დაკავშირებით, სადაც მთავრობას შეუძლია მასზე ზედამხედველობის განხორციელება.

საქართველოს ციფრული ვალუტების ნორმატიულ-სამართლებრივი ბაზის განვითარება ჩამორჩება მისი დანერგვის სწრაფ განვითარებას, რამაც შეიძლება გამოიწვიოს პოტენციური სამართლებრივი და ტექნოლოგიური დაცვის პრობლემები. ციფრული ვალუტების ფართოდ გამოყენება აუცილებლად გამოიწვევს არსებული ფინანსური ინსტიტუტებისა და სისტემების ცვლილებებს, რასაც შეიძლება მოჰყვეს ეკონომიკური განვითარების გარკვეული რყევები.

მსოფლიოს სხვადასხვა ქვეყნის ცენტრალური ბანკების ციფრული ვალუტები. ციფრული ვალუტის დანერგვის განვითარებასთან ერთად მსოფლიოს რამდენიმე ქვეყანამ წამოიწყო საკუთარი მთავრობის მიერ მხარდაჭერილი ციფრული ვალუტის შემუშავების პროექტები. თითოეულ მათგანს აქვს თავისი უნიკალური მიზნები, სტრატეგიები და გამოწვევები.

დღეისათვის მსოფლიოში ისეთი ქვეყნის ბანკებმა, როგორიცაა: ნიგერია, იამაიკა, ბაჰამის კუნძულები და სხვა – მიმოქცევაში უკვე ჩაუშვა ცენტრალური ბანკის ციფრული ვალუტები. ხოლო ისეთი ქვეყნების ბანკები, როგორიცაა: ჩინეთი, ინდოეთი, განა, ურუგვაი და სხვა – იმყოფებიან ცენტრალური ბანკის ციფრული ვალუტის პილოტირების სტადიაზე. ამ მიმართულებით ყველაზე წინაა ჩინეთი, სადაც უკვე გახსნილია დაახლოებით 120 მილიონი ელექტრონული საფულე. მათში ტრანზაქციების მოცულობამ კი შეადგინა 1.8 ტრილიონი ციფრული იუანი [26].

ჩინეთმა გამოუშვა 2 მილიარდი ერთეული „ციფრული იუანი“ და 100-100 ათასი ცალი დაურიგა შანხაის მოსახლეობას [24]. ამ უკანასკნელმა მნიშვნელოვნად შეუწყო ხელი ჩინეთის დიდ ქალაქებში მსგავსი საპილოტე პროექტების განხორციელებას.

ჩინეთის მსგავსად Riksbank-ის მიერ შვედეთში წარმატებით მიმდინარეობს შვედური ელექტრონული კრონის ანუ „eKrona“-ს ციფრული ვერსიების შემუშავება, რომლის მიზანია ნაღდი ფულის გამოყენების შემცირება და მისი მთავრობის მიერ მხარდაჭერილი ციფრული ალტერნატივის უზრუნველყოფა. პროექტი ჯერ კიდევ საპილოტე ფაზაშია, იკვლევს ტექნოლოგიურ გადაწყვეტილებებსა და სრულმასშტაბიანი განხორციელების შედეგებს [27].

ბაჰამის კუნძულებმა გამოუშვა ქვიშის დოლარი (Sand Dollar), რითაც იგი გახდა პირველი ქვეყანა მსოფლიოში, რომელმაც მობილური აპლიკაციის საშუალებით ოფიციალურად განახორციელა ციფრული ვალუტის შემოღება.

ქვიშის დოლარით შესაძლებელია ტრანზაქციების განხორციელება ინტერნეტის გარეშეც [28]. თუმცა, როგორც იუწყებიან, ქვეყანაში ქვიშის დოლარის დანერგვაში წარმოიშვა პრობლემები მას შემდეგ, რაც გასული წლის ნოემბერში ბირჟა TX-მა საკუთარი თავი გამოაცხადა გაკოტრებულად. ბირჟა დაფუძნებული იყო ბაჰამის კუნძულებზე [29].

ევროპის ცენტრალური ბანკი აქტიურად იკვლევს ციფრული ევროს პოტენციალს. მიმდინარეობს ფართო კვლევა და საჯარო კონსულტაციები, რათა შეფასდეს ციფრული ვალუტის გამოყენების მიზანშეწონილობა და საზოგადოების ინტერესი მის მიმართ.

ევროპის ცენტრალური ბანკის მიზანია ევროს შენარჩუნება ციფრული ეპოქისთვისაც. ამით მას სურს შესთავაზოს ადამიანებს გადახდის უსაფრთხო მეთოდი და შეინარჩუნოს ფულადი სუვერენიტეტი კერძო ციფრულ ვალუტებზე. ციფრული ევროს გამოშვების დაწყებას ევროპის ცენტრალური ბანკი გეგმავდა 2024 წლისთვის. ცენტრალური ბანკის ციფრული ვალუტის შემოღება გამორიცხავს შუამავლის საჭიროებას. თუმცა, იმასაც

არ გამორიცხავენ, რომ მის შემოღებას შეიძლება მოყვეს გარკვეული რისკები. კერძოდ, მსოფლიოს საფინანსო ბაზარზე არასტაბილურობის ფონზე ევროპის კომერციულ ბანკებში შეიძლება შემცირდეს აქტივები [30].

გარდა ზემოთ განხილული ქვეყნებისა, სადაც წარმატებით მიმდინარეობს ცენტრალური ბანკების ციფრულ ვალუტაზე გადასვლის სამუშაოები, შეიძლება გამოვყოთ რამდენიმე ქვეყანა, რომელიც სწავლობს და იკვლევს ქვეყანაში ციფრული ვალუტის შესაძლო გამოყენების, ცენტრალური ბანკის ციფრული ვალუტის ფიატურ ფულთან დამოკიდებულებისა და ფინანსური კონკურენტუნარიანობის შენარჩუნების საკითხებს. ასეთია, მაგალითად, იაპონია. იაპონიის ცენტრალურმა ბანკმა წარმატებით გაიარა საკუთარი ციფრული ვალუტის – იენის POC (Proof of Capacity) კონცეფციის ექსპერიმენტის მეორე ფაზა და გადავიდა პილოტირების ფაზაზე. აღნიშნული ექსპერიმენტის პროცესი მიმდინარეობდა 2022 წლის აპრილიდან 20-23 წლის მარტის ჩათვლით [31].

კორეის ბანკი იწყებს ცენტრალური ბანკის ციფრული ვალუტის გამოყენების ტესტირებას. კრიპტოვალუტისგან განსხვავებით ცენტრალური ბანკის ციფრული ვალუტა წარმოადგენს ოფიციალურ საგადახდელო საშუალებას, რომელსაც აკონტროლებს სახელმწიფო [32].

ქვეყნის ცენტრალური ბანკის ციფრული ვალუტის გამოყენების მთავარი ტექნოლოგიური გამოწვევაა ისეთი საიმედო სისტემების შემუშავება, რომელსაც შეეძლება დააკმაყოფილოს მისადმი მოთხოვნები ეროვნული მასშტაბით.

საქართველოს ეროვნული ბანკი ახალი ფინანსური ტექნოლოგიების გამოყენების ხელშეწყობის, საგადასახდო სისტემის ეფექტიანობის გაზრდისა და ფინანსური ჩართულობის გაუმჯობესების მიზნით 2020 წლიდან აქტიურად იკვლევს ცენტრალური ბანკის ციფრული ვალუტის მახასიათებლებს, მათ შორის, ციფრული ლარის შესაძლებლობებს, სისტემურ მოწყობასა და ბაზარზე მისი გამოყენების გზებს. ამის დასტურია ის ფაქტი, რომ 2021 წლის 30 აპრილს, საქართველოს ეროვნულმა ბანკმა, ციფრული ლარის პროექტის პირველი ეტაპის დაწყების შესახებ გა-

ნაცხადა და დაინტერესებული ფინანსური ტექნოლოგიების მიმწოდებელი კომპანიები თანამშრომლობისთვის მოიწვია. პროექტის პირველი ეტაპის დამთავრების საბოლოო ვადად განისაზღვრა 2023 წლის 15 თებერვალი [33].

გრძელვადიანი კვლევისა და სათანადო განხილვების შემდეგ, ეროვნულმა ბანკმა 2023 წელს გამოაქვეყნა ისეთი კომპანიებისგან შემდგარი სია, რომელთაც პლატფორმის რეალურ გარემოში ტესტირების შესაბამისი გამოცდილება და საკმარისი ტექნოლოგიური პოტენციალი გააჩნდათ. ესენია: AUGENTIC GmbH, Bitt Inc, Broxus Holdings Ltd, Currency Network Ltd, DCM Corp Limited, eCurrency Mint Inc, FARI Solutions Ltd, Ripple Labs, Inc, Sovereign Wallet Co., Ltd.

ჩამოთვლილი კომპანიებიდან ეროვნულმა ბანკმა 2023 წელს პარტნიორად აირჩია კომპანია „Ripple“ [34].

ციფრული ვალუტის შექმნასა და დანერგვასთან დაკავშირებული ღონისძიებები. სახელმწიფოს მიერ მხარდაჭერილი ციფრული ვალუტის შექმნა მრავალმხრივი გამოწვევაა. იგი სცილდება ტექნოლოგიურ ინფრასტრუქტურის სფეროებს და მოიცავს მარეგულირებელ, ეკონომიკურ და სოციალურ ასპექტებს.

ცენტრალური ბანკის ციფრული ვალუტის გამოშვების ძირითადი ტექნოლოგია შეიძლება იყოს ბლოკჩეინი ან განაწილებული რეესტრის სხვა ფორმა. არჩევანის გაკეთება მათ შორის ხშირად დამოკიდებულია ტრანზაქციის სასურველ სიჩქარეზე, უსაფრთხოების დონესა და დეცენტრალიზაციის ხარისხზე.

ცენტრალური ბანკის ციფრული ვალუტის მოხერხებულობა, უსაფრთხოება, ხელმისაწვდომობა და ციფრული საფულეს შექმნა გადამწყვეტია საზოგადოების მიერ მისი აღიარებისა და ცნობადობისთვის.

ციფრული ვალუტის შემოღებას სჭირდება მკაფიო სამართლებრივი განმარტება და პასუხის გაცემა ისეთ საკითხებზე, როგორიცაა: ციფრული ვალუტისა და ნაღდი ფულის ტოლფასობა, მის მიერ პროცენტის გამომუშავება, მისი მფლობელის უფლებები, მოვალეობები და სხვ.

არსებობს ფულის გათეთრების წინააღმდეგ ბრძოლის სტანდარტები: AML (Anti Money Laundering – ფულის გათეთრების წინააღმდეგ ბრძოლის სტანდარტი) და KYC (know your customer – იცნობდე შენს მომხმარებელს) [35]. KYC (know your customer – იცნობდე შენს მომხმარებელს) არის საბანკო და საფინანსო რეგულირების ტერმინი საფინანსო ინსტიტუტებისთვის და ბუკმეკერული კომპანიებისთვის.

ციფრული ვალუტის გამოყენების შემთხვევაში შემუშავებულია მომხმარებელთა უსაფრთხოების რეგულაციებმა უნდა დაიცვას მომხმარებლები თაღლითობის, სისტემის გაუმართაობისა და ციფრულ ტრანზაქციებთან დაკავშირებული სხვა რისკებისაგან.

ცენტრალური ბანკების მოვალეობაა განიხილონ ციფრული ვალუტის ზემოქმედება დაკრედიტების განაკვეთებზე, ინფლაციასა და მთლიან ეკონომიკურ ზრდაზე.

მნიშვნელოვანია იმის გარკვევა, თუ როგორი იქნება ცენტრალური ბანკის ციფრული ვალუტის თანაარსებობა არსებულ საბანკო სისტემასთან: ჩაანაცვლებს, შეავსებს, თუ იმუშავებს იგი არსებული ფინანსური სტრუქტურების პარალელურად.

ციფრულ ვალუტაზე გადასვლისას საჭიროა გათვალისწინებული იქნას საზოგადოების დამოკიდებულება მისადმი. საწყის ეტაპზე ამ მიმართულებით, საზოგადოების ცნობადობის ამაღლების მიზნით აუცილებელი იქნება სასწავლო დაწესებულებებთან ან მუნიციპალიტეტებთან ციფრული ვალუტის გამოყენების, უპირატესობებისა და უსაფრთხოების შემსწავლელ ცენტრების შექმნა.

სახელმწიფოში ცენტრალური ბანკის მიერ ციფრული ვალუტის სრულმასშტაბიან დანერგვამდე დიდი მნიშვნელობა აქვს საზოგადოებასთან მჭიდრო კავშირს, რათა გათვალისწინებულ იქნას რეალურ ცხოვრებაში არსებული პრობლემები და საზოგადოების გამოხმაურებები. ციფრული ვალუტის გამოყენებისას მნიშვნელოვანია ტრანზაქციული მონაცემებისა და მომხმარებლების პირადი ინფორმაციის კონფიდენციალურობის უზრუნველყოფა, მათი დაცვა ჰაკერების კიბერშეტევებისაგან და სხვ.

დაბოლოს, ციფრული ვალუტის გამოყენებისას საერთაშორისო ვაჭრობის განხორციელებისა ან ფულის გადარიცხვისათვის აუცილებელია ფულის გაცვლითი კურსის, საგარეო პოლიტიკის, საერთაშორისო რეგულაციებისა, ფინანსურ სისტემებთან თანამშრომლობისა და სხვა გარემოებების გათვალისწინება.

ციფრული ფულისა და ფიატური ფულის შექმნასა და დანერგვასთან დაკავშირებული ხარჯები. ციფრული ვალუტის შემოღება მნიშვნელოვან გავლენას მოახდენს არსებულ ფინანსურ სისტემაზე, ვინაიდან ამით არსებითად იცვლება ასევე მთლიანად ქვეყნის ფინანსური ლანდშაფტი.

ციფრული ვალუტის, კერძოდ, ცენტრალური ბანკის ციფრული ვალუტის, შემუშავება, დანერგვა და შენარჩუნება დაკავშირებულია გარკვეულ ხარჯებთან.

ცენტრალური ბანკის ციფრული ვალუტის პროექტის დაწყებამდე სასიცოცხლოდ აუცილებელია მისი სავარაუდო ეკონომიკური და სოციალური შედეგების წინასწარი შეფასება. ამისათვის საჭიროა საპილოტე პროგრამების მიერ ციფრული ვალუტის შემოწმება კონტროლირებად გარემოში, რაც საშუალებას იძლევა გაირკვეს საზოგადოების რეაქცია მის მიმართ მანამ, სანამ ის დაინერგება საერთოდ ქვეყნის მასშტაბით. საპილოტე პროგრამებმა შეიძლება მოითხოვოს მათი ინფრასტრუქტურის, ადამიანისუფლი რესურსებისა და საზოგადოების ჩართულობის აუცილებლობა.

ციფრული ვალუტის დანერგვა მოითხოვს ისეთი ხარჯების გაღებას, როგორიცაა: ბლოკჩეინის ან სხვა რომელიმე განაწილებული რეესტრის ტექნოლოგიური სისტემის აგება, კონსენსუსის მექანიზმების ინტეგრირება, სისტემის მასშტაბურობა და სხვ. გარკვეული ინვესტიციების ჩადება იქნება საჭირო ციფრული საფულეს ინტერფეისისა და უსაფრთხოების მახასიათებლების შესამუშავებლად. აუცილებელი იქნება უსაფრთხოების ძლიერი სისტემების შექმნა, რომელიც მოითხოვს დაცვის სისტემების რეგულარულ განახლებებს, დაუცველობის ხარისხის შეფასებას, პოტენციური საფრთხეებისგან დაცვის ზომების გატარებას და სხვ. რაც დაკავშირებული იქნება გარკვეულ ხარჯებთან. აგრეთვე საჭირო იქნება ხარჯების გაწევა საზოგადოების განათლებისა და ცნობიერების ამაღლებისთვის, სარეკლამო მასა-

ლების, ტრენინგსესიებისა და საზოგადოების ინფორმირებულობის კამპანიების ორგანიზებისთვის. ეს უკანასკნელი ხელს შეუწყობს ახალი სისტემისთვის მხარდაჭერას და მის აღიარებას. დანახარჯების განევა აგრეთვე საჭირო იქნება არსებულ ფინანსურ სისტემებთან ინტეგრირებისთვის. სისტემის დანერგვასა და გამოყენებას დასჭირდება აგრეთვე ისეთი საოპერაციო ხარჯების განევა, როგორიცაა: ადამიანისეული რესურსების, ელექტროენერგიის, მომხმარებლის მხარდაჭერისა და სერვერის ხარჯები, რიგი გაუთვალისწინებელი ხარჯები და სხვ.

ფიატური ფულის გამოყენება მოითხოვს დანახარჯებს მის დასაბეჭდად (მოსაჭრელად) და მასალების, შრომისა და უსაფრთხოების უზრუნველსაყოფად. აღნიშნული ხარჯების გარდა, ფიატური ვალუტის გამოყენება დაკავშირებულია ბანკნოტების ცვეთასთან, გაყალბების პრევენციასთან და დაზიანებული, გაცვეთილი, დაკარგული ბანკნოტებისა და მონეტების შეცვლასთან. ციფრული ვალუტის დაზიანება პრაქტიკულად ნულოვანია, რადგან ის ელექტრონულია.

ფიატური ფულის გამოყენება საჭიროებს ფიზიკური ვალუტის ტრანსპორტირებისა და უსაფრთხოების დაცვის, ასევე ბანკომატების მოვლასთან ბანკის ფილიალების მუშაობასთან და სხვა დაკავშირებული ხარჯების განევას.

ციფრული ვალუტის შემთხვევაში ტრანზაქციებზე განეული ხარჯების საკომისიო გადასახადი ან მინიმალურია, ან საერთოდ არ გაიღება. გაიწევა მხოლოდ ხარჯები, რომელიც დაკავშირებულია ციფრული ვალუტის სხვა ფორმებად გადაქცევასთან. ფიატური ფულის შემთხვევაში ხარჯების გაღება აუცილებელია საკომისიო გადასახადის სახით საბანკო ტრანზაქციებზე, განსაკუთრებით საერთაშორისო გადარიცხვებზე. გასათვალისწინებელია ასევე საკრედიტო-სადებეტო ბარათით განხორციელებულ ოპერაციებთან დაკავშირებული ხარჯები, დამუშავების საკომისიო გადასახადის ჩათვლით.

გარკვეული ხარჯების განევაა საჭირო როგორც ციფრული ვალუტის, ასევე ფიატური ფულის შესანახად და უსაფრთხოების უზრუნველსაყოფად. ციფრული ვალუტის შემთხვევაში ეს ხარჯები დაკავშირებულია ჰაკერებისაგან და მონაცემთა გაჟონვისა და არაავტორიზებული წვდომისგან დაცვასთან. შენახვის ხარ-

ჯები მინიმალურია და ჩვეულებრივ ასოცირდება განაწილებული რეესტრის ან ბლოკჩეინის უსაფრთხოებასთან. ფიატური ვალუტის შემთხვევაში კი დიდია ნაღდი ფულის, მათ შორის ბანკის სარდაფებისა და კერძო სეიფების უსაფრთხოდ დაცვის ღირებულება. ამას ემატება აგრეთვე დაზღვევის ხარჯები, რომლებიც დაკავშირებულია პოტენციურ ქურდობასთან, დაზიანებასთან და სხვ.

ციფრული ვალუტის შემთხვევაში მონეტარული პოლიტიკის განსახორციელებლად პირდაპირი მონიტორინგისა და რეალურ დროში კორექტირების გზით ხდება ხარჯების პოტენციური დაზოგვა, რაც საშუალებას იძლევა სწრაფად მოხდეს რეაგირება ეკონომიკური პირობების ცვლილებაზე. ფიატური ვალუტის შემთხვევაში კი საჭიროა ღია ბაზრის ოპერაციებთან, სავალუტო ინტერვენციებთან და სხვა ტრადიციულ ფულად ინსტრუმენტებთან დაკავშირებული ხარჯების გაღება.

ციფრულ ვალუტას გააჩნია განუსაზღვრელი გამოყენების ვადა. ამიტომ მისი გამოყენების შემთხვევაში ხარჯები ძირითადად დაკავშირებულია ტექნოლოგიისა და სისტემის განახლებასთან. ფიატურ ვალუტას კი აქვს სიცოცხლის შეზღუდული ხანგრძლიობა და, შესაბამისად, მოითხოვს ჩანაცვლების (მაგ., ქალაქის კუპონები და მონეტები შეიძლება გაცვდეს, დაზიანდეს, დაიკარგოს და ა.შ.) ხარჯების გაღებას.

ციფრული ვალუტის მომავალი. როგორც ზემოთ იყო აღნიშნული, ციფრული ვალუტების დანერგვის სწრაფი ზრდა და განვითარება მნიშვნელოვან როლს შეასრულებს გლობალური ფინანსური ლანდშაფტის შეცვლაში. სავარაუდოდ, ქვეყნის მასშტაბით საპილოტე ფაზების დამთავრების შემდეგ, ბევრი ქვეყანა გადავა ცენტრალური ბანკის ციფრულ ვალუტებზე, რაც გაზრდის მის საჯარო ხელმისაწვდომობას და გამოყენებას. შემოთავაზებულ სისტემებში ტრანზაქციისთვის პერსპექტივაში უფრო და უფრო მეტი მსხვილი და მცირე ბიზნესი დაიწყებს ციფრული ვალუტებით ანგარიშსწორებას. ციფრული ვალუტის შემოღება გაზრდის ფულად ურთიერთობათა უსაფრთხოების დონეს. მოსალოდნელია უფრო სწრაფი ტრანზაქციების, უფრო ენერგოეფექტიანი კონსენსუსის მექანიზმებისა და უკეთესი მასშტაბური გა-

დანყვეტილებების მიღება. ციფრული ვალუტის მიწოდებაზე მეტი კონტროლის განხორციელების შედეგად, ცენტრალურ ბანკებს შეეძლებათ გაატარონ პირდაპირი და ადაპტიური მონეტარული პოლიტიკა. ტრადიციული საბანკო დანესებულებები უდავოდ დაინახავენ ცვლილებებს მათ ოპერაციულ პარადიგმაში, იქნებიან რა ორიენტირებული ციფრულ სერვისებზე, ინტეგრაციაზე და შემოსავლის ახალ მოდელებზე. რაც უფრო მეტი ქვეყანა გადავა ცენტრალური ბანკის ციფრულ ვალუტაზე, მით უფრო მეტად შემცირდება ტრანსსასაზღვრო ტრანზაქციების დრო და დანახარჯები. გლობალური ფინანსური სტრუქტურების პოტენციალისა და სხვადასხვა ცენტრალური ბანკის ციფრული ვალუტის თავსებადობის გაცნობიერება ხელს შეუწყობს საერთაშორისო ვაჭრობისა და ფულად ურთიერთობათა განვითარებას, საერთაშორისო ორგანიზაციების მიერ ციფრულ ვალუტებზე საერთო სტანდარტების დანესებასა და სხვ.

ფინანსური ეკოსისტემის მნიშვნელოვანი ნაწილად ციფრული ვალუტების გადაქცევის კვალდაკვალ, სავარაუდოდ, გაძლიერდება ზომები მომხმარებელთა უფლებებისა და აქტივების დასაცავად. ინტერნეტის სწრაფი გავრცელება მსოფლიოს ამჟამად ბანკებთან ნაკლებად დაკავშირებული მოსახლეობის დიდ ნაწილს მისცემს ფინანსურ სერვისებთან წვდომის შესაძლებლობას. ამიტომ აუცილებელია აქცენტი გაკეთდეს საგანმანათლებლო პროგრამებში ციფრული ვალუტების, კიბერუსაფრთხოებისა და მასთან დაკავშირებული საკითხების გაცნობიერების პროცესზე, რათა უფრო სრულყოფილად განვითარდეს კაცობრიობის ურთიერთთანამშრომლობის უნარი, როგორც ცივილიზაციის მნიშვნელოვანი უპირატესობა და მონაპოვარი გლობალურ ეკონომიკაში.

8.3. ბიტკოინის ფასზე მოქმედი ფაქტორები

ბიტკოინის ფასის ფორმირებაზე სხვადასხვა ფაქტორი სხვადასხვაგვარად მოქმედებს. მათ შორის ძირითადია: ბიტკოინზე მოთხოვნა-მიწოდება, ბიტკოინის წარმოების ღირებულება, ბიტკოინის მიმოქცევის საკანონმდებლო რეგულირება, ალტკოინებს

შორის კონკურენცია, ბირჟებზე ბიტკოინის დეფიციტი, ინფორმაციული ფონი, ბიტკოინის მიმოქცევის ქსელის სირთულე, მონეტების „დანვა“, ე. წ. „ვეშაპები“* და სხვ. [36]. განვიხილოთ ზოგიერთი მათგანი დანვრილებით.

ბიტკოინზე მოთხოვნა-მიწოდება. საერთოდ მოთხოვნა და მიწოდება არის ყველაზე მნიშვნელოვანი ფაქტორი, რომელიც განსაზღვრავს ნებისმიერი აქტივის ფასს. ბიტკოინიც არაა გამონაკლისი. იგი საქონელია. ამიტომ მისი ფასის ფორმირება ძირითადად წარმოებს ნებისმიერი საქონლის ფასის ფორმირების მსგავსად. მაგ., ოქროს ფასი იმიტომ მაღალი, რომ მისი მარაგები შეზღუდულია და მოპოვება რთული. თუ ბაზარზე უეცრად გამოჩნდება ოქროს დიდი რაოდენობა, მისი ფასიც შესაბამისად დაეცემა. ოქროს მსგავსად ბიტკოინის მარაგებიც შეზღუდულია 21 მლნ მონეტის რაოდენობით. მაგრამ ბიტკოინის კურსი მაინც ხასიათდება მაღალი ვალანტილობით და მისი ფასიც შეიძლება შეიცვალოს წამიერად. ერთ-ერთი ცნობის მიხედვით, მაგ., 2010 წლის 2 მაისს ამერიკელმა პროგრამისტმა ლაზლო ჰანეშმა ორ პიცაში, რომლის ფასი იყო – 25 დოლარი, გადაიხადა 10000 ბიტკოინი. ბიტკოინის მაშინდელი საბაზრო ფასი ტოლი იყო 0,39 დოლარის [37].

დანყებული აქედან, ბიტკოინის კურსმა 2017 წლის ბოლოსთვის მიაღწია – 20000 დოლარს. დღეისათვის მოპოვებულია 19,88 მილიონი მონეტა [36]. ყოველ 10 წუთში ხდება ერთი ახალი ბლოკის გენერაცია, რისთვისაც მაინერები გასამრჯელოს სახით, დებულობდნენ 6,25 ბიტკოინს, რომელთა რაოდენობა ავსებს მსოფლიოში არსებული ბიტკოინების მარაგს. ვინაიდან ბიტკოინებზე მოთხოვნა მეტია, ვიდრე მიწოდება, ამიტომ ბიტკოინის ფასი მატულობს. როგორც ცნობილია 2020 წლის მაისში მოხდა მაინერების ჯილდოს ჰალვინგი. მაინერების მიერ ბიტკოინის ბლოკის მოპოვებისთვის ჯილდოს განახევრება წარმოებს ყოველ ოთხ წელიწადში, რაც ხელს უწყობს მარაგების გაზრდის შეჩერებას, შესაბამისად მასზე ფასის ზრდას. 2020 წლის მაისი-

* „ვეშაპები“ არიან ადამიანები, რომლებიც ფლობენ დიდი ოდენობით ფინანსურ რესურსებს.

დან ბლოკის ფორმირებისთვის ჯილდო ტოლი გახდა 6,25 ბიტკოინის. ჰალვინგი იმოქმედებს იქამდე, სანამ მოთხოვნა იქნება მეტი, ვიდრე მარაგების შევსება. ეს უკანასკნელი გამოიწვევს ბიტკოინის ფასის ზრდას. როგორც ცნობილი გახდა, თუ ადრე ბლოკის გამოშვების ინტერვალი შეადგენდა 10 წუთს, ახლა ეს მაჩვენებელი გახდა 7 წუთი, რაც აუცილებლად გამოიწვევს სატოში ნაკამოტოს მიერ 21 მილიონი ბიტკოინის საბოლოო ემისიის დროის კორექტირებას, მისი შემცირების მიმართულებით [38].

წარმოების ღირებულება. ერთი ბიტკოინის მოსაპოვებლად საჭირო ელექტროენერგიის ღირებულება სხვადასხვაა იმისდა მიხედვით, თუ სად წარმოებს მისი მოპოვება. იმ რაიონში, სადაც ელექტროენერგიის ღირებულება ნაკლებია, მოპოვებული ბიტკოინის ღირებულებაში ელექტროენერგიის ღირებულებაც დაბალია [36]. ამიტომ მაინერები ცდილობენ ბიტკოინის მონაცემთა ცენტრები განათავსონ ელექტროენერგიის დაბალი ღირებულების მქონე განახლებად ელექტროენერგიის მწარმოებელ ობიექტებთან.

მკვლევარებს შორის მიმდინარეობს დავა ბიტკოინის ღირებულებასთან დაკავშირებით. ერთნი ამტკიცებენ, რომ „მარქსისტული შრომითი ღირებულების თეორიის“ მიხედვით ბიტკოინის ფასი დაკავშირებულია მისი მოპოვების ხარჯებთან. მეორენი ამტკიცებენ, რომ საქონლისა და მომსახურების ფასი განისაზღვრება არა მასზე გაწეული დანახარჯებით, არამედ იმ ფასით, რამდენსაც გადაიხდის მყიდველი მოცემულ მომენტში, მიუხედავად მასზე დახარჯული შრომის ღირებულებისა. ბიტკოინის შემქმნელი, სატოში ნაკამოტო მხარს უჭერს მარქსისტულ შრომითი ღირებულების თეორიას და აღნიშნავს „ნებისმიერი საქონლის ფასი მიისწრაფის მის საწარმოებლად საჭირო დანახარჯების ღირებულებისკენ“ [36].

ბიტკოინის ჰალვინგი, რომელიც ხდება ყოველ ოთხ წელიწადში ერთხელ, იწვევს ბიტკოინის მონეტის მოპოვების ღირებულების გაზრდას. თუ ბიტკოინის ფასი დაეცემა მისი თვითღირებულებაზე დაბლა, მაშინ მისი მოპოვება არამომგებიანი გახდება, რის გამოც მაინერები შეწყვეტენ მის მოპოვებას.

კრიპტოვალუტის ემისია. კრიპტოვალუტის შემქმნელები სხვადასხვაგვარად უდგებიან კრიპტოვალუტის ემისიის პროცესს. უმეტეს შემთხვევაში წინასწარაა განსაზღვრული კრიპტოვალუტების ემისიის რაოდენობა და დრო. მაგ., ბიტკოინის მონეტების რაოდენობა მისმა შემქმნელმა სატოში ნაკამოტომ წინასწარ განსაზღვრა – 21 მილიონი მონეტით. პროექტის მიხედვით Litecoin-ის რაოდენობა განსაზღვრულია 84 მილიონი მონეტით, Ripple-ს – 100 მლრდით, Stellar-ის 100 მლრდით ერთეულით, EOS-ის – ერთი მლრდით ერთეულით, TRON-ის – 99.281.283.283754 ერთეული მონეტით, Cardano-ს – 45 მლრდით, ხოლო რაც შეეხება EthReum-ს, Bitcoin Cash-ს და Monero-ს მათი ემისიის საბოლოო რაოდენობა წინასწარ არ არის განსაზღვრული [39].

ისმის კითხვა რა უფრო მომგებიანია კრიპტოვალუტის დამფუძნებლებისთვის, ის, რომ მათ მიერ გამოსაშვები ვირტუალური მონეტების რაოდენობა წინასწარ იყოს განსაზღვრული, თუ პირიქით? თუ კრიპტოვალუტის ემისიის რაოდენობა და დრო წინასწარაა განსაზღვრული და კრიპტოვალუტის ბაზარზე მოიმატებს მასზე მოთხოვნა, მაშინ შეიძლება შექმნას მისი დეფიციტი და მისმა ფასმა მოიმატოს. აგრეთვე, შეზღუდული და წინასწარ ცნობილი ემისიის რაოდენობა ხელსაყრელია მათი შემქმნელებისთვის, ვინაიდან ვირტუალური მონეტების შემქმნელებს ეძლევათ შესაძლებლობა მოახდინონ მათი რეგულირება. მაგ., განახორციელონ მონეტების „დანვა“.

კრიპტოვალუტის ფასის დაცემას იწვევს: თუ მისი ემისია წინასწარ არაა განსაზღვრული, გამოშვებულია დიდი რაოდენობით და ბაზარზე მასზე არაა მოთხოვნა.

ბიტკოინის ქსელში ჩაშვების მომენტისთვის ბლოკის მოპოვებისთვის პრემია შეადგენდა 50 ბიტკოინს. აქედან დაწყებული ყოველი ოთხი წლის ინტერვალით ბლოკის მოპოვების ღირებულება 2-ჯერ მცირდებოდა და 2020 წლის შეადგინა 6,25 მონეტა. 2032 წლისთვის მოპოვებული იქნება 20,671 მილიონი მონეტა [40].

ბიტკოინის ემისიის დამამთავრებელ ეტაპზე ბიტკოინის ბოლო ბლოკის მოპოვებისთვის პრემია გახდება ერთი სატოშის ტო-

ლი. ასეთი დაბალი პრემიის გამო მაინერები იძულებული გახდებიან უარი თქვან ბლოკის მოპოვებაზე [40]. ბიტკოინით მოხდება ძვირადღირებული საქონლისა და მომსახურების საფასურის გადახდა.

ბირჟებზე ბიტკოინის არ არსებობა – დეფიციტი. ადამიანს ბიტკოინის ყიდვა-გაყიდვა ძირითადად შეუძლია ბირჟებზე და გადამცვლელ პუნქტებში. თუ ბირჟებზე და გადამცვლელ პუნქტებში ბიტკოინების მონეტების რაოდენობა შემცირდება, მაშინ, მისი შეძენა გართულდება, რამაც საბოლოოდ შეიძლება გამოიწვიოს კრიპტოვალუტის კურსის გაზრდა.

ალტკოინების მხრიდან კონკურენცია. დღეისათვის, მსოფლიო მასშტაბით დომინირებს ბიტკოინი და ძირითადად მასთან მიმართებაში წარმოებს ალტკოინებზე ფასის ცვლილება. თუ კრიპტოვალუტის ბაზარზე გამწვავდება კონკურენცია ალტკოინებს შორის, მაშინ მოხდება ფულადი საშუალებების გადადინება ალტკოინების ბაზარზე, რომელიც გამოიწვევს ბიტკოინის კაპიტალიზაციის შემცირებას და შესაბამისად მისი ფასის დაცემას.

უნდა აღვნიშნოთ რომ კრიპტოვალუტის ბაზარზე კრიპტოვალუტების **Libra**-სა და **Gram**-ის გამოჩენა მნიშვნელოვან გავლენას მოახდენს ბიტკოინის ეკოსისტემაზე, მისი ფასის დაცემის მიმართულებით. მათი უპირატესობა ბიტკოინის მიმართ, როგორც ლეონიდ დელცინი აღნიშნავს, მდგომარეობს მომხმარებელთა დიდ აუდიტორიაში. ლიბრისათვის ეს რაოდენობა შეიძლება გახდეს ორი მილიარდი მომხმარებელი, გრამისთვის კი ას მილიონამდე, რომლებსაც შეეძლება ფულის გადასაგზავნად გამოიყენონ მარტივი და მოხერხებული საფულებები. აგრეთვე გაიზრდება იმ მაღაზიების რიცხვი, რომლებიც საქონლისა და მომსახურების ღირებულების ასანაზღაურებლად გამოიყენებენ აღნიშნულ ვირტუალურ ციფრულ ვალუტებს [41].

ბიტკოინის რეგულირება. ბიტკოინის არ გააჩნია კონკრეტული ემიტენტი, განსხვავებით ეროვნული ვალუტებისგან (საქართველოს ეროვნული ბანკი, რუსეთის ცენტრალური ბანკი, უკრაინის ეროვნული ბანკი და სხვ.). არავის არ შეუძლია „დაბეჭდოს“ ბიტკოინის ახალი მონეტები, ან „დანვას“ იგი, მისი მფლო-

ბელის თანხმობის გარეშე [42] და ამით მოახდინოს ზეგავლენა სხვა ვალუტის კურსზე. ადამიანთა გარკვეული ნაწილი ბიტკოინის ამ დადებითი თვისებების გამო ნდობას უცხადებს და იყენებს მას დანაზოგის შესანახად, რაც დადებითად მოქმედებს მის ფასზე.

რეგულირება არის ერთ-ერთი მნიშვნელოვანი ფაქტორი, რომელიც ზემოქმედებს ბიტკოინის ფასზე. მსოფლიოს ბევრი ქვეყანა ცდილობს მოახდინოს ბიტკოინის ბაზრის რეგულირება. ზოგიერთ ქვეყანაში მისი გამოყენება აკრძალულია და მის გამოყენებელს სასჯელი ემუქრება. ზოგიერთ ქვეყანაში კი კრიპტოვალუტის გამოყენება არც აკრძალულია და არც დაშვებული. მისი რეგულირების შემთხვევაში, კრიპტოვალუტის, კერძოდ კი ბიტკოინის მომხმარებელთა რაოდენობა საგრძნობლად მოიმატებს, რაც გამოიწვევს მისი ფასის ზრდას.

თითოეული სახელმწიფოს დამოკიდებულება კრიპტოვალუტის მიმართ განსხვავებულია. ზოგიერთ ქვეყანაში იგი აღიარებულია საგადასხდელ საშუალებად, ზოგიერთ ქვეყანაში კი მისი გამოყენება აკრძალულია. მაგ., აშშ-მა მსოფლიოში პირველმა აღიარა ბიტკოინი. აქ მას განიხილავენ როგორც ფასიან ქონებას. იგი აღიარებულია კანონიერ საგადასხდელ საშუალებად. ხოლო რაც შეეხება ქვეყნებს: კანადას, გერმანიას, უკრაინას, ბელორუსს, ავსტრალიას, ნორვეგიას, შვეიცარიას ბულგარეთს და სხვ. ამ ქვეყნებში მისი რეგულირება ხდება საკანონმდებლო დონეზე. ისეთ ქვეყნებში კი როგორიცაა რუმინეთი, ისლანდია, ყირგიზეთი, ჩინეთი, აქ ციფრული ვალუტის გამოყენება ითვლება კანონგარეშედ. ქვეყანაში ბიტკოინის რეგულირება, კონკრეტულად მისი აღიარება საგადასხდელ საშუალებად გაზრდის მისადმი ნდობას, რაც გამოიწვევს მასზე მოთხოვნის ზრდას.

ინფორმაციული ფონი. ბიტკოინის მიმართ ინფორმაციული საშუალებების მიერ შექმნილი ფონი, ინტერნეტპორტალებზე მისი რეკლამა, მისადმი მიძღვნილი სხვადასხვა კონფერენციები, ცნობილი ადამიანთა გამონათქვამები და სხვა გარკვეულ ზეგავლენას ახდენს ტრეიდერებზე და აიძულებს მათ შეიძინონ ბიტკოინის მონეტები, ანუ ადგილი აქვს ბიტკოინზე მოთხოვნის ზრდას. მარაგის შევსების დაბალი ტემპის გამო მასზე მოთხოვნა

იზრდება, შესაბამისად იზრდება მისი ფასი. ბიტკოინის ფასის ცვლილება შეიძლება გამოიწვიოს ბიტკოინის მიმართ ცნობილი ადამიანების გამონათქვამებმა, მოკლედ გავეცნოთ რამდენიმე ცნობილ ადამიანის გამონათქვამებს ბიტკოინის მომავალზე:

1. მარკ ჰალბერტი – ფინანსური ანალიტიკოსის და market-watch.com-ის მიმომხილველის აზრით ბიტკოინის ელის გარდაუვალი კრახი. არგამართლდა [45].

2. ინვესტორ მაიკლ ნოვოგრაძის აზრით ბიტკოინის ღირებულება 2018 წლისთვის უნდა გაზრდილიყო 4-ჯერ და მიეღწია 40 000 დოლარს. არ გამართლდა.

3. ჯონ მაკაფის პროგნოზით 2020 წელს ერთი ბიტკოინის ფასი მიაღწევს 1 მილიონ დოლარს. არ გამართლდა.

4. ჯეიმს ალტუშერი ყველაფერში უჭერდა მხარს მაკაფის, გარდა იმ დაპირებისა, რომ წაგების შემთხვევაში თავს დაისახიჩრებდა. ჯეიმს ალტუშერის პროგნოზით 2020 წელს ერთი ბიტკოინის ფასი მიაღწევს 1 მილიონ დოლარს. არ გამართლდა.

5. პიტერ სმითი თვლის, რომ კრიპტოვალუტები გახდებიან უფრო სტაბილურები და ყველა ადამიანისთვის გამოსაყენებელი.

ქსელის სირთულე. კრიპტოვალუტის დეცენტრალიზაციას ხელს უწყობს მაინინგი. ერთბაშად, რომ არ მომხდარიყო 21 მლ. ბიტკოინის მოპოვება, სატოში ნაკამოტომ 10 წუთის ხანგრძლივობით განსაზღვრა ერთი ბლოკის გენერაციის დრო. მაინინგ-მოწყობილობების სიმძლავრეების გაიზრდის შესაბამისად რთულდება მისი მოპოვების ალგორითმი. ქსელის სირთულეს აქვს უდიდესი მნიშვნელობა ბიტკოინის მოპოვების პროცესში. რაც უფრო რთულია ქსელი, მით უფრო მძლავრი მოწყობილობებია საჭირო ერთი ბიტკოინის მოსაპოვებლად. ბოლო დროს შექმნილი სიტუაცია, ბლოკის მოპოვების პრემიის განახევრება, აიძულებს მაინერებს უარი თქვან ბიტკოინის მოპოვებაზე, რადგან ფინანსურად ეს პროცესი წამგებიანია. ასეთ სიტუაციაში მაინინგ სიმძლავრეების უდიდესი ნაწილი აღმოჩნდება რამდენიმე გიგანტ მონაცემთა ბაზების მფლობელთა ხელში, ანუ ადგილი აქვს ბიტკოინის მოპოვების ცენტრალიზაციას, რაც ინვესტორებს უკარგავს

სურვილს მოახდინონ ბიტკოინის ინვესტირება. ასეთ შემთხვევაში მცირე და საშუალო ბიზნესი იძულებული ხდება გამოეთიშოს ბაზარს.

მონეტების „დანვა“. მონეტების „დანვა“ არის კრიპტოვალუტის ფასის შენარჩუნების, ან მომატების ერთ-ერთი საშუალება. ამ მეთოდის გამოყენებისას ნადგურდება გაყიდული კრიპტოვალუტის მონეტების შესაბამისი რაოდენობა. ასეთ ხერხს მისი შემქმნელები ხშირად მიმართავენ, რათა შემცირდეს მიწოდების რაოდენობა და არ დაეცეს კრიპტოვალუტის კურსი. დანვის პროცესის განხორციელება ხდება სმარტ-ფუნქციის დახმარებით, რომლის პრაქტიკაში რელიზაცია წარმოებს სმარტ კონტრაქტის ფუნქციის საშუალებით. მაგალითად, ყოველი კვარტლის ბოლოს Binance-ის მფლობელი განხორციელებული ვაჭრობის რაოდენობის შესაბამისად წვავს მონეტებს. აღნიშნული პროცესი გამჭვირვალეა და წინასწარაა საჯაროდ განცხადებული. დანვის ოპერაციის ჩანერა ხორციელდება ბლოკჩეინში, როგორც ტრანზაქცია, რაც იძლევა საშუალებას დაინტერესებულმა პირმა შეძლოს მისი შემოწმება. განადგურებული კრიპტოვალუტის მონეტების აღდგენა შეუძლებელია.

მონეტების დანვის პროცესი ანალოგიურია ეკონომიკაში გაყიდული აქციების გამოსყიდვის პროცესის. ბრუნვიდან ამოიღება გაყიდული აქციები, რათა უზრუნველყოფილი იქნეს აქციებზე ფასის მომატება. ანალოგიურად წარმოებს პროექტების განსახორციელებლად (ICO) მოზიდული იმ რაოდენობის ტოკენების მიმოქცევიდან ამოღება, რომლებიც არ იქნა გაყიდული პროექტის დამთავრების მომენტისთვის.

„ვეშაპები“. ბიტკოინის კურსი შეიძლება გაიზარდოს იმ შემთხვევაშიც, თუ ადამიანთა გარკვეული ჯგუფი, რომელთაც გააჩნიათ დიდი რაოდენობით ფულადი საშუალებები დიდი ოდენობით შეიძენენ ბიტკოინებს. აღნიშნული პროცესი ფსიქოლოგიურად მოქმედებს ტრეიდერებზე. ხედავენ რა ტრეიდერები კრიპტოვალუტაზე მოთხოვნის ზრდას, იწყებენ კრიპტოვალუტის შეძენას, რასაც მოყვება კრიპტოვალუტის კურსის დაცემა. როდესაც ბიტკოინის ფასი მიაღწევს პიკს, მაშინ კრიპტოვალუტის დიდი ოდენობით მფლობელები ე. წ. „ვეშაპები“ იწყებენ მათ გაყიდ-

ვას, რამაც შეიძლება გამოიწვიოს კრიპტოვალუტის კურსის დაცემა. ამის გამო ადამიანთა გარკვეული ჯგუფი მდიდრდება, გარკვეული კი ღარიბდება [44].

2025 წლის 24 მაისის მონაცემებით ბიტკოინის ფასმა მორიგი რეკორდი დაამყარა, რა დროსაც ერთი მონეტის ფასმა 111,861.97 დოლარიან ნიშნულს გადააჭარბა. ხოლო ბიტკოინის საბაზრო კაპიტალიზაციამ 2.2 ტრილიონ დოლარს გადააჭარბა. ამ მაჩვენებლით, ბიტკოინი მსოფლიოს ერთ-ერთი ყველაზე ძვირად ღირებული ფინანსური ინსტრუმენტია, რომელსაც მხოლოდ ფიზიკური ოქრო და Microsoft-ის, NVIDIA-ს და Apple-ის აქციები უსწრებს [45].

8.4. კრიპტოვალუტა ბიტკოინის ეკოსისტემა

ამ პარაგრაფის მიზანია კრიპტოვალუტის ეკოსისტემის არსებული მდგომარეობის შესწავლა და ანალიზი, კრიპტოვალუტის დადებითი მხარეების გამოვლენა, რომელთა განხორციელებამ უნდა უზრუნველყოს ფიატური ფულის ნაკლოვანებების აღმოფხვრა, ეკონომიკის გაციფროვნების მოთხოვნების რეალიზაცია და სხვ. კვლევის მიზნის განხორციელებისთვის აუცილებელია მსოფლიო მასშტაბით შესწავლილ იქნეს კრიპტოვალუტის მიმოქცევისთვის საჭირო ტექნიკური საშუალებები, ბირჟები და მოხდეს კრიპტოვალუტის რეგულირების არსებული მდგომარეობის ანალიზი.

კრიპტოვალუტის პრობლემებზე მრავალი ნაშრომია გამოქვეყნებული, როგორც უცხოელი, ასევე ქართველი მკვლევარების მიერ (ვ. პაპავა, დ. სიჭინავა, მ. მალრაძე გ. ტომარაძე, ნ. ჭყოიძე ე. ლეკაშვილი, ლ. მამალაძე და სხვ.). თუმცა პრობლემა კვლევის პროცესშია და საჭიროებს უფრო ღრმად შესწავლას.

ცნობილია, რომ ბიოლოგიური ეკოსისტემის გარემო ძირითადად ჩამოყალიბებული და შემოსაზღვრულია [46]. რაც შეეხება კრიპტოვალუტის ეკოსისტემას არ გააჩნია შემოსაზღვრული გარემო. ბიტკოინის ეკოსისტემა მისი ფუნქციონირების გარემოა, რომელიც გულისხმობს მის მოპოვებას, გამომუშავებას, ყიდ-

ვა-გაყიდვას, გადაცვლას, შენახვას და ამ პროცესებში ჩართულ ადამიანისეული რესურსების, ტექნიკური საშუალებებისა და ტექნოლოგიების ერთობლიობას.

ბიტკოინის ეკოსისტემა შეიძლება განვიხილოთ მაკრო და მიკრო დონეზე. მაგალითად, ბიტკოინის მაკროეკოსისტემად შეიძლება ჩავთვალოთ მთელი მსოფლიო, მიკროსისტემად კი ნებისმიერი სახელმწიფო, დარგი, ადამიანთა ჯგუფი და პიროვნება. ბიტკოინის ეკოსისტემა განიცდის ცვლილებას, რომელიც განპირობებულია არსებული ფინანსური ურთიერთობებით, ელექტრონული ბიზნესით, ელექტრონული კომერციით, ბიტკოინის პოპულარიზაციით, ბიტკოინის ეკოსისტემასთან დაკავშირებული პროცესების სრულყოფის აუცილებლობით და სხვ.

კრიპტოვალუტის ეკოსისტემის გაფართოების მიზნით აუცილებელ და გადაუდებელ სამუშაოა ციფრული ფულისა და ბლოკ-ჩეინტექნოლოგიის გამოყენების დადებითი მხარეების ადამიანთა ფართო მასებამდე დაყვანა, რათა გაიზარდოს მათი ნდობა ვირტუალური ვალუტისადმი.

სახელმწიფოს მხრიდან კრიპტოვალუტის აღიარება საყოველთაო საგადამხდელო საშუალებად [20]. გამოიწვევს და ხელს შეუწყობს არსებული ეროვნული ეკონომიკის ციფრულ ეკონომიკაზე გადასვლის პროცესის დაჩქარებას, ფიატური ვალუტის გამოშვებასა და მიმოქცევასთან დაკავშირებული ხარჯების მნიშვნელოვნად შემცირებას. გარდა აღნიშნულისა ვირტუალური ვალუტის შემოღება დააჩქარებს ბლოკ-ჩეინტექნოლოგიის სხვადასხვა სფეროში დანერგვის პროცესს, ახალი ინვესტიციების მოზიდვას, მეწარმეობის განვითარებას, სახელმწიფო ბიუჯეტის შემოსავლების გაზრდას, ინფორმაციულ ტექნოლოგიებთან დაკავშირებული ახალი სამუშაო ადგილების აღმოცენებას, სხვადასხვა ქვეყნების ვალუტების გადაცვლის დროის შემცირებას და მსოფლიო მასშტაბით ქვეყნის იმიჯის მნიშვნელოვან გაზრდას.

დღეისათვის კრიპტოვალუტის ბაზარზე გარდა ბიტკოინისა გამოჩნდა ათასობით კრიპტოვალუტა – ალტკოინი. თუმცა მათი უდიდესი ნაწილი არაა ფართოდ აღიარებული. ალტკოინები შეიქმნა იმ ნაკლოვანებების აღმოსაფხვრელად, რომლებიც გამოვლინდნენ ბიტკოინის მიმოქცევის პროცესში. ასევე, როგორც

ბიტკოინის ალტერნატივა და, ზოგიც კიდევ, კონკრეტულად ბლოკჩეინის ტექნოლოგიაზე დაფუძნებული რომელიმე სფეროში გამოსაყენებლად. მაგალითად, „დოგიკოინი“. იგი არის ალტკოინი, რომელიც გამოიყენება სპორტში, კულტურაში და ა.შ. სხვადასხვა ფონდების ორგანიზაციისთვის. დღითიდღე ფართოვდება კრიპტოვალუტის გამოყენების არეალი. მისი გამოყენება დაიწყო საქონლისა და მომსახურების ღირებულების ასანაზღაურებლად.

ბიტკოინის მომხმარებლებს აინტერესებთ როდის დადგება ბიტკოინის ბოლო მონეტის ემისიის თარიღი და იარსებებს თუ არა ამ თარიღის დადგომამდე ბიტკოინი. აღნიშნულ კითხვაზე ზუსტი პასუხის გაცემა შეუძლებელია. დასმული კითხვის პირველ ნაწილზე მკვლევარების შეხედულება თითქმის ერთგვაროვანია. ბოლო ბლოკი, რომელიც მოახდენს ბიტკოინის მონეტების გენერაციას იქნება ბლოკი ნომრით 62299999, რომლის მაინინგი მოხდება 2140 წელს [47] და ამ დროისთვის მოპოვებული ბიტკოინის მონეტების რაოდენობა სავარაუდოდ მიაღწევს – 20,999,999,9769 მონეტას.

კითხვის მეორე ნაწილზე პასუხის გასაცემად საჭიროა გავითვალისწინოთ შემდეგი: ბიტკოინების მოპოვების სირთულის გაზრდა (იგულისხმება პროგრამული მხარე), სოციალური მდგომარეობა, ბიტკოინის ეკონომიური დამოკიდებულება, ტექნოლოგიის განვითარება და სხვ. თუ მომავალში ევროკავშირში შემავალი ქვეყნები მოილაპარაკებენ ბიტკოინის აკრძალვის შესახებ, ხოლო აშშ მკვეთრად შეამცირებს ბიტკოინის მიმოქცევას, მაშინ ეს უკანასკნელი გამოიწვევს ბიტკოინის ფასის დაცემას, შესაბამისად, ბიტკოინის ბაზრის მონაწილეთა ინტერესის დაკარგვასაც ბიტკოინისადმი. აღნიშნულის გამო შესაძლებელია ბიტკოინის საბოლოო ემისიის დრო გაიწელოს და არ მოხდეს 2140 წელს. ან კიდევ, შესაძლებელია, დარჩენილი 118 წლის განმავლობაში გამოჩნდეს უფრო უკეთესი კრიპტოვალუტები ან მნიშვნელოვნად შეიცვალოს მისი მოპოვების ტექნოლოგია, ამით ბიტკოინის ემისიის საბოლოო დრო შესაძლებელია კიდევ უფრო გადაიწიოს.

ზემოაღნიშნულიდან, შეიძლება გავაკეთოთ დასკვნა, რომ ბიტკოინის ბოლო მონეტის ემისიის ზუსტი დროის განსაზღვრა შეუძლებელია.

ბიტკოინის ეკოსისტემის საფულები, ბირჟები და ეროვნული კრიპტოვალუტები. მარკეტში ან ბაზარში პროდუქტებით ვაჭრობა, ინტერნეტში მუშაობა, ტრანსპორტით სარგებლობა და ა.შ. საჭიროებს დღეისთვის არსებული სხვადასხვა სახის საფულებებიდან ერთ-ერთის გამოყენებას. ციფრული ეკონომიკის პირობებში ვირტუალური ვალუტის გამოყენება შეუძლებელია ელექტრონული საფულეს გარეშე. ამისათვის საჭიროა ელექტრონული საფულის გახსნა, რომელიც წარმოადგენს კომპიუტერულ პროგრამას და იძლევა ინტერნეტით (Online) ან ინტერნეტის გარეშე ოფლაინ (Offline) ანგარიშსწორების განხორციელების საშუალებას (Термин: Онлайн-оффлайн). იგი წარმოადგენს საბანკო ანგარიშის ანალოგს, რომელიც არ ექვემდებარება ბანკის მხრიდან კონტროლს, ასრულებს ტრადიციული საფულეს ყველა ფუნქციას და დამატებით გააჩნია ციფრული ვალუტის უნიკალური თვისებები.

ბიტკოინის ეკოსისტემის მნიშვნელოვან მდგენელს წარმოადგენს კრიპტოვალუტის ბირჟები, რომელთა რაოდენობა სწრაფად იზრდება. დღეისთვის მსოფლიოში რამდენიმე ასეული კრიპტობირჟა ფუნქციონირებს. მათ შორის ყველაზე საუკეთესოებია: Bybit, OKX, Binance, BingX, MEXC, KuCoin, HTX, Gate.io, Bitget, CoinEx და სხვ. [48].

კრიპტობირჟები იმით განსხვავდებიან ჩვეულებრივი ბირჟებისაგან, რომ მათი მართვა დეცენტრალიზებულია. ეს განსხვავება გამოიხატება იმაში, რომ სახელმწიფოს მხრიდან არ ხდება მათი რეგულირება. კრიპტოვალუტის ბირჟებისთვის დამახასიათებელია: დეცენტრალიზებული მართვა, მაღალი ვალანტილობა, განსაზღვრული სტატუსის უქონლობა და სხვ.

კრიპტოვალუტის პოპულარობამ მსოფლიოში ისეთ დონეს მიაღწია, რომ მრავალი ქვეყნის მთავრობამ გადაწყვიტა გამოუმუშავას საკუთარი კრიპტოვალუტა, რათა აიცილონ ფიატური ფულის დამზადებასა და მიმოქცევასთან დაკავშირებული დიდი ხარჯები, სხვა სახელმწიფოს ზემოქმედების შესაძლებლობა ფულად აქტივებზე (მათი „გაყინვა“ საზღვარგარეთის ქვეყნებში და ეკონომიკაში წარმოქმნილი პრობლემები). მრავალი სპეციალის-

ტის აზრით ეროვნული კრიპტოვალუტა ბევრ ქვეყანაში შეიძლება აღიარებულ იქნას საგადასახადო საშუალებად, რაზედაც მიუთითებს სხვადასხვა ქვეყნებში ონლაინ-მაღაზიებში და სერვისების გადასახდელად კრიპტოვალუტის გამოყენება. დღეისათვის შექმნილია ეროვნული კრიპტოვალუტების შემდეგი სახეობები: ქართული კრიპტოვალუტა – „ოქროს სანმისი“, ბელორუსული კრიპტოვალუტა „ტალერი“, ისლანდიის კრიპტოვალუტა – Auroracoin (AUR), ვენესუელას კრიპტოვალუტა – El Perto, იაპონიის კრიპტოვალუტა – I-Coin და სხვ.

მიუხედავად ზოგიერთი სახელმწიფოს მიერ გატარებული ღონისძიებებისა, შეაჩერონ ან აკრძალონ კრიპტოვალუტის მიმოქცევა, ადამიანები მაინც განაგრძობენ მათ გამოყენებას: მოიპოვებენ, ვაჭრობენ, ინახავენ და სხვ.

ვირტუალური ვალუტის მფლობელთა სერვისის გაუმჯობესების მიზნით იქმნება სხვადასხვა საშუალებები, მონეობილობები და პროგრამები. ერთ-ერთი ასეთი საშუალებაა ბანკომატი, რომლის მეშვეობით მომხმარებელს შეუძლია ნებისმიერ დროს განახორციელოს კრიპტოვალუტის შეტანა-გამოტანისა და გადაცვლის ოპერაციები.

ბოლო წლებში კრიპტოვალუტა საქართველოში სულ უფრო და უფრო პოპულარული ხდება. კრიპტო ვალუტის ახალი ტერმინალები დაყენებულია საქართველოს მრავალ ქალაქში. ამ ტერმინალის საშუალებით შესაძლებელია ბიტკოინების ყიდვა-გაყიდვა ლარებში.

კრიპტოვალუტების ბანკომატების დაყენება მიმდინარეობს მსოფლიოს მრავალ ქვეყანაში.

2022 წლის აგვისტოს მონაცემებით მსოფლიოს 77 ქვეყანაში ფუნქციონირებდა 39000-ზე მეტი კრიპტობანკომატი. ყველაზე მეტი კრიპტობანკომატი ფუნქციონირებს აშშ-ში – 34299, ანუ მსოფლიოში არსებული კრიპტობანკომატების 87%. ევროპაში დაყენებულია კრიპტობანკომატების საერთო რაოდენობის – 3,8%. კანადაში კი ორჯერ მეტი [49].

ჩვენი აზრით, აღნიშნული მონაცემებიდან გამომდინარე, მსოფლიო მასშტაბით ფუნქციონირებადი ბანკომატების რაოდენობა კატასტროფულად არასაკმარისია.

8.5. კრიპტოვალუტის რეგულირება მსოფლიოსა და საქართველოში

ფულად ურთიერთობათა მონესრიგების საკითხი ყოველთვის იყო და დღესაც კი კაცობრიობის ეკონომიკური განვითარების ერთ-ერთი აქტუალური პრობლემაა. დღეისათვის ნებისმიერ სახელმწიფოში ეკონომიკის წარმატებული განვითარება შეუძლებელია ციფრული ტექნოლოგიების დანერგვის გარეშე. შესაბამისად, დღის წესრიგში დგება ფულად ურთიერთობათა ელექტრონულად მონესრიგების საკითხი. ამიტომ წინამდებარე პარაგრაფი ეხება სწორედ ელექტრონული ფულის (კრიპტოვალუტის) დანერგვისა და მისი რეგულირების პრობლემებს.

კრიპტოვალუტა ელექტრონული ფულის (ვირტუალური ფულის) ნაირსახეობაა, რომლის აღმოცენება და გამოყენება განაპირობა ფულის უნაღდო ანგარიშსწორების განვითარების საჭიროებამ თანამედროვე ინფორმაციულ ტექნოლოგიებზე დაყრდნობით [12]. იგი ემყარება დაცვის კრიპტოლოგიურ მეთოდებს და ასრულებს ფულის ყველა ფუნქციას.

კრიპტოვალუტას, როგორც ელექტრონული ფულის თანამედროვე ნაირსახეობას, რომელთა უმრავლესობა აღმოცენებულია ბლოკჩეინ ტექნოლოგიის საფუძველზე, 10 წელიც კი არ დასჭირდა იმისათვის, რათა დანერგილიყო მსოფლიოს რამდენიმე ქვეყანაში. იგი შეიქმნა ინფორმაციის უსაფრთხოდ შენახვის, ტრანზაქციების დაჩქარების და შუამავალი რგოლებისაგან (ბანკები, ნოტარიუსები, სხვადასხვა საგადამხდელი სისტემები და სხვ.) გვერდის ავლისთვის. დღეისათვის მისი მართვა არ ხდება მსოფლიოს რომელიმე ერთი ცენტრალური ორგანოს ან კერძო სტრუქტურის მიერ და, ამდენად, ფუნქციონირებს დეცენტრალიზებულად [20].

კრიპტოვალუტის როლი მსოფლიოს ეკონომიკაში და ძირითადი გამოწვევები. კრიპტოვალუტები სულ უფრო მნიშვნელოვან როლს ასრულებენ გლობალურ ეკონომიკაში. ამის მაჩვენებელია კრიპტოვალუტების პოპულარობის სწრაფი ზრდა და შესამჩნევი გავლენა ფინანსურ ბაზრებზე. მათი დეცენტრალი-

ზებული ბუნება და მაღალი შემოსავლის მიღების პოტენციალი, რითაც ისინი ინტენსიურად იზიდავენ როგორც ინდივიდუალურ, ისე ინსტიტუციონალურ ინვესტორებს.

ამაზე მეტყველებს ის გარემოება, რომ კომპანია Crypto.com-ის 2024 წლის მონაცემების მიხედვით, კრიპტოვალუტების საერთო კაპიტალიზაციამ მსოფლიოში მიაღწია 3,9 ტრილიონ ამერიკულ დოლარს, რომელიც წინა წელთან შედარებით გაიზარდა 127%-ით [50].

კრიპტოვალუტა იძლევა ახალ შესაძლებლობებს საინვესტიციო პორტფელის დივერსიფიკაციისთვის და ემსახურება ჰეჯირების ინსტრუმენტს ინფლაციის წინააღმდეგ. მათი, როგორც ალტერნატიული ფინანსური ინსტრუმენტების გამოყენება აფართოებს ფინანსურ სერვისებზე წვდომის შესაძლებლობებს, განსაკუთრებით შეზღუდული საბანკო ინფრასტრუქტურის მქონე რეგიონებში. ამით კრიპტოვალუტები ხელს უწყობენ ფინანსური ინკლუზიის გაზრდას და ეკონომიკის განვითარების სტიმულირებას.

ამდენად, კრიპტოვალუტები კვლავაც ახდენენ მნიშვნელოვან გავლენას გლობალურ ეკონომიკაზე ფინანსური ბაზრების გარდაქმნისა და ინოვაციების გაძლიერების სახით. მათი მზარდი პოპულარობა და ინტეგრაცია ტრადიციულ ფინანსურ სისტემებში ხაზს უსვამს რეგულირების დაბალანსებული მიდგომის აუცილებლობას, რომელიც მხარს უჭერს ინოვაციებს და იცავს ფინანსურ სტაბილურობას.

კრიპტოვალუტების ძირითადი გამოწვევები. კრიპტოვალუტების გამოყენება, მიუხედავად მათი უპირატესობებისა, აწყდება ისეთ სერიოზულ გამოწვევებს, როგორიცაა: ფულის გათეთრება და ტერორიზმის დაფინანსება, კიბერდანაშაულები, ეკონომიკური არასტაბილურობა, ერთიანი რეგულირების არარსებობა და სხვ.

ფულის გათეთრება და ტერორიზმის დაფინანსება. კრიპტოვალუტების ანონიმურობა და დეცენტრალიზებული ბუნება მათ მიმზიდველს ხდის უკანონო ქმედებებისთვის. ტერორისტული ორგანიზაციები და კრიმინალური ჯგუფები სულ უფრო ხშირად იყენებენ ციფრულ ვალუტებს თავიანთი ოპერაციების დასაფი-

ნანსებლად ტრადიციული ფინანსური კონტროლის სისტემების გვერდის ავლით. კრიპტოვალუტების გამოყენება ფულის გასათეთრებლად და ტერორიზმის დასაფინანსებლად სერიოზულ საფრთხეს უქმნის საერთაშორისო უსაფრთხოებას.

კიბერდანაშაულები. კრიპტოვალუტების მზარდ პოპულარობას თან ახლავს მათი მოპარვისკენ მიმართული კიბერშეტევების რაოდენობის ზრდა. ჰაკერები იყენებენ მავნე პროგრამებს და ფიშინგშეტევებს მომხმარებლების კრიპტო საფულეზე წვდომის მისაღწევად. მკაფიო რეგულაციის არარსებობის შემთხვევაში, კრიპტოვალუტები ხშირად ხდება უკანონო ქმედებების სამიზნე. ეს ქმნის საჭიროებას შემუშავდეს საიმედო ზომები ციფრული აქტივების რეგულირებისა და დაცვის მიზნით, მათი გამოყენების ყველა ეტაპზე.

ეკონომიკური არასტაბილურობა. კრიპტოვალუტების ფასის მაღალმა ცვალებადობამ შეიძლება გამოიწვიოს ინვესტორების ფინანსური ზარალი და ფინანსური ბაზრების დესტაბილიზაცია. რეგულაციების არარსებობა უამრავ საფრთხეს უქმნის მოქალაქეებსა და სახელმწიფოებს, ვინაიდან, ჯერ ერთი, მათი გამოყენება შესაძლებელია გადასახადებისგან თავის არიდების მიზნით და, მეორეც, შავი ბაზრების ფუნქციონირების ზრდისათვის.

სხვადასხვა ქვეყანაში კრიპტოვალუტის რეგულირებისადმი განსხვავებულმა მიდგომებმა შეიძლება გამოიწვიოს რიგი სამართლებრივი გაუგებრობა, რაც ართულებს არაკანონიერი საქმიანობის ზრდისა და მომხმარებელთა უფლებების დაცვის შესაძლებლობებს.

ამ რისკების მინიმიზაციისთვის აუცილებელია კრიპტოვალუტების რეგულირების საერთაშორისო სტანდარტების შემუშავება და დანერგვა, რომლებიც უზრუნველყოფენ ბალანსს ინოვაციასა და უსაფრთხოებას შორის.

კრიპტოვალუტების რეგულირება მთავარ როლს თამაშობს ინვესტორების დაცვასა და უკანონო ქმედებების თავიდან აცილებაში. მკაფიო მარეგულირებელი ჩარჩოების არარსებობამ შეიძლება გამოიწვიოს თაღლითობა, ფულის გათეთრება და ტერორიზმის დაფინანსება. ამიტომ, სახელმწიფოები ცდილობენ შეიმუშაონ მარეგულირებელი ზომები, რომლებიც უზრუნველყო-

ფენ ბაზრის მონაწილეთა უსაფრთხოებას და ფინანსური სისტემების სტაბილურობას [51]. ამავდროულად, ზედმეტად მკაცრმა რეგულაციამ შეიძლება ჩაახშოს ინოვაცია ფინანსურ ტექნოლოგიებში. ამიტომ აუცილებელია ბალანსის პოვნა ტექნოლოგიური პროგრესის სტიმულირებასა და უსაფრთხოების უზრუნველყოფას შორის [52].

მნიშვნელოვანია ასევე საერთაშორისო დონეზე კრიპტოვალუტების რეგულაციების ჰარმონიზაცია. ეროვნულ მიდგომებში განსხვავებულობამ შეიძლება შექმნას არალეგალური საქმიანობის შესაძლებლობები და ძირი გამოუთხაროს უსაფრთხოების მცდელობებს. ამიტომ საერთაშორისო თანამშრომლობა ჰარმონიზებული მარეგულირებელი სტანდარტების შემუშავებაში სულ უფრო მნიშვნელოვანი ხდება [53].

ამრიგად, კრიპტოვალუტების ეფექტური რეგულირება აუცილებელია ინვესტორების დასაცავად, უკანონო ქმედებების თავიდან ასაცილებლად და ფინანსურ სექტორში ინოვაციების მხარდასაჭერად. ამიტომ მთავრობები აგრძელებენ ოპტიმალური მიდგომების ძიებას, რომლებიც ითვალისწინებენ როგორც რისკებს, ასევე შესაძლებლობებს, კრიპტოვალუტების გამოყენების ეფექტიანი განვითარებისათვის.

კრიპტოვალუტის რეგულირების არსებული მდგომარეობა მსოფლიოში. მთელ მსოფლიოში არსებობს კრიპტოვალუტის რეგულირებისადმი სხვადასხვა მიდგომა, რაც ასახავს შესაბამისი სუბიექტების ეკონომიკურ, პოლიტიკურ და კულტურულ მდგომარეობას. ზოგიერთი ქვეყანა ცდილობს ციფრული ვალუტების ინტეგრირებას თავის ფინანსურ სისტემებში, ზოგი კი მათ მკაცრ შეზღუდვებს ან პირდაპირ აკრძალვებს აწესებს [54].

მაგალითად, ჩინეთი ცნობილია კრიპტოვალუტებისადმი მკაცრი მიდგომით. 2021 წელს ქვეყანამ აკრძალა კრიპტოვალუტის მაინინგი და ვაჭრობა ფინანსური რისკების თავიდან ასაცილებლად და საკუთარი ცენტრალური ბანკის ციფრული ვალუტის, ციფრული იუანის მხარდასაჭერად [55].

ინდოეთი ასევე მკაცრ პოზიციას იკავებს კრიპტოვალუტების მიმართ. მიუხედავად იმისა, რომ ინდოეთის უზენაესმა სასამართლომ 2020 წელს გააუქმა კრიპტოვალუტის კომპანიების სა-

ბანკო სერვისების აკრძალვა, მთავრობა განიხილავს ახალი შეზღუდვების შემოღებას, მათ შორის კერძო კრიპტოვალუტების აკრძალვას, ფინანსური სტაბილურობის დასაცავად და უკანონო ქმედებების თავიდან ასაცილებლად [56].

ევროკავშირი და იაპონია, პირიქით, უფრო პროგრესულ მიდგომას იჩენენ მსგავსი რეგულირების მიმართ. ევროკავშირმა შეიმუშავა კრიპტოაქტივების ბაზრების რეგულაცია (MiCA), რომელიც მიზნად ისახავს შექმნას ერთიანი საკანონმდებლო ბაზა ციფრული ვალუტებისთვის და უზრუნველყოს ინვესტორების დაცვა [57].

იაპონიამ, კრიპტოვალუტები აღიარა გადახდის ლეგალურ საშუალებებად და დაადგინა მათი გამოყენების მკაფიო წესები, რაც ხელს უწყობს ქვეყანაში კრიპტო ინდუსტრიის განვითარებას [56].

ამრიგად, კრიპტოვალუტის მარეგულირებელი გლობალური ლანდშაფტი ხასიათდება მნიშვნელოვანი განსხვავებებით, რაც ასახავს თითოეული ქვეყნის უნიკალურ თავისებურებებსა და პრიორიტეტებს.

რეგულირების რეგიონალური თავისებურებები. შეერთებულ შტატებში კრიპტოვალუტის რეგულირებას ახორციელებს რამდენიმე ორგანო, მათ შორის ფასიანი ქაღალდებისა და ბირჟის კომისია (SEC) და სასაქონლო ფიუჩერსების სავაჭრო კომისია (CFTC). SEC ბევრ კრიპტოვალუტას ფასიან ქაღალდად მიიჩნევს, რაც მოითხოვს მათ რეგისტრაციას და სათანადო რეგულაციებთან შესაბამისობაში მოყვანას. მაგალითად, 2023 წელს, SEC-მა აღიარა 37 კრიპტოვალუტა ფასიან ქაღალდად, რამაც გამოიწვია მნიშვნელოვანი დისკუსიები ინდუსტრიაში [58].

ევროკავშირმა მიიღო კრიპტოაქტივების ბაზრის რეგლამენტის (MiCA), რომელიც ძალაში შევიდა 2024 წლის 30 დეკემბერს. კრიპტოაქტივების მიმოქცევისთვის, MiCA ევროკავშირის ფარგლებში ადგენს ერთიან წესებს, რაც მიზნად ისახავს ინვესტორების დაცვას და ფინანსური სტაბილურობის უზრუნველყოფას. რეგულაცია აწესებს მოთხოვნებს კრიპტოაქტივების ემიტენტებისა და მათთან დაკავშირებული სერვისის პროვაიდერებისთვის, რაც

ხელს უწყობს ევროკავშირის წევრ ქვეყნებში კანონმდებლობის ჰარმონიზაციას [59].

ძირითადი გამოწვევები და ტენდენციები. კრიპტოვალუტების რეგულირების გლობალური სტანდარტის არარსებობა მნიშვნელოვან გამოწვევებს უქმნის საერთაშორისო ფინანსურ ბაზარს. ეროვნულ მდგომარეობაში განსხვავებები იწვევს სამართლებრივ გაურკვევლობას და ხელს უშლის შესაძლებლობებს არბიტრაჟისთვის, რაც ართულებს მათზე ეფექტურ ზედამხედველობას და კონტროლს.

ზემოაღნიშნულიდან გამომდინარე მსოფლიოს არაერთმა ქვეყანამ შეზღუდა ან კიდევ პირდაპირ აკრძალა კრიპტოვალუტის გამოყენება. ასე, მაგალითად, 2024 წლის 6 მარტის მონაცემებით, მსოფლიოს 51 ქვეყანასა და რეგიონში აკრძალულ იქნა კრიპტოვალუტა. მათ შორის 9 ქვეყანამ მთლიანად აკრძალა კრიპტოვალუტის მოპოვება, შენახვა, ვაჭრობა და გამოყენება. მათ რიცხვს მიეკუთვნება: ალჟირი, ბანგლადეში, ჩინეთი, ეგვიპტე, ერაყი, მაროკო, ნეპალი, კატარი, ტუნისი და სხვ. გარდა აღნიშნულისა, 42 ქვეყანამ და რეგიონმა შემოიღო არაცხადი აკრძალვები, რომლებიც ბანკებსა და საფინანსო ორგანიზაციებს უკრძალავენ მიიღონ მონაწილეობა კრიპტოვალუტის ბიზნესში. ასევე ბირჟებს ეკრძალებათ იმუშაონ ქვეყნის საზღვრებში. ასეთი ქვეყნებისა და რეგიონების რიცხვში შედიან: ყაზახეთი, ტანზანია, კამერუნი, თურქეთი, ლიბანი, ცენტრალური აფრიკის რესპუბლიკა, კონგოს დემოკრატიული რესპუბლიკა, ინდონეზია, ბოლივია, ნიგერია და სხვ. ამ ქვეყნებსა და რეგიონებში კრიპტოვალუტის აკრძალვა მეტწილად განპირობებულია ისეთი მოსაზრებებით, როგორიცაა: ფინანსური სტაბილურობა, მონეტარული სუვერენიტეტი, ფულის გათეთრება, ტერორიზმთან ბრძოლა და სხვ. ზოგიერთ ქვეყანას ემინია, რომ კრიპტოვალუტამ შეიძლება გამოიწვიოს მათ კანონიერ ვალუტაზე ზენოლა და შექმნას სოციალური პრობლემები. ამიტომ ამ ქვეყნებმა გადაწყვიტეს აღმოფხვრან კრიპტოვალუტის უარყოფითი ზეგავლენები თავიანთ ქვეყნებში [60].

კრიპტოვალუტის რეგულირების არსებული მდგომარეობა საქართველოში. კრიპტოვალუტის მზარდი პოპულარობის მიუ-

ხედავად, საქართველოში არ არსებობს კრიპტოვალუტის რეგულირებისა და გამოყენების საკანონმდებლო ბაზა, რაც ქმნის როგორც კრიპტოვალუტის განვითარების, ისე ფინანსური დანაშაულების ჩადენის შესაძლებლობებს. ამიტომ აუცილებელია განვიხილოთ საქართველოში კრიპტოვალუტის ბაზრის დღევანდელი მდგომარეობა, მისი მახასიათებლები, უპირატესობები და გამოწვევები, რომელსაც აწყდება ქვეყანა მარეგულირებელი მექანიზმების არარსებობის გამო.

რეგულირების ბაზა. დღეისათვის საქართველოში კრიპტოვალუტები არაა აღიარებული საგადასახდლო საშუალებად, თუმცა მათი გამოყენება გაცვლასა და ინვესტირებაში არაა აკრძალული. ეს ქმნის ბაზრის მონაწილეებისთვის სამართლებრივ გაურკვევლობასა და პოტენციურ რისკებს.

კრიპტოვალუტის დაბეგვრის თვალსაზრისით საქართველო კრიპტოვალუტის მაინინგის კომპანიებს თავაზობს შეღავათიან პირობებს. კერძოდ, მაინინგიდან მიღებული შემოსავალი არ იბეგრება დამატებითი ღირებულების გადასახადით, რაც ქვეყანას ხდის მიმზიდველს მაინერებისთვის, თუმცა კრიპტოვალუტის ოპერაციებთან მიმართებაში მკაფიო წესების არ არსებობამ შეიძლება გამოიწვიოს გაურკვევლობა და საგადასახადო ორგანოებთან პოტენციური დავა.

როგორც აღვნიშნეთ, საქართველოში არ არსებობს სპეციალური მარეგულირებელი ორგანო, რომელიც განახორციელებს კრიპტოვალუტის ოპერაციებზე ზედამხედველობას. კრიპტოვალუტის ოპერაციებზე მონიტორინგისა და კონტროლის მექანიზმების არარსებობამ შეიძლება გამოიწვიოს ფულის გათეთრებასთან, ფინანსურ ტერორიზმთან და სხვა არაკანონიერ მოქმედებებთან დაკავშირებული რისკები.

მაინინგის კომპანიების საქმიანობა. საქართველო, მსოფლიოში ელექტროენერგიაზე დაბალი ფასებისა და ხელსაყრელი საგადასახადო პირობების გამო, გახდა კრიპტოვალუტის ერთერთი წამყვანი მაინინგ-ცენტრი, რომელიც იზიდავს როგორც მსხვილ კომპანიებს, ასევე ინდივიდუალურ მაინერებს [61].

მიუხედავად ამისა, აღნიშნულ სფეროში სათანადო რეგულირებისა და კონტროლის არარსებობა სერიოზულ გამოწვევებს

წარმოშობს საქართველოს ენერგეტიკული სისტემისა და ინფრასტრუქტურისთვის.

კრიპტოვალუტის მიღების მაჩვენებელი. ბოლო წლებში საქართველოს მოსახლეობაში კრიპტოვალუტების ათვისების მნიშვნელოვანი ზრდა დაფიქსირდა. შავი ზღვის საერთაშორისო უნივერსიტეტის Journal of Business-ში გამოქვეყნებული კვლევის მიხედვით, საქართველო ერთ-ერთი წამყვანი ქვეყანაა მსოფლიოში კრიპტოვალუტების გამოყენებაში, ხელსაყრელი საგადასახადო პოლიტიკისა და მაინინგის დაბალი ხარჯების გამო. მიუხედავად კრიპტოვალუტების მზარდი პოპულარობისა, გამონვევები კვლავ დაკავშირებულია საზოგადოების ნაკლებ ინფორმირებულობასა და ამ ტექნოლოგიებისადმი ნდობასთან. შავი ზღვის საერთაშორისო უნივერსიტეტის მიერ 2022 წელს ჩატარებულმა კვლევამ აჩვენა, რომ საქართველოს მოსახლეობა იცნობს კრიპტოვალუტის კონცეფციას, მაგრამ მათი ფუნქციონირებისა და მასთან დაკავშირებული რისკების გაგების დონე მაინც დაბალია, რაც ხაზს უსვამს ამ სფეროში საგანმანათლებლო ინიციატივების ზრდის საჭიროებას [62].

ქვეყანაში იზრდება იმ ბიზნესების რიცხვი, რომლებიც იღებენ კრიპტოვალუტებს, როგორც გადახდის საშუალებას. ExpatHub-ის ინფორმაციით, თბილისში და სხვა დიდ ქალაქებში იზრდება რესტორნების, კაფეების, სასტუმროებისა და მაღაზიების რაოდენობა, სადაც მომხმარებელს ციფრული ვალუტით გადახდა შეუძლია [63].

მიუხედავად იმისა, რომ დღემდე საქართველოში არ არსებობს კანონი კრიპტოვალუტის რეგულირების შესახებ, ეს სფერო მაინც არაა დატოვებული მთავრობისაგან უყურადღებოდ. ამ მხრივ აღსანიშნავია საქართველოს ფინანსთა მინისტრის მიერ 2019 წლის 28 ივნისს გამოცემული საჯარო გადაწყვეტილება #201, რომელიც აღნიშნული სფეროში ერთადერთი საკანონმდებლო აქტია. იგი სრულად განსაზღვრავს რა არის კრიპტოვალუტა და მასთან დაკავშირებული რეგულირების საკითხები.

საქართველოს კანონმდებლობა არ იძლევა კრიპტოვალუტის იურიდიულ განსაზღვრას. საქართველოს ფინანსთა სამინისტრო იზიარებს ვირტუალური ვალუტის ევროპის ცენტრალური ბან-

კის მიერ დადგენილ განსაზღვრას, რომელიც კრიპტოაქტივებს განმარტავს შემდეგნაირად „... ვირტუალური ვალუტა/-კრიპტო-ვალუტა – არის ღირებულების ციფრული გამოხატვა, რომელიც არაა გამოშვებული ცენტრალური ბანკის მიერ, არაა კრედიტი ან ემიტენტის ელექტრონული ფული, რომელიც ზოგიერთ შემთხვევაში შეიძლება გამოყენებულ იქნას, როგორც ფულის ალტერნატივა“ [64].

კრიპტოვალუტას არ გააჩნია ფიზიკური ფორმა, არ იმყოფება განსაზღვრულ ადგილას, არ ინახება ფინანსური დაწესებულების არცერთ ანგარიშზე და, როგორც წესი, შეუძლებელია მისი ემიტენტის იდენტიფიცირება. კრიპტოვალუტის მაინიგი იურიდიული პირისთვის იბეგრება მოგების გადასახადის 15%-ით, ხოლო დივიდენდზე 5%-იანი გადასახადით. საგადასახადო კოდექსის მიხედვით, კომპანიები, რომლებიც ეწევიან ნებადართულ სქმიანობას თავისუფალ ინდუსტრიულ ზონაში, თავისუფლდებიან დამატებითი ღირებულების გადასახადის, კორპორატიული გადასახადის და დივიდენდზე გადასახადისგან. თუ კრიპტომაინინგის კომპანიები ეწევიან თავისუფალ ინდუსტრიულ ზონაში კრიპოვალუტის მოპოვებას და არ გააჩნიათ „ნებადართული საქმიანობის“ სტატუსი, მაშინ ისინი იხდიან 15%-იან კორპორაციულ გადასახადს და 5%-იან გადასახადს დივიდენდზე [64].

კითხვები თვითშემოწმებისთვის

1. რა არის ელექტრონული ფული?
2. რა არის კრიპტოვალუტა?
3. ასრულებს თუ არა კრიპტოვალუტა ფულის ყველა ფუნქციას?
4. რომელია კრიპტოვალუტის უპირველესი და ძირითადი სახეობა?
5. ვინ არის ბიტკოინის შემქმნელი?
6. როდის შეიქმნა ბიტკოინი?
7. გაიცემა თუ არა ბიტკოინი რომელიმე ცენტრალური საფინანსო ინსტიტუტის ან ორგანიზაციის მიერ?

8. რომელია ბიტკოინის უმცირესი ერთეული და ბიტკოინის რა ნაწილია იგი?
9. რა არის მაინინგი?
10. კრიპტოვალუტის მოპოვების, ანუ მაინინგის (გამომუშავების) რომელი ხერხები არსებობს?
11. რა არის მაინინგ პული?
12. რა არის კაპტჩა?
13. რა არის ბლოკჩეინი და ბლოკჩეინტექნოლოგია?
14. რა არის ჰეში?
15. რა არის სტეიბლკოინი?
16. რომელია ციფრული ვალუტის სახეები?
17. რა არის ალტკოინი?
18. რას გულისხმობს მონეტების „დანვა“ და ვინ არიან „ვეშაპები“?
19. რა მონეობილობაა ASIC?
20. რას გულისხმობს ღრუბლოვანი მაინინგი?
21. კრიპტოვალუტის ეკოსისტემაში ტერმინები მოპოვება და გამომუშავება ერთი და იგივეა?

თავი 9. საერთაშორისო საფინანსო ტელესაკომუნიკაციო სისტემა S.W.I.F.T.

9.1. S.W.I.F.T.-ის შექმნის ისტორია

გასული საუკუნის სამოციან წლებში აშშ-ის და ევროპის მთელმა რიგმა ბანკებმა გადანყვიტეს, შეექმნათ ბანკთაშორისი სისტემა, რომელიც უზრუნველყოფდა ბანკებისა და საფინანსო ორგანიზაციების დაცვას არასანქცირებული შეღწევებისაგან და 24-საათიანი მუშაობის რეჟიმს. საბანკო სისტემა **S.W.I.F.T.**-ის შექმნის აუცილებლობა განაპირობა მრავალმა ფაქტორმა: საერთაშორისო ვაჭრობის მოცულობის ზრდამ; საბანკო ოპერაციების მოცულობის სწრაფად გადიდებამ; არსებული მეთოდებითა და ხერხებით (ფოსტა, ტელეგრაფი) შეუძლებელი გახდა განსაზღვრულ დროში დიდი მოცულობის მონაცემების დამუშავება; ადგილი ჰქონდა დიდი რაოდენობის შეცდომებს, შეცდომების გასწორება მოითხოვდა დიდ დროს; არ არსებობდა სტანდარტები საბანკო ინფორმაციის დამუშავებაში. შექმნილი სიტუაციიდან გამოსვლის მიზნით, 1960 წელს 60 ამერიკული ბანკი და ევროპული ბანკები შეიკრიბნენ და გადანყვიტეს, შეექმნათ საერთაშორისო საფინანსო ტელესაკომუნიკაციო სისტემა **S.W.I.F.T. (Society for World-wide Interbank Financial Telecommunication)**, რომელსაც უნდა დაეკმაყოფილებინა შემდეგი მოთხოვნები:

- საგადამხდელო ოპერაციების უქალაქოდ შესრულება;
- ახალი ტელესაკომუნიკაციო სისტემის გამოყენებით ბანკებს შორის ინფორმაციის გაცვლის დროის შემცირება;
- ტიპური საბანკო რისკების (ინფორმაციის დაკარგვა, შეცდომები, საგადამხდელო დავალებათა ფალსიფიკაცია) მინიმუმამდე დაყვანა;
- სისტემის რენტაბელობის მიზნით, ერთი შეტყობინების გადაცემის ღირებულება ტოლი უნდა ყოფილიყო 0,15 დოლარის, ხოლო სისტემის წარმადობა კი, არანაკლებ 100000 შეტყობინება დღე-ღამეში.

1973 წელს ევროპისა და სამხრეთ ამერიკის 250-მა ბანკმა დააარსა საერთაშორისო საფინანსო ტელესაკომუნიკაციო საზოგადოება **S.W.I.F.T.** [64].

შემდგომი ოთხი წლის განმავლობაში მიმდინარეობდა ორგანიზაციულ-ტექნიკური საკითხების გადაწყვეტა და 1977 წლის 9 მაისს მოხდა სისტემის ოფიციალური გახსნა. ჯერ კიდევ 1987 წელს, ანუ 10 წლისთავზე სისტემა დღეში ასრულებდა 1 მლნ. ბანკთაშორის ოპერაციას. დღეისთვის SWIFT-ში 215 ქვეყნიდან გაერთიანებულია 10500-მდე მსხვილი ბანკი. იგი ყოველდღიურად გადაცემს 1,8 მილიარდ შეტყობინებას.

S.W.I.F.T.-ის ქსელში გადაცემული შეტყობინებათა მოცულობა მუდმივად იზრდებოდა. ყოველდღიურად გადაცემული შეტყობინებათა მოცულობა თანხობრივად შეადგენდა 2 ტრილიონ ამერიკულ დოლარს. 2003 წლისთვის აღნიშნული სისტემით სარგებლობდა 198 ქვეყანა, სისტემის ნამდვილი წევრი იყო 2206, ასოცირებული წევრების რაოდენობა კი – 3057. მონაწილეთა რაოდენობა – 214, მომხმარებელთა საერთო რაოდენობა – 7407. **S.W.I.F.T.**-ში შეტყობინებების ტრაფიკის განაწილებამ 2003 წლის იანვრისთვის შეადგინა: გადახდებმა 60,7%, ოპერაციებმა ფასიან ქალაქებზე 30,5%, ფორექსულმა გარიგებებმა, და ფულადმა ბაზრებმა 6,15%, დოკუმენტურმა ოპერაციებმა 2,4%, სისტემურმა შეტყობინებებმა 0,4%.

დღეისათვის **S.W.I.F.T.**-ით სარგებლობს მსოფლიოს 200-ზე მეტი ქვეყანა, 7500 საფინანსო დაწესებულება.

S.W.I.F.T.-ი სააქციო საზოგადოებაა, რომლის მფლობელები არიან ბანკი-წევრები. დარეგისტრირებულია ბელგიაში (შტაბბინა და მთავარი მოქმედი ორგანოები განლაგებულია ქ. ლაუვლში, ბრიუსელთან ახლოს). საზოგადოება ფუნქციონირებს ბელგიის კანონების მიხედვით. უმაღლეს ორგანოს წარმოადგენს საერთო კრება. აქცია ერთი ხმაა. დირექტორთა საბჭოში უპირატესობა ენიჭება აშშ-ისა და ევროპის ქვეყნების წარმომადგენელ ბანკებს. აქციათა განაწილება წარმოებს გადასაცემ შეტყობინებათა ტრაფიკის პროპორციულად. აქციათა უმეტესი ნაწილის მფლობელები არიან: აშშ-ი, გერმანია, შვეიცარია, საფრანგეთი და დიდი ბრიტანეთი.

S.W.I.F.T.-ის წევრი შეიძლება გახდეს ნებისმიერი ბანკი, რომელსაც უფლება აქვს, ჩაატაროს საერთაშორისო საბანკო ოპერაციები. გარდა ძირითადი ბანკ-წევრებისა, სისტემით შეუძლიათ ისარგებლონ ორი კატეგორიის წევრებმა: ასოცირებულმა და მონაწილემ. პირველებს მიეკუთვნებიან აქციონერები, რომლებსაც არა აქვთ უფლება, მიიღონ მონაწილეობა სააქციო საზოგადოების მართვაში, გადაწყვეტილების მიღებაში (საბროკერო და სადილერო კანტორები, სადაზღვევო კომპანიები, საინვესტიციო კომპანიები).

სისტემის წევრად გახდომა მოიცავს მოსამზადებელ ეტაპს: ინერება განცხადება სისტემის წევრად მიღების შესახებ, ბანკმა უნდა შეასრულოს მოთხოვნები; განახორციელოს დროული ანგარიშსწორება, დააფიქსიროს სისტემასთან თანამშრომლობისათვის პასუხისმგებელი პირები. აღნიშნულის შემდეგ **S.W.I.F.T.**-ის დირექტორთა საბჭო განიხილავს შემოსულ განცხადებას და ბანკს აძლევს უფლებას, გადაიხადოს ერთჯერადი გადასახადი და მიიღოს ერთი აქცია, ერთი ხმის უფლებით. სისტემაში გაწევრიანება ძვირია. ერთჯერადი გადასახადია 400000 ბელგიური ფრანკი. 200000 ბელგიური ფრანკია დაწესებული ასოცირებული წევრობისათვის. ბანკმა, გარდა აღნიშნულისა, უნდა შეიძინოს ერთი აქცია ხმის უფლებით, რომლის ღირებულებაა 55 000 ბელგიური ფრანკი.

მეორე ეტაპზე ხდება ბანკის ფიზიკური ჩართვა სისტემაში. ამ ეტაპზე წყდება ყველა ტექნიკური საკითხი. კერძოდ, ტელესაკომუნიკაციო საშუალებების შეძენა, რაც საკმაოდ დიდ ხარჯებს მოითხოვს (რამდენიმე ათასი დოლარი). სისტემაში ჩართვის დრო წინასწარ არის დაფიქსირებული – მარტის, ივნისის, სექტემბრისა და დეკემბრის თვეების პირველი ორშაბათი. პრაქტიკამ დაამტკიცა, რომ სისტემის დანერგვაზე განეული დანახარჯების ამოღება წარმოებს 5 წელიწადში.

S.W.I.F.T.-ის უპირატესობა მდგომარეობს: ინფორმაციის დამუშავების ერთიან ტექნოლოგიაში, მონაცემების გადაცემის მაღალი სისწრაფესა და დამუშავების მაღალ საიმედოობაში, საოპერაციო დანახარჯების შემცირებაში.

S.W.I.F.T.-ით ერთი შეტყობინების გადაცემის დროის ხანგრძლივობაა 20 წუთი. დამატებითი ანაზღაურების შემთხვევაში შეტყობინების გადაცემის დრო შეიძლება შემცირდეს 1-დან 5 წუთამდე. **S.W.I.F.T.**-ის მთელი დღე-ღამის მუშაობის შემთხვევაში, გარიგებების 20% სრულდება ოპერატორის ჩარევის გარეშე. იგი ასრულებს შემდეგ პროცედურებს: კლიენტსა და ბანკს შორის სატელეგრაფო გზავნილები, ვალუტის გაცვლა, დებეტისა და კრედიტის დამოწმება, ანგარიშის გამოწერა და სხვა. შეტყობინება ბანკიდან ბანკში გადაეცემა ყველანაირი შემონმებით, რაც ხდება ავტომატურ რეჟიმში. თუ შეტყობინების გადამცემი და მიმღები ერთდროულად მუშაობენ ქსელში, მაშინ შეტყობინების გადაცემა ხდება 20 წამის ფარგლებში. სისტემის დაცვა არ დაუშვებს „შეცდომიანი“ შეტყობინების სისტემაში შეყვანას და ცვლილების შეტანას გადაცემის მომენტში. ყველა გადასაცემი შეტყობინება გადაგზავნის მომენტში იშიფრება. სისტემამ არ იცის გადასაგზავნი შეტყობინების შინაარსი, გარდა იმ ნაწილისა, რომელიც ინფორმაციის სწორად გადაცემის მიზნით მოიცავს: გადამცემისა და მიმღების იდენტიფიკატორებს, შეტყობინების ტიპსა და პრიორიტეტებს.

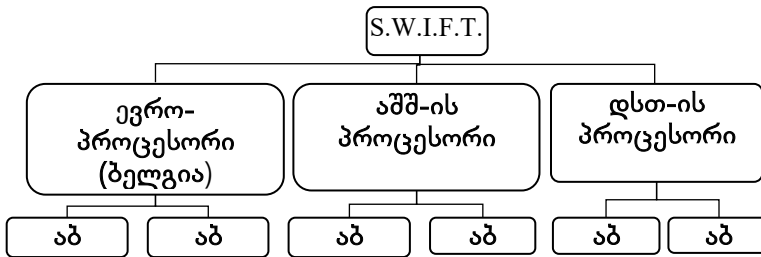
სისტემაში ყველა საგადამხდელო დოკუმენტი სტანდარტულია, რაც იძლევა მათი ავტომატიზებული დამუშავების შესაძლებლობას. სისტემაში სტანდარტულ შეტყობინებათა გამოყენება გამორიცხავს შეტყობინებათა არასწორ, ინტერპრეტაციას როგორც შეტყობინების მიმღების, ასევე გადამცემის მხრიდან. 130 ტიპის (ცხრილი 9.1.) შეტყობინების მაკეტი შედგება ორი სახის დანომრილი ველისაგან: აუცილებელი და არააუცილებელი ველები. აუცილებელი ველი შეიცავს ინფორმაციას მონაცემების სწორად დამუშავებისათვის. დამატებითი ინფორმაცია მოცემულია კოდებში. სისტემა შედგება: შეტყობინებათა გამწმენდისაგან (გამორიცხავს უზუსტობას); ტექსტის ანალიზატორისაგან (ბირთვი); შეტყობინებათა ინსპექტორისაგან და ფორმალიზატორისაგან.

ოპერაციულ ცენტრში მიღებული შეტყობინებები მოწმდება დოკუმენტის ფორმატის სისწორეზე, ვადაზე და გამგზავნ-მიმღების მისამართზე, აგრეთვე, მონყობილობათა სტატუსზე (შეტ-

ყობინებათა წყაროზე). დაშიფრული შეტყობინება გადაეცემა მოცემული ქვეყნის რეგიონულ პროცესორს, იქიდან კი – იქვე განლაგებულ ბანკ-მიმღებს. გადაცემის ოქმის შენახვის ვადა შეადგენს 14 დღეს.

S.W.I.F.T.-ი წარმოადგენს გლობალურ გამოთვლით სისტემას, რომელიც შედგება სხვადასხვა არხებით დაკავშირებული კომპიუტერული ცენტრებისაგან. **S.W.I.F.T.**-ის მართვა ხდება ოთხიდან ერთი კომპიუტერის საშუალებით. ეს ოთხი კომპიუტერი განლაგებულია: ორი ჰოლანდიაში და ორიც – აშშ-ში. აქედან სამი კომპიუტერი იმყოფება ე.წ. „ცხელ“ რეზერვში. **S.W.I.F.T.**-ის საერთო სტრუქტურა მოცემულია 9.1. სურათზე. სადაც აბრევიატურა „აბ“ არის ავტომატიზებული ბანკი. ეს ცენტრები ერთმანეთთან დაკავშირებულია რეგიონალური ჰოსტ-კომპიუტერებით, რომლებიც განლაგებულია ამ სისტემის წევრ ქვეყნებში. შეტყობინების გადაცემა ბანკ-გადამცემის მიერ ხდება მოდემის საშუალებით, სპეციალური არხების მეშვეობით ჰოსტ-კომპიუტერამდე. **S.W.I.F.T.**-ის რეგიონულ ცენტრში ხდება მიღებული შეტყობინების შემოწმება, შედარება სტანდარტთან, დაგროვება, გაშიფვრა და მითითებულ მისამართზე გაგზავნა. ყოველი შეტყობინება სტრუქტურულად მოიცავს: სათაურს, ტექსტს, დამონმებასა და დანართს. შეტყობინებათა ტექსტი მოიცავს ველებს, რომელთა ნაწილი წარმოადგენს სავალდებულოს. ზოგიერთი ველის კოდირება ხდება სხვადასხვა მეთოდით. ყველა ველი წინასწარ არის დანომრილი. სავალდებულო ველები მოიცავენ ინფორმაციას, რომელიც უზრუნველყოფს შეტყობინებათა სწორ დამუშავებას. დამატებითი ინფორმაცია განლაგებულია არასავალდებულო ველში.

ბანკთაშორისი ანგარიშსწორების სისტემა უზრუნველყოფს შემდეგი კატეგორიის საბანკო ოპერაციების შესრულებას: კლიენტის გადარიცხვები, საბანკო გადარიცხვები, სავალუტო ოპერაციები, დოკუმენტური ოპერაციები.



სურ.9.1 . S.W.I.F.T.-ის საერთო სტრუქტურა

S.W.I.F.T. ახორციელებს: კლიენტებისა და ბანკების სატელეგრაფო გზავნილების ადრესატებისათვის გადაცემას, გზავნილების მიღების შესახებ შეტყობინების მიღებას; ვალუტის გაცვლას; სესხებისა და ანაბრების შესახებ მოთხოვნებისა და შეტყობინებების მიღებას; გრძელვადიანი სესხებისა და ანაბრების მიღებას; პროცენტების გადახდას; დებეტისა და კრედიტის დადასტურებას; ანგარიშიდან ამონაწერის მიღებას. აღნიშნული შესაძლებლობას იძლევა, შემცირდეს ქალაქის დოკუმენტების გამოყენება და გადავიდეთ მონაცემების გაცვლის ელექტრონულ ფორმაზე.

დღეისათვის მიმდინარეობს სისტემის გადაყვანა **S.W.I.F.T.-2** მოდერნიზებულ სქემაზე. იგი აღჭურვილია ახალი მძლავრი პროცესორებით და შედგება პრობლემურ-ორიენტირებული და დამოუკიდებელი მოდულებისაგან. ინფორმაციის გადაცემის სიჩქარეა 9600 ბოდი წამში. ინფორმაციის შენახვის ვადა 14 დღიდან გაიზარდა ოთხ თვემდე. იგი იყენებს პროტოკოლ X.400-ს. **S.W.I.F.T.**-თან მიერთებული ბევრი მომხმარებელი ქმნის განანილებულ სისტემებს, დაფუძნებულს ისეთ ლოკალურ გამოთვლით ქსელებზე, როგორიცაა **Ethernet** და **TokenRing**. შემუშავებულია ბანკთაშორისი სისტემები, რომელთა დახმარებითაც დედამიწის ნებისმიერ წერტილში განლაგებული ბანკის ფილიალებს საშუალება აქვთ დაუკავშირდნენ **S.W.I.F.T.**-ს. ასეთ პროგრამულ კომ-

პლექსს მიეკუთვნება **MERVA**. აღნიშნული პროგრამული კომპლექსი დაყენებულია **S.W.I.F.T**-ის წევრი-ბანკების 15%-ში. თავდაპირველად **S.W.I.F.T**-ში მონაცემების გადასაცემად იყენებდნენ სატელეგრაფო და სატელეფონო ხაზებს. მოგვიანებით ინფორმაციის გადასაცემად გამოყენებულ იქნა ტელექსური კავშირი. დღეისათვის მიმდინარეობს სამუშაოები **S.W.I.F.T**-ში ფაქსი-მილური კავშირის გამოყენებისათვის. ბანკის სიდიდიდან გამომდინარე, შეტყობინების მიღება-გადაცემის მიზნით, იყენებენ ტერმინალურ კომპლექსებს – **ST200**, **ST400** და **ST500**.

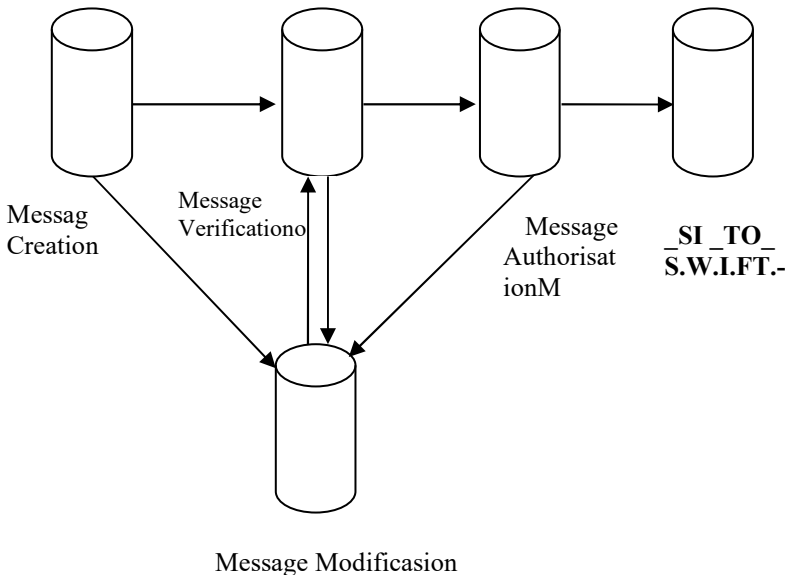
9.2. დაცვის მექანიზმი **S.W.I.F.T**-ში

S.W.I.F.T-ის გამოყენებისას დიდი მნიშვნელობა აქვს უსაფრთხოების საკითხებს [65]. ამიტომ **S.W.I.F.T** – **Alliance**-ის პროგრამაში გათვალისწინებულია ბანკის ლოკალურ ქსელში მუშაობის დაცვის სხვადასხვა ხერხები. მაგალითად, სერვერთან მუშაობა შეუძლიათ მხოლოდ **S.W.I.F.T**-**Alliance**-ის სერვერზე დარეგისტრირებულ მომხმარებლებს და მხოლოდ მითითებული ქსელის მისამართებიდან. თითოეულ მომხმარებელს სერვერთან ურთიერთობის დასამყარებლად უნდა ჰქონდეს თავისი სამომხმარებლო სახელი და პაროლი.

როდესაც მომხმარებელი მუშაობის დასაწყებად დაუკავშირდება **S.W.I.F.T**-**Alliance**-ის სერვერს, იგი ვალდებულია სისტემაში შეიყვანოს თავისი საიდენტიფიკაციო სახელი და პაროლი. თუ მომხმარებელმა 5-ჯერ არასწორად შეიტანა მონაცემები სისტემაში, მაშინ მისი ანგარიში **S.W.I.F.T**-**Alliance**-ის სერვერზე დაიბლოკება. მის გასახსნელად იგი ვალდებულია, მიმართოს **SWIFT**-**Alliance**-ის ადმინისტრატორს. **SWIFT**-ის ქსელამდე მისაღწევად შეტყობინებამ უნდა გაიაროს 3 საფეხური:

1. შეტყობინების შექმნა (Message Creation);
2. შეტყობინების შემოწმება (Message Verifikation);
3. შეტყობინების ავტორიზაცია (Message Autho-risation).

S.W.I.F.T.-ის მოთხოვნების თანახმად, ყოველი საფეხური შესრულებული უნდა იქნეს სხვადასხვა ოპერატორის მიერ. პირველ ოპერატორს უნდა შეეძლოს მხოლოდ შეტყობინების შექმნა და გადაგზავნა შესამოწმებლად. მეორეს უნდა ჰქონდეს ამ შეტყობინების შემოწმების პრივილეგია, რაც გულისხმობს იმას, რომ დადებითი პასუხის შემთხვევაში მას მიეცეს გადაგზავნის უფლება ავტორიზაციის მისაღებად. ხოლო შეცდომების აღმოჩენის შემთხვევაში უფლება მის გასასწორებლად. მესამე დონის ოპერატორს ევალება შემოწმებული შეტყობინების დათვალიერება და მისი გადაგზავნა **S.W.I.F.T.**-ის ქსელში. სქემატურად შეტყობინების შექმნის ამ პროცესს აქვს შემდეგი სახე (იხ. სურ. 9.2.).



სურ. 9.2. შეტყობინების ფორმირების სქემა

როგორც სურათი 9.2.-დან ჩანს, შეტყობინებამ **S.W.I.F.T.**-მდე მისაღწევად უნდა გაიაროს 3 საფეხური. ამასთან, ნებისმიერი

საფეხურიდან შესაძლებელია მისი დაბრუნება შესასწორებლად **Message Modification**-ის პროგრამაში, ხოლო შესწორების შემდეგ მას შეუძლია მხოლოდ შემონმების საფეხურზე დაბრუნება.

გარდა **S.W.I.F.T.-Alliance**-ის პროგრამის დაცვის საფეხურებისა, **S.W.I.F.T.**-ის ქსელში ჩართვისა და შეტყობინების გაგზავნისათვის ბანკის სისტემა **S.W.I.F.T.**-ის ქსელში თვითონაც გადის რეგისტრაციის რამდენიმე საფეხურს. ფინანსური შეტყობინების გაგზავნისათვის ის ვალდებულია, გაცვალოს გასაღებები თავის კორესპონდენტ ბანკთან და გამოიყენოს ეს გასაღები შეტყობინების ხელმოწერისათვის.

როგორც აღვნიშნეთ, შეტყობინებამ, **S.W.I.F.T.**-ის მოთხოვნით, უნდა გაიაროს 3 საფეხური. მისათვის საჭიროა **S.W.I.F.T.-Alliance** სისტემაში სამი მომხმარებლის რეგისტრაცია. თუ გარკვეული პირობების გამო ეს არ ხერხდება, მაშინ შესაძლებელია ერთი მომხმარებლისათვის რამდენიმე პრივილეგიის მინიჭება, ანუ მას შეეძლება შეტყობინების შექმნაც, შემონმებაც და ავტორიზაციაც. ცხადია, ასეთი მომხმარებლის შექმნა არ არის მიზანშეწონილი. ვინაიდან იზრდება შეცდომების დაშვების ალბათობა. მას შემდეგ, რაც შეტყობინებამ გაიარა შემონმების ყველა საფეხური და მოთავსდა **S.W.I.F.T.**-ის გასაგზავნ შეტყობინებათა სიაში, საჭირო ხდება **S.W.I.F.T.**-ის ქსელში ჩართვა და ამ შეტყობინების გაგზავნა ადრესატისათვის.

S.W.I.F.T.-ს შეუძლია განახორციელოს: კლიენტებისა და ბანკების სატელეგრაფო გზავნილების გადაცემა, ვალუტის გაცვლა, გზავნილის მიღების შესახებ შეტყობინების გადაცემა, გრძელვადიანი სესხებისა და ანაბრების, პროცენტების გადახდის, შეკითხვებისა და შეტყობინებების ოპერაციების დამუშავება სესხისა და ანაბრების შესახებ.

S.W.I.F.T.-ში გამოიყენება სტრუქტურული ფინანსური შეტყობინებები, რომელთა საფუძველზეც შესაძლებელია ყველა საბანკო და ფინანსური ოპერაციის განხორციელება. სტანდარტული შეტყობინების ფორმები ისეა შემუშავებული, რომ არ იყოს დამოკიდებული ცალკეული ქვეყნის ნაციონალური ბანკების სფეროს თავისებურებებზე. სტანდარტულ ფორმატში ინფორმაციის გა-

დაცემა საშუალებას იძლევა მოხდეს მონაცემების ავტომატიზებული დამუშავება და გამოირიცხოს შეტყობინების სხვადასხვანაირად გაგება. ფორმატების უნიფიცირება მნიშვნელოვნად აიოლებს გაგზავნილი შეტყობინების კორექტულობის კონტროლს, რაც უზრუნველყოფს სწორად ფორმულირებული შეტყობინებების, შემთხვევითი შეცდომებისაგან დაცვას და სისტემის გამტარუნარიანობას ამაღლებს.

ორგანიზაციული, ფიზიკური და ტექნიკური მეთოდების კომბინაცია უზრუნველყოფს გადაცემული ინფორმაციის დაცვას და გასაიდუმლოებას. კაეშირის ყველა არხი მუშაობს დაშიფრულ ინფორმაციასთან და ტელესაკომუნიკაციო მოწყობილობებთან. წვდომა მკაცრად შეზღუდულია. შეტყობინებების შეგროვებისას დაცულია აგრეთვე გადასაცემი შეტყობინება შესაძლო დაკარგვისაგან, რადგან ინფორმაციის დამუშავების ცენტრებში ინახება გადაცემული ინფორმაციის ასლები და ცალკეული შეტყობინების მიღების ფაქტი დასტურდება ინდივიდუალურად. რაიმე ეჭვის გაჩენის შემთხვევაში შეტყობინების გამგზავნის შეუძლია მოითხოვოს გაგზავნილი შეტყობინების ასლი.

გადაცემული შეტყობინების ღირებულება დამოკიდებული არ არის გადაცემის მანძილზე. თუ შეტყობინება ერთი დღე-ღამის განმავლობაში არ გადაიცემა ადრესატს **S.W.I.F.T**-ის მიზეზით, მაშინ იგი თავის თავზე ღებულობს პასუხისმგებლობას პირდაპირი და ირიბი დანაკარგების ანაზღაურების შესახებ.

9.3. **S.W.I.F.T**-ის სტანდარტი

სისტემაში შეტყობინებების გაცვლა წარმოებს შემუშავებული სტანდარტის მიხედვით. სისტემაში ძირითადად გამოყენებულია მსოფლიოში მიღებული **ISO** და **ICC** სტანდარტები. **S.W.I.F.T**-სთვის შემუშავებულია ტექსტური შეტყობინებისთვის სტანდარტი. ეს სტანდარტები აღიარებულია სტანდარტების საერთაშორისო ორგანიზაციის მიერ. ყველა ტიპის შეტყობინება აგებულია საერთო პრინციპების მიხედვით და შედგება: საწყისი ნაწილისაგან, რომელიც მოიცავს შეტყობინების დასაწყისის ჭდეს, სათაურს და ტექსტის დაწყების ჭდეს; შეტყობინების

ტექსტს; შეტყობინების დასასრულს, რომელიც თავის მხრივ მოიცავს: ტექსტის დასასრულის ჭდეს, პარამეტრებს და შეტყობინების დასასრულის ჭდეს. დასაწყისი და დამთავრება ქმნის „კონვერტს“, რომელშიაც გადაიგზავნება შეტყობინება და რომელიც მოიცავს ქსელში შეტყობინების სამართავ ინფორმაციას. სათაური მოიცავს შეტყობინების მიმღების კოდიდენტიფიკატორს (**BIC**)¹, და გამგზავნის ტერმინალის კოდს, რომელიც ხუთნიშნაა და ასრულებს საკონტროლო და დაცვის ფუნქციას - შეტყობინების სამნიშნა კოდი და პრინტერის ორნიშნა კოდი. პარამეტრებში ნაჩვენებია იდენტიფიკაციის კოდი და სხვა შეტყობინებები, მაგალითად, შეტყობინება ბანკ-მიმღებისთვის შეტყობინების გადაცემის დაყოვნების შესახებ. შეტყობინების სწორად მიწოდების მიზნით, **S.W.I.F.T**-ის ყველა მომხმარებელი მომარაგებულია **BIC**-ის კოდებით, რომლებიც წარმოადგენენ მათ მისამართებს ქსელში. კოდები ქვეყნდება რეგულარულად სპეციალურ ცნობარებში, დაბეჭდილი ან ელექტრონული ფორმით. მისამართი (**BIC**) შედგება რვა ან თერთმეტი თანრიგისგან, გამომდინარე იქიდან, გააჩნია თუ არა კოდს განყოფილება. **ISO** შეტყობინებაში გამოყენებული ყველა შეტყობინება უნდა დარეგისტრირდეს. **BIC**-კოდს გააჩნია შემდეგი სტრუქტურა: 1.4 – სიმბოლო – არის საფინანსო ორგანიზაციის უნიკალური კოდი; 2.2 – სიმბოლო – **ISO**-ს სტანდარტების შესაბამისად, ქვეყნის კოდი; 4.2 - სიმბოლო – ქვეყნის შიგნით საფინანსო ორგანიზაციის ადგილმდებარეობის კოდი; 5.3 სიმბოლო – განყოფილების კოდი.

შეტყობინების ტექსტი შედგება ველებისგან და აღინიშნება ორნიშნა ციფრული კოდით. შეტყობინების ტექსტში ინფორმაციის შეტანა წარმოებს მკაცრი თანმიმდევრობის დაცვით, თანაც ზოგიერთი ველის შევსება სავალდებულოა, ზოგიერთის არა, შეიძლება მათი გამოტოვება ან შევსება.

დღეისათვის გამოყენებულია 11 კატეგორია და შეტყობინების 130 ტიპი. იგი აგებულია ისეთი სახით, რომ მაქსიმალური სიზუსტით შესრულდეს ფინანსური ოპერაციები.

¹ SWIFT/BIC - არის 8 ან 11 თანრიგიანი კოდი, რომელიც მიუთითებს ქვეყანას, ქალაქს, ფილიალს..

შეტყობინება არის სისტემური და ფინანსური. სისტემური შეტყობინება გამოიყენება მონაცემთა ბაზაში შეტყობინების მოსაძებნად, განსაზღვრული მოქმედებების შესასრულებლად, სასწავლოდ და სავარჯიშოდ, ანგარიშგებების მისაღებად.

არსებობს სამი ძირითადი სისტემური ტიპის შეტყობინება:

1. **LOGIN/OUT** – სისტემაში შესვლის (გამოსვლის სისტემური შეტყობინება);

2. **RETRIEVAL** – ამ მოთხოვნის მიხედვით, სისტემა გზავნის შენახული შეტყობინების ასლს;

3. **REPORTS** – იძლევა საშუალებას მივიღოთ სხვადასხვა ანგარიშგებები.

სისტემურ შეტყობინებას გააჩნია ყველაზე მაღალი პრიორიტეტი, რამდენადაც იგი შეიცავს ინფორმაციას ქსელის ფუნქციონირების შესახებ, და გააჩნია 0 კატეგორია. ფინანსური შეტყობინებები იყოფა კატეგორიებად:

1. კლიენტის გზავნილები და ჩეკები.

2. ფინანსური ორგანიზაციების გზავნილები.

3. ფინანსური გარიგებები. ინკასო და განკარგულებები ნაღდი ფულით ანაზღაურებაზე.

4. ფასიანი ქაღალდები.

5. ძვირფასი ლითონები და კონსორციუმები.

6. დოკუმენტური აკრედიტივები და გარანტიები.

7. სამგზავრო ჩეკები.

საბალანსო ანგარიშსწორება, ნაშთის შეცვლა, „ნოსტრო“ და საცნობარო ანგარიშები და სხვ.

ამ კატეგორიების ყველა შეტყობინებას ენიჭება სამნიშნა ციფრული კოდი, რომლებიც განსაზღვრავს შეტყობინების სახეს, პირველი ციფრი შეესაბამება ოპერაციის კატეგორიას, ორი ნიშანი კი – შეტყობინების ტიპს. მაგალითად, კლიენტის გზავნილი აღინიშნება კოდით – 100, ბანკის საშუალებების გზავნილი კი კოდით – 200 და ა. შ. ფინანსური შეტყობინებების აღწერა მოცემულია ცხრილში 9.1.

ფინანსური შეტყობინებების აღწერა

კატ- ეგორია	შეტყობი- ნებათა ჯგუფი	აღწერა
1	0	კლიენტის გზავნილები
	1	ოპერაციები ჩეკებზე
2	0	საფინანსო ორგანიზაციების გზავნილები
	1	შეტყობინება გზავნილის მიღების შესახებ
3	0	სავალუტო დილინგი და სავალუტო ოპციონები
	2	ფიქსირებული განაკვეთებით საკრედიტო- სადეპოზიტო ოპერაციები
	3	სესხები, სასწრაფო დეპოზიტები და დეპოზიტები მოთხოვნამდე
	4	საპროცენტო განაკვეთებზე ფორვარდული შეთანხმებები
	5	კრედიტებისა და დეპოზიტების მიხედვით პროცენტების გადახდა
	6	ფასიანი ქაღალდების გაცვლითი ოპერაციები
4	0	შეტყობინებები გადახდების შესახებ
	1	შეტყობინებები
	2	მოთხოვნები გადახდების მიმდინარეობის შესახებ
	3	შესწორებები
	5	განკარგულებები ნაღდი ფულით გადახდის შესახებ
5	0	მოთხოვნები
	1	შეტყობინებები და მოთხოვნების დადასტურებები და გარიგებები
	2	ფასიანი ქაღალდების მიხედვით კრედიტების და ფასიანი ქაღალდების გადაცემისა და მიღების შესახებ ინსტრუქციები
	3	დამოწმება მიღებისა და გადაცემის შესახებ
	5	კორპორაციის სარჩელები, შეტყობინებები და პრეტენზიები

	6	კორპორაციების გაყიდვები ფასდაკლებით
	7	ბალანსები და პორტფელის მართვა
	8	სპეციალური ინსტრუქციები
6	0	ძვირფასი ლითონები
	1	სინდიკატები და კონსორციუმები
7	0	დოკუმენტური აკრედიტივის გაცემა, შესწორება, წინასწარი შეტყობინება
	1	მესამე ბანკის აკრედიტივების დოკუმენტების შესახებ შეტყობინება
	2	დოკუმენტური აკრედიტივის გადაცემა
	3	დამოწმება და შეტყობინება
	4	დაფარვები
	5	შეტყობინებები და სანქციები
	6	გარანტიები
8	0	გაყიდვები და ანგარიშსწორებები
	1	ხარჯების ანაზღაურება
	2	მარაგების მართვა
9	0	სადებეტო დადასტურება
	1	საკრედიტო დადასტურება
	2	მოთხოვნები საბალანსო ანგარიშებზე
	3	შეტყობინება განაკვეთების ცვლილებაზე
	4	კლიენტის ბალანსისა და ანგარიშების მიხედვით ამონაწერები
	5	„ნოსტროს“ ანგარიშების მიხედვით ამონაწერები
	7	„ნეტროს“ ანგარიშების მიხედვით ამონაწერები
	8	მოთხოვნები ფინანსური მდგომარეობის შესახებ
	9	დანახარჯები, პროცენტები, გასაღები და შემოსულობები, გაუქმებული მოთხოვნები. შეკითხვები და პასუხები, შეტყობინებები თავისუფალი ფორმატების შესახებ

წყარო: Банковские информационные системы: Учебник Под редакцией профессора В. В. Дика. М: Маркет ДС, 2006. გვ. 745, 746.

პირველი კატეგორიის შეტყობინებები დაკავშირებულია გადახდებთან ან მათ შესახებ ინფორმაციასთან, როცა დამკვეთი ან ბენეფიციარი, ან ორივე ერთად, არ წარმოადგენს საფინანსო ორგანიზაციას.

მე-2 კატეგორიის შეტყობინებებს მიეკუთვნება ის შეტყობინებები, რომლებსაც ერთმანეთში ცვლიან საფინანსო ორგანიზაციები. მათ მიეკუთვნება ფულადი საშუალებების მოძრაობის შესახებ მოთხოვნების შემცველი გადარიცხვები, რომელსაც საფინანსო ორგანიზაციები ღებულობენ თავიანთი ან სხვა საფინანსო ორგანიზაციების სასარგებლოდ; აგრეთვე, შეტყობინებები მომავალ ვალდებულებებზე, რომელიც საფინანსო ორგანიზაციებს ატყობინებს იმ თანხის შესახებ, რომელიც უნდა ჩაირიცხოს გამგზავნის ანგარიშზე.

მე-3 კატეგორიის შეტყობინებები არის მტკიცება, რომელიც უკვე ცნობილია ორივე მხარისთვის, შეტყობინება გარიგებებისა და რეგულირების თანხმობის შესახებ. მათ მიეკუთვნება ინფორმაცია სავალუტო-გაცვლითი კონტრაქტების შესახებ, შეთანხმებები ვადამდე საპროცენტო განაკვეთების შესახებ და ფულადი საშუალებების დაბანდება სესხის ოპერაციების მიხედვით.

მე-4 შეტყობინებები, რომელიც მიეკუთვნება მეოთხე კატეგორიას, არ ითვალისწინებს ერთიანი წესების დაცვას, რომელიც დადგენილია ინკასოს გადახდებით, თუმცა ინკასოს გადახდები სხვადასხვა ვალუტის საფუძველზე არცერთი შეტყობინებით არ არის გათვალისწინებული.

მე-5 კატეგორიის შეტყობინებები შეიცავს ფასიანი ქაღალდების გაყიდვებისა და ანაზღაურების შესახებ ინსტრუქციებს და შესაბამის დამოწმებებს, ინფორმაციას ერთობლივი მოქმედებების შესახებ, შეტყობინებებს კაპიტალისა და მოგების შესახებ, ანგარიშგებებს, ფასიანი ქაღალდების პორტფელისა და დაკრედიტების რეგულირების შესახებ ინფორმაციას.

მე-6 კატეგორიის შეტყობინებები ისეთი ინფორმაციის შემცველია, რომელიც უშუალოდ მიეკუთვნება ძვირფასი ლითონების მიხედვით შესრულებულ ოპერაციებს (სავაჭრო დამოწმება, გარიგებების მიხედვით შეტყობინებები და ინსტრუქციები). აგრეთვე, სხვადასხვა სახის შეტყობინებები, რომელიც მოიცავს

ინფორმაციას სესხების, ინსტრუქციების და ანგარიშგებების, დაკრედიტების ოპერაციების და გარანტიების შესახებ.

შეტყობინებები, რომლებიც ეკუთვნის მე-7 კატეგორიას, შეიცავს ინფორმაციას სესხების გამოშვების, ინსტრუქციებისა და ანგარიშგებების შესახებ, დაკავშირებულს საკრედიტო ოპერაციებთან და წარმოდგენილ გარანტიებთან. ამ კატეგორიის შეტყობინებებზე არ ვრცელდება მკაცრი შეზღუდვა ინგლისური ენის აუცილებლად გამოყენების თაობაზე.

მე-8 კატეგორიის შეტყობინებებში ასახულია ინფორმაცია ჩეკების გაყიდვისა და ანაზღაურების შესახებ, აგრეთვე შეტყობინებები, რომელთა გაცვლაც წარმოებს ჩეკების ემიტენტების და ფულადი გზავნილების გამგზავნებს შორის.

მე-9 კატეგორიის შეტყობინებებში მოცემულია ინფორმაცია საბალანსო ანგარიშგებებზე, (ინფორმაცია ფულადი ოპერაციების რეგულირების, დაწვრილებითი ინფორმაცია ბალანსისა და ოპერაციების შესახებ), შეკითხვები კლიენტებისა და ორგანიზაციების შესახებ. საერთო შეტყობინების კოდი ასეთია – „n 0M“.

სადაც n-ის შეცვლა წარმოებს იმ კატეგორიის ნომრით, რომლის შინაარსიც მაქსიმალურად შეესაბამება შეტყობინების მიზანს; 0 – მიუთითებს თითოეულ კატეგორიაში შეტყობინების განსაკუთრებულ თვისებას; M – განსაზღვრავს შეტყობინების კონკრეტულ ტიპს (მაგალითად, 0 – შეტყობინება, 2 – მოთხოვნის გაუქმება, 5 – მოთხოვნები).

შეტყობინების ფორმირებისას დაცული უნდა იყოს შემდეგი წესი:

- შეტყობინების ცალკეული ტიპის ფორმატი უნდა განსაზღვრავდეს ცვალებადი და მუდმივი სიგრძის ველების რაოდენობას;
- ველები შეიძლება იყოს როგორც აუცილებელი, ისე არა-აუცილებელი;
- ველი, რომელიც განსაზღვრული არ არის კონკრეტული ტიპის შეტყობინებით ფორმატის აღწერაში, არ უნდა იქნეს გამოყენებული;

- ველი შეიძლება გამოყენებულ იქნეს ერთხელ, თუ მითითებული არ არის მისი განმეორება;
- ველები უნდა იყოს გამოყოფილი უნიკალური გამყოფებით.

კითხვები თვითშემოწმებისთვის

1. რამ განაპირობა **S.W.I.F.T**-ის შექმნა?
2. როგორ ხდება **S.W.I.F.T**-ში შეტყობინების ფორმირება?
3. როგორია **S.W.I.F.T**-ის სტრუქტურა?
4. როგორ წარმოებს ინფორმაციის დაცვა **S.W.I.F.T**-ში?
5. როგორი სტრუქტურისაა **S.W.I.F.T**-ის შეტყობინების სტანდარტი?
6. რამდენი კატეგორიის და ტიპისაა ფინანსური შეტყობინებები? დაახასიათეთ ისინი.

თავი 10. ზანკის საინფორმაციო სისტემების შეძენისა და ამორჩავის კრიტერიუმები

10.1. საინფორმაციო სისტემების ფლობის მთლიანი ღირებულება

საინფორმაციო სისტემის (სს) გამოყენება არ შემოიფარ-
გლება მხოლოდ მის შეძენაზე განეული ხარჯებით. სს ექსპლუა-
ტაციის პერიოდში საჭიროებს გარკვეულ დანახარჯებს, რომე-
ლიც აისახება სს-ის ფლობის მთლიან ღირებულებაში (**TCO-Total
cost of Ownership**) მისი სიცოცხლის ციკლის ყველა ეტაპზე. ამ
მოდელის საფუძველზე შეიძლება გამოვთვალოთ სს-ის ეფექტუ-
რობის ეკონომიკური კრიტერიუმი საინფორმაციო სისტემის
ფლობის მთლიანი ღირებულება.

$$C_{TCO} = \sum_{k=1}^n C_k$$

სადაც C_k არის დანახარჯები სს-ის სიცოცხლის ციკლის სხვადა-
სხვა ეტაპზე. თითოეული დანახარჯის ოდენობა საერთო დანახა-
რჯებში სხვადასხვაა. საწარმოსათვის დანახარჯების ყველა
კომპონენტს არ გააჩნია თანაბარი მნიშვნელობა. აღნიშნულიდან
გამომდინარე, ანგარიშობენ სს-ის ფლობის შეწონილ მთლიან ღი-
რებულებას – $C_{TCO_{\text{შეწ}}}$.

$$C_{TCO_{\text{შეწ}}} = \sum_{k=1}^n A_k(t) C_k(t)$$

სადაც A_k არის შეწონის კოეფიციენტი, რომელიც გამოხატავს
შემოთავაზებული მოდელის მიხედვით K -ური დანახარჯების
მნიშვნელობას. სს-ის სიცოცხლის ციკლის ეტაპებია:

- დაპროექტების;
- შექმნის;
- გამოცდის;
- დანერგვის;

- ათვისების;
- თანხლების;
- მხარდაჭერის;
- მომსახურების;
- ლიკვიდაციის.

TCO-ს მოდელი, პირველ რიგში, საშუალებას იძლევა, ყველა კომპონენტის მიხედვით დავიანგარიშოთ რეალური დანახარჯები.

10.2. ინფორმატიზაციის პროექტების რეალიზაციის ვარიანტების საერთო ანალიზი

ბანკში სს-ის შექმნისას, მიუხედავად იმისა, როგორი ფორმით მოხდება მისი რეალიზაცია (საკუთარი ძალებით თუ გარე ორგანიზაციის მიერ), მონაწილეობა უნდა მიიღოს უშუალოდ მომხმარებელმა. ასეთი მონაწილეობა საშუალებას იძლევა, გათვალისწინებულ იქნას ინფორმატიზაციის შესაძლო შედეგები როგორც ცალკეული სამუშაო ადგილებისათვის, ასევე მთლიანად ბანკის ორგანიზაციულ სტრუქტურაში (არსებული კადრების კვალიფიკაციის შეცვლა, ინფორმაციის დეცენტრალიზებული ან ცენტრალიზებული მეთოდით მონაცემების დამუშავების შეცვლა). საინფორმაციო სისტემის შექმნა და განვითარება მეცნიერება ტევადი სფეროა, რომლის წარმატებული საქმიანობა საჭიროებს შემდეგ შესაბამის პოტენციალს: შესაბამისი კვალიფიკაციის პერსონალს, მსგავსი საინფორმაციო სისტემების შექმნის გამოცდილებას, შესაბამისი ტექნოლოგიური და მეთოდოლოგიური აღჭურვილობას. ასეთი პოტენციალი შეიძლება არ გააჩნდეს ყველა კომერციულ ბანკს, თუ იქ შექმნილი არ არის ინფორმატიზაციის ძლიერი სამსახური.

პრაქტიკაში ჯერ კიდევ გავრცელებულია ისეთი შეხედულება, რომ თითქოს სს-ის შექმნა საკუთარი ძალებით უფრო ეფექტურია, ვიდრე მისი შემუშავება სპეციალური ორგანიზაციის მიერ. აღნიშნული დებულების დაცვის მიზნით, მათ მოჰყავთ შემდეგი არგუმენტები:

- ბანკის სპეციალისტებმა უფრო კარგად იციან ბანკის პირობები და ტრადიციები;

- ისინი ყოველთვის იმყოფებიან ადგილზე და შეუძლიათ ნებისმიერ დროს გაუწიონ დახმარება ბანკის თანამშრომლებს;

- მათი შრომის ანაზღაურება გაცილებით დაბალია, ვიდრე გარედან მოწვეული სპეციალისტების.

ბოლო არგუმენტი მართლაც მხედველობაშია მისაღები, ვინაიდან ამ სფეროში არსებული ფასებიდან გამომდინარე, გარე ორგანიზაციას საინფორმაციო სისტემის შექმნისთვის უნდა გადაუხადოთ გაცილებით დიდი თანხა. ბანკის მომუშავეების ხელფასის დონე გაცილებით დაბალია.

ბანკის მიერ საკუთარი ძალებით შექმნილ საინფორმაციო სისტემის ხარისხი დამოკიდებულია ბანკის ინფორმატიზაციის დარგში არსებული კადრების კვალიფიკაციის დონეზე, ძირითადად, პროგრამისტებისა და ანალიტიკოსების კვალიფიკაციაზე. თუმცა როგორც ზემოთ აღვნიშნეთ, ზოგიერთ ბანკს ასეთი მაღალკვალიფიციური კადრები შეიძლება არ გააჩნდეს. ვინაიდან ახლად შექმნილი ბანკების თანამშრომლებს შესაძლებელია არ გააჩნდეს ბანკის ინფორმატიზაციის სფეროში საკმარისი გამოცდილება, ამიტომ დღეისათვის ისინი ვერ შეძლებენ ეფექტიან საინფორმაციო სისტემების შემუშავებას. სწორედ ეს არის მიზეზი იმისა, რომ ბანკის ძალებით შემუშავებული საინფორმაციო სისტემები ვერ უზრუნველყოფს ინფორმატიზაციაზე ბანკის თანამედროვე მოთხოვნებს, რაც იწვევს ამ მიმართულებით რისკების გაზრდას.

მიუხედავად აღნიშნულისა, ბანკში უნდა შეიქმნას სპეციალისტთა კოლექტივი, რომლის მოღვაწეობის სფერო იქნება ბანკის ინფორმატიზაცია. კოლექტივის წევრებმა უნდა შეძლონ სსის პროექტის ამა თუ იმ ელემენტის შემუშავება, გარე ორგანიზაციებთან კონტაქტების საფუძველზე. კერძოდ, მათ უნდა შეძლონ ინფორმატიზაციას დაქვემდებარებული ამოცანების ასახვა და შესრულებული სამუშაოს მიღება. ამ კოლექტივს ხელმძღვანელობა უნდა გაუწიოს ინფორმაციული ტექნოლოგიების მენეჯერმა ან საინფორმაციო სამსახურის დირექტორმა.

ინფორმატიზაციის ტექნოლოგიური, ტექნიკური, პროგრამული და ინფორმაციული საშუალებების შექმნასა და შეძენაზე იხარჯება დიდი მოცულობის ფულადი, მატერიალური, დროითი და შრომითი რესურსები. ძალიან ხშირად ბანკები ცდილობენ, **სს** შექმნან საკუთარი ძალებით, რაც ხშირად, არც თუ იშვიათად იწვევს **სს**-ის შექმნის პროცესის განელვას დროში და საბოლოოდ ამცირებს ბანკის ეფექტიან ფუნქციონირებას. ამიტომ, რიგ შემთხვევებში, საინფორმაციო სისტემების შეძენა წარმოებს მთლიანად, რომელიმე ტიპური ვარიანტის მიხედვით, გარე მომწოდებელი ორგანიზაციისგან.

შემოთ აღნიშნული მიუთითებს იმაზე, რომ აუცილებელია ისეთი მოდულის შემუშავება, რომელიც უზრუნველყოფს **სს**-ის შექმნის ეფექტიანი ვარიანტის შერჩევას და ტენდერის საფუძველზე ისეთი ორგანიზაცია-მომწოდებლის შერჩევას, რომელიც დადგენილი ეკონომიკური ეფექტიანობის კრიტერიუმებიდან გამომდინარე, ხელსაყრელი იქნება დამკვეთისათვის. შერჩევის ეფექტიანობის კრიტერიუმი უნდა იყოს ეკონომიკური მაჩვენებელი, კერძოდ, **სს**-ის შექმნის ფლობის მთლიანი ღირებულება – **TCO**. **TCO** იანგარიშება როგორც საკუთარი ძალებით საინფორმაციო სისტემის შესამუშავებლად, ასევე დაკვეთით – გარე ორგანიზაციებისა და აუტსორსინგისათვის (ნაწილი სამუშაოების შესრულება გარეორგანიზაციის მიერ). გადანყვეტილება ამა თუ იმ ვარიანტის სასარგებლოდ მიიღება გამომდინარე **TCO** მნიშვნელობიდან.

10.3. გარე მომწოდებლისგან საინფორმაციო სისტემის შეძენის ფლობის მთლიანი ღირებულების მოდელი

სს-ის ფორმირების საწყის ეტაპს წარმოადგენს კონსალტინგი. ამ ეტაპზე ამა თუ იმ სახით ხორციელდება სისტემის სტრუქტურის ფორმირება, ტარდება ტენდერი. ამ პროცესში რთავენ გარედან მოწვეულ სპეციალისტებს ან შესაბამის გამოკვლევებს ატარებენ ბანკის ინფორმატიზაციის სპეციალისტები და სხვა

თანამშრომლები. არსებითად ეს ეტაპი მიეკუთვნება პროექტი-რების ეტაპს და მოითხოვს დანახარჯებს. მიღებული სპეციფიკაციების შესაბამისად, საჭიროა კაპიტალდაბანდებები სისტემის კომპონენტების შესაძენად, რომელიც წარმოებს ნებისმიერ შემთხვევაში ეს დანახარჯები შეიძლება გაიღოს როგორც ერთბაშად, ასევე ნაწილ-ნაწილ. აღნიშნული განხორციელებები მაშინ, თუ სისტემა შეიქმნება სრული მოცულობით. შემდეგი ეტაპია სისტემის დანერგვა, რისთვისაც ორგანიზაციაში იწყება სამუშაოების გაშლა და სისტემის შემმუშავებლის მიერ მისი მახასიათებლების დემონსტრირება. ეს პროცესი რთული სისტემებისათვის შეიძლება გაგრძელდეს საკმაოდ დიდხანს, საერთოდ კი მთავრდება მიღება-ჩაბარების ორმხრივი აქტის გაფორმებით და სისტემის ექსპლუატაციაში შეყვანით. ამის შემდეგ ხდება ექსპლუატაციაში შესული სისტემის სანარმოს ბალანსზე აყვანა.

დანერგვის T მომენტიდან **სს** ითვლება მთლიანად მზად. ამით იწყება **სს**-ის საგეგმო-სანარმოო გამოყენება, რომელმაც სრულად უნდა უპასუხოს მის დანიშნულებას და მაქსიმალური წვლილი შეიტანოს ბანკის საქმიანობაში. ეს არაპირდაპირ შეიძლება შეფასდეს **სს**-ის მიერ შესრულებული სამუშაოს მოცულობით, ან მისი მწარმოებლურობით – *Q*_{პროექტ}. ეს უკანასკნელი როგორც საგეგმო და სასურველი, განისაზღვრება კონსალტინგის ეტაპზე.

ამ მომენტიდან აღმოცენდება დანახარჯები **სს**-ის ამორტიზაციაზე. ამორტიზაციის თანხა შევა ბანკის მიერ გამოშვებული პროდუქტების თვითღირებულებაში. სისტემის ღირებულებაში ასევე შეიტანება ყველა სახის ხარჯი, განეული მის შეძენაზე, დამონტაჟებაზე და ა.შ. თანხის სიდიდე დამოკიდებულია სისტემის ღირებულებაზე და შეიძლება იყოს საკმაოდ დიდი, თუ საქმე გვაქვს მასშტაბური **სს**-ის ღირებულებასთან, რომელმაც შეიძლება შეადგინოს ასობით ათასი და მილიონი დოლარი.

სს-ის ათვისება არის პროცესი, როდესაც სისტემა უნდა გავიდეს საპროექტო სიმძლავრეზე - *Q*_{პროექტ}. აღნიშნული პროცესის განხორციელება საჭიროებს დანახარჯებს, პირველ რიგში, ტიპური ტექნოლოგიური პროცესების გასამართად. პერსონალის სწავლებისა და განვრთნის ეტაპის შემდეგ სისტემას ექნება საპ-

როექტო მწარმოებლურობა, ანუ შეიძლება ითქვას, რომ სისტემა მზადაა სრულყოფილი მუშაობისათვის. ამ თუ იმ ზომით, სისტემის მწარმოებლურობა დაკავშირებულია იმ წვლილთან, რომელიც მას შეაქვს ბანკის ძირითად საქმიანობაში.

შემდეგ ეტაპზე, როცა ამოიწურება საგარანტიო ვადა – $T_{\text{გარ-ანტ.}}$ – წარმოებს ss -ის თანხლება და მხარდაჭერა, რომელიც მოითხოვს გარკვეულ ხარჯებს. რთული სისტემების მიწოდებისას საგარანტიო ვალდებულებების აღება ხდება სპეციალური შეთანხმების საგანი და შეიძლება გააჩნდეს რთული შედგენილობა.

მომსახურების ხარჯები მიმდინარე ხარჯებია, რომლის გაღებაც აუცილებელია, რათა საინფორმაციო სისტემა იყოს მუშა მდგომარეობაში – როგორც მთლიანად, ისე მისი ცალკეული მდგენელი. დანახარჯები საჭიროა სათადარიგო ნაწილების შესაძენად, სარემონტო სამუშაოების შესასრულებლად და სისტემის განყოფილების (გამართვისათვის).

ss -ის ეფექტიანი მუშაობის დაგეგმილი დროის სიდიდე შეიძლება გამოითვალოს შემდეგი ფორმულით:

$$T_{\text{ეფ პროექტ}} = T_{\text{დგრ}} - T_{\text{მზაპროექტ}}$$

სადაც $T_{\text{ეფ პროექტ}}$ არის დრო, რომლის განმავლობაშიც შემუშავებულ სისტემას შეუძლია ეფექტიანი მუშაობა, საწარმოს წინაშე დასახული მიზნების განხორციელება; $T_{\text{დგრ}}$ არის დროის პერიოდი, რომლის განმავლობაშიც სისტემის ფუნქციონირება ეფექტიანი ანუ სისტემის მომსახურების ვადა, რომლის გასვლის შემდეგ ss -ას აღარ შეუძლია ნორმალური ფუნქციონირება, მორალურად და ფიზიკურად მოძველებულია; $T_{\text{მზაპროექტ}}$ არის ss -ის პროექტის შემუშავებისა და დანერგვის დრო. თუ $T_{\text{ეფ პროექტ}}$ არის დიდი, მაშინ ss საწარმოს საქმიანობაში შეიტანს მნიშვნელოვან წვლილს, შეასრულებს რა შესაბამისად დიდი მოცულობის სამუშაოებს. $T_{\text{ეფპროექტ}}$ გადიდებისათვის საჭიროა შემცირდეს საინფორმაციო სისტემის ყველა ის მდგენელი, რომელსაც იგი გაჰყავს საპროექტო სიმძლავრეზე. ss -ის შეძენის ვარიანტისთვის, პირველ რიგში, უნდა შემცირდეს სისტემის ათვისების დრო –

$T_{\text{ათვ}}$ და სასურველია უზრუნველყოფილ იქნეს თანაფარდობა $T_{\text{დგვრ}} > T_{\text{მზაროექტ}}$ (სისტემის შემუშავების დრო), რაც მოითხოვს ამ სამუშაო პერიოდში დანახარჯების გაზრდას. აღნიშნულის გარდა, საჭიროა ყურადღების გამახვილება $T_{\text{დგვრ}}$ -ზე, რომელიც წარმოადგენს სს-ის ამორჩეული ვარიანტის პერსპექტიულობის მაჩვენებელს, სხვადასხვა მომწოდებლისთვის მას შეიძლება ჰქონდეს სხვადასხვა მნიშვნელობა.

10.4. ფლობის მთლიანი ღირებულების საფუძველზე საკუთარი ძალებით საინფორმაციო სისტემის შექმნის მოდელი

როგორც შეძენილი საინფორმაციო სისტემის ეფექტიანობა უნდა შევავსოთ ფლობის მთლიანი ღირებულებით, ანალოგიურად, ფლობის მთლიანი ღირებულებით უნდა შევავსოთ საკუთარი ძალებით შექმნილი საინფორმაციო სისტემის ეფექტიანობა.

სს-ის კონსალტინგი შესრუდება შეძენილი საინფორმაციო სისტემის კონსალტინგის მსგავსად. ამ ეტაპზე მიიღება საერთო გადანყვეტილება: განისაზღვრება საინფორმაციო სისტემის შედგენილობა და მისი საბაზისო მოწყობილობები. კონსალტინგი შეიძლება შესრულდეს როგორც ბანკის სპეციალისტების მიერ, ასევე გარე კონსალტინგური ფირმის მეშვეობით. კონსალტინგის ხარჯები შეიძლება იყოს სხვადასხვა. ასეთი ხარჯების გაღება საჭიროა სანყის ეტაპზე. ადრე თუ გვიან მიიღება გადანყვეტილება სს-ის შედგენილობის შესახებ. შემდეგ იწყება სისტემის შექმნის სამუშაოები. კონსალტინგი განიხილება, როგორც დაპროექტების შემადგენელი. მასთან, საკუთრივ სს-ის დაპროექტება, მისი შინაარსიდან (ესკიზური დაპროექტება, ტექნიკური დაპროექტება, სამუშაო პროექტის შედგენა) გამომდინარე, შეიძლება გაგრძელდეს განუსაზღვრელი დროით, როგორც წესი, დადგენილი რიგის ან კომპონენტების მიხედვით, რაც იწვევს ამ ეტაპის დამთავრების დროის დადგენის შეუძლებლობას. ასე თუ ისე, საინფორმაციო სისტემის დაპროექტების ეტაპის დამთავრება განსაზღვრავს მის შექმნას, მზადყოფნას, მის საპროექტო ვარი-

ანტს, რაც ფიქსირდება წარმოების ხელმძღვანელის მიერ ბრძანების გამოცემით. ბრძანებით განისაზღვრება სს-ის შედგენილობა და კომპონენტების მახასიათებლები, მისი გეგმიური და საპროექტო მწარმოებლურობა.

მონყოილობებისა და სისტემის სხვა კომპონენტების შეძენა შეიძლება განხორციელდეს პარტიებად, ერთმანეთის მიყოლებით. პარტიების ფორმირება ან მონოდების დაკომპლექტება, ან კიდევ პარტიის ღირებულების ანაზღაურების ფორმა წარმოადგენს ოპტიმიზაციის ცალკე ამოცანას. საკუთარი ძალებით სს-ის შექმნას და გარემომწოდებლისგან მის შეძენას ექნება შემდეგი სახე:

სს-ის ცალკეული კომპონენტების შეძენაზე განეული დანახარჯები ნაკლებია სს-ის მთლიანად შეძენაზე განეულ დანახარჯებზე, ვინაიდან ამ შემთხვევაში უნდა ანაზღაურდეს მხოლოდ საბაზისო ტექნიკური და პროგრამული საშუალებების ღირებულება. ხოლო როდესაც ხდება მთლიანად საინფორმაციო სისტემის შეძენა, მაშინ უნდა ანაზღაურდეს პროგრამული დანართების ღირებულებაც და სს-ის მომწოდებლის მიერ შესრულებული სამუშაოებიც, აგრეთვე, კომპანია მომწოდებლის გეგმიური მოგება.

საკუთარი ძალებით ორგანიზაციაში სს-ის დამზადება ერწყმის დაპროექტების ეტაპს, თუმცა ამ დროს შეიძლება საჭირო გახდეს არასაპროექტო სამუშაოების შესრულებაც. მაგ., ენერგომომარაგების სისტემის შექმნა, ქსელის გაყვანა და ა.შ. ამ შემთხვევაში ჩვენ მხედველობაში გვაქვს ისეთი დანახარჯები, რომლებიც არ მიეკუთვნება პროექტირების დანახარჯებს.

სს-ის ძირითადი ფონდების ამორტიზაციის ფონდის ფორმირება წარმოებს ეტაპიდან ეტაპამდე, ანუ ერთი რიგის სამუშაოების ჩაბარებიდან მეორე რიგის სამუშაოების ჩაბარებამდე, მწყობრში შეყვანის მიხედვით. პირველ რიგში, ეს არის სს-ის კომპონენტების შეძენა, რაც უნდა მოხდეს დაპროექტების დამთავრებისთანავე. უნდა განხორციელდეს სს-ის ქვესისტემების, მოდულების დაკომპლექტება საბაზისო საშუალებებით. უნდა აღინიშნოს, რომ საკუთარი ძალებით სს-ის შექმნისას ადგილი აქვს საინფორმაციო სისტემის კომპონენტების აღრიცხვის სპეციფიკურობას. საქმე იმაშია, რომ საკუთარი ძალებით სს-ის

შექმნისას სს-ის კომპონენტები აღირიცხება, როგორც ძირითადი ფონდები, არამატერიალური აქტივების სახით. საბუღალტრო აღრიცხვის დებულების მიხედვით მატერიალურ აქტივებს მიეკუთვნება ის აქტივები, რომელთა გამოყენება წარმოებს სამეურნეო საქმიანობაში, მომსახურების ვადა ერთ წელზე მეტია და მოაქვს შემოსავალი საწარმოსათვის. ამ ჩამონათვალში ხვდება კომპიუტერები, პროგრამები, მონაცემთა ბაზები და სს-ის სხვა კომპონენტები. აღნიშნულიდან გამომდინარე, მათი შეფასება უნდამოხდეს მათი საბალანსო ანუ პირვანდელი ღირებულებით და დაერიცხოს ამორტიზაცია, შემდგომში მათი აღდგენისათვის. რაც მატერიალურ აქტივებზე ვრცელდება იგივე წესი, რაც ძირითად ფონდებზე. ე.ი. მათი საბაზრო ღირებულების განსაზღვრა და აღრიცხვა წარმოებს, როგორც ძირითადი საშუალებების.

გარკვეული დროის გასვლის შემდეგ არამატერიალური აქტივები ცვდება, მცირდება მათი სარგებლიანობა და ისინი უნდა შეიცვალოს უფრო სრულყოფილი და თანამედროვე საშუალებებით. ამიტომ მათ ერიცხებათ ცვეთა, ამორტიზაცია. არამატერიალური აქტივები, რომელიც გამოიყენება პროდუქციის გამოსაშვებად, განიცდის ცვეთას. ცვეთის თანხა შეიტანება პროდუქციის თვითღირებულებაში. ზოგიერთ ქვეყანაში, მაგ., რუსეთში, გამოთვლით ტექნიკაზე, საინფორმაციო სისტემებსა და მონაცემთა დამუშავების სხვა სისტემებზე წლიური ამორტიზაციის ნორმა 25%-ის ტოლია. არამატერიალური აქტივებისათვის ამორტიზაციის ნორმა დგინდება საგეგმო პერიოდში მათი გამოყენების მიხედვით. მაგრამ თუ ასეთი არ არის დადგენილი, მაშინ ეს ვადა უდრის 10 წელს. სს-ის თითოეული კომპონენტის გამოყენების ხანგრძლივობა საწარმოში შეიძლება დაადგინოს სპეციალისტმა, მათი გამოყენების მიხედვით, ხელშეკრულების საფუძველზე. ასე იანგარიშება, მაგალითად, ამორტიზაციის ნორმა პროგრამულ საშუალებებზე.

ინფორმატიზაციის საშუალებები სხვა ძირითად ფონდებთან შედარებით, ძალიან დინამიურია, სწრაფად ძველდება, ამიტომ მათი აღდგენისათვის საჭიროა მნიშვნელოვანი თანხები, რომელთა შექმნა წარმოებს ამორტიზაციის საფუძველზე. გამოთვლით

ტექნიკაზე ამორტიზაციის ნორმის გაზრდა 25 %-მდე უზრუნველყოფს მათი აღდგენისათვის თანხების დაგროვების დაჩქარებას.

საკუთარი ძალებით სს-ის შექმნისას და დანერგვისას ათვისების ეტაპების განხორციელება წარმოებს ეტაპობრივად ანუ ციკლურად, სს-ის კომპონენტების ექსპლუატაციაში შეყვანის შესაბამისად, ანუ სს-ის ექსპლუატაციაში შეყვანის რიგის მიხედვით. ექსპლუატაციაში შეყვანის ამ რიგებს შორის შეიძლება აღმოცენდეს პაუზა, ისინი შეიძლება ერთმანეთს დაემთხვეს. რა თქმა უნდა, სხვადასხვა რიგის სამუშაოებზე გაწეული დანახარჯები შეიძლება იყოს სხვადასხვა, ასევე სხვადასხვა შეიძლება იყოს სს-ის ეტაპების ხანგრძლივობა. ამ შემთხვევაში, თანხლებისა და მხარდაჭერის ორგანიზაცია შესაძლებელია საკუთარი ძალების გამოყენებით. სს-ის ფორმირების შემდეგ იზრდება დანახარჯები თანხლებისა და მხარდაჭერის სამუშაოების შესასრულებლად. თუ ეს ასე არ მოხდა, მაშინ შემცირდება სს-ის მუშაობის ხარისხი.

სს-ის მომსახურება საკუთარი ძალების საფუძველზე ხდება შეძენილი სს-ის ვარიანტის მომსახურების მსგავსად.

თუმცა ამ პროცესის განვითარება წარმოებს ციკლურად - სამუშაოთა რიგის ჩაბარების შესაბამისად. ამ პროცესში სს-ის კომპონენტების მომსახურება მიმდინარეობს მიღება-ჩაბარების აქტის მიხედვით, ექსპლუატაციაში შეყვანის შესაბამისად. სს-ის შექმნის მიმდინარეობისას ადგილი აქვს სს-ის გამოცდას როგორც მთლიანად, ისე მისი ცალკეული კომპონენტების მიხედვით, რასაც შეიძლება ჰქონდეს ციკლური ხასიათი.

დროთა განმავლობაში სს-ის კომპონენტებზე (თანხლება, მხარდაჭერა, მომსახურება და გამოცდა) გაწეული დანახარჯები იზრდება, რაც იწვევს სს-ის შექმნისა და შენახვის ხარჯების გადიდებას.

10.5. საინფორმაციო სისტემების შექმნის ვარიანტების შედარება

სს-ის ვარიანტების შედარება შეიძლება ფლობის მთლიანი ღირებულების მოდელის საფუძველზე. ამასთან, მხედველობაში უნდა მივიღოთ ის, რომ ორივე ვარიანტის (საკუთარი ძალებით და შეძენილი გარეორგანიზაციიდან) შემთხვევაში იქნება ერთი და იგივე **სს**. მართალია, ამის უზრუნველყოფა პრაქტიკულად საკმაოდ რთულია, თუმცა მაინც ხდება დასკვნების მეთოდოლოგიური დამტკიცების მიზნით.

უთუოდ უნდა აღვნიშნოთ, რომ თუ **სს**-ის შექმნა ხორციელდება ბანკში, სპეციალურად შექმნილ მუდმივმოქმედი კოლექტივის ძალებით, ამ მიზნისათვის გამოყოფილი გეგმური რესურსების ზრდის გარეშე, მაშინ სამუშაოთა რიგის დანერგვის ციკლი გაგრძელდება. საკუთარი ძალებით სისტემის შექმნის მომენტი ($T_{სს}$) სულ უფრო და უფრო გადაინევს, შეიძლება ვთქვათ, რომ **სს**-ის საკუთარი ძალებით შექმნის ტემპი იქნება დაბალი, ვიდრე მზა სისტემის მთლიანად შეძენისა. ე.ი. ყოველთვის სამართლიანია იქნება ფორმულა $T_{შე} < T_{სს}$. უფრო მეტიც, ამის გამო შეიძლება **სს** ვერ შეიქმნას ბოლომდე სრული მოცულობით და ვერ მიიღოს საპროექტო მწარმოებლურობას ($Q_{სს}$) იმ ინტერვალში, რომელშიც **სს**-ის შესაქმნელი ვარიანტი პოტენციურად შეიძლება იყოს ეფექტიანი. თუ გავაგრძელებთ სამუშაოებს კონცეფციის ცვლილების გარეშე, მაშინ შექმნილი **სს** იქნება მორალურად მოძველებული. შემოთავაზებული **სს**-ის ვარიანტებიდან უპირატესობა მიენიჭება იმ ვარიანტს, რომლისთვისაც ეფექტიანობის მაჩვენებელი მიაღწევს ყველაზე მაღალ მნიშვნელობას, ე.ი. ყველა **n**-ური ვარიანტისათვის გვექნება $\Phi_n = \max$.

ზემოთ წარმოდგენილ მასალებში განხილული იყო ეფექტიანობის კრიტერიუმების ფორმირება საკუთარი ძალებით და გარე მომწოდებლისგან შეძენილი მზა სისტემისათვის. როგორც ჩანს, შეძენილმა **სს**-მამ შეიძლება სწრაფად უზრუნველყოს ინფორმაციის დამუშავებაზე ორგანიზაციის მოთხოვნები სრული მოცულობით, ვიდრე საკუთარი ძალებით შექმნილმა **სს**-მ, თუმ-

ცა გარე მომწოდებლისგან შეძენილი მზა სისტემისათვის ფულის გადახდა ერთბაშად იქნება საჭირო.

თუ **სს** ბანკში მნიშვნელოვნად განსაზღვრავს ბიზნესის წარმატებას, მაშინ იგი სტრატეგიული სისტემაა. ამ შემთხვევაში, წამყვან კრიტერიუმს მის შექმნაში წარმოადგენს სისტემის სწრაფქმედება ან მოქმედებაში შეყვანის სისწრაფე, ეს ნიშნავს, რომ **სს**-ის შექმნის ამოცანა შეიძლება დაისვას, როგორც ოპტიმალურობის ამოცანა, მართვის სწრაფმოქმედების მიხედვით შესაძლო შეზღუდვებით. ამ შემთხვევაში ბანკმა **სს**-ის შექმნაში ერთდროულად უნდა ჩადოს მის განკარგულებაში მყოფი საშუალებები.

სს-ის შექმნა შესაძლებელი და გამართლებულია მხოლოდ მაშინ, როცა მისი ექსპლუატაციაში სწრაფად შეყვანა მთლიანი საპროექტო სიმძლავრით განსაზღვრავს ბანკის წარმატებას.

სს-ის საკუთარი ძალებით სისტემის შექმნისათვის გამოყოფილი საშუალებები შეიძლება საკუთარი შეხედულებით განაწილდეს დროში ხანგრძლივი პერიოდისათვის, რაც მიმზიდველია ნებისმიერი ორგანიზაციისთვის, თუმცა სისტემაში გათვალისწინებული მწარმოებლურობის მაჩვენებლების მიღწევა შეიძლება გაჭიანურდეს, რაც მიუღებელია ბანკის ძირითადი საქმიანობისათვის, ამიტომ **სს**-ის შექმნა უფრო მიმზიდველია. იმავედროულად ნათელია, რომ საკუთარი ძალებით **სს**-ის შექმნისას მისი ცალკეული ნაწილის შექმნა ხდება გარეთ. **სს**-ის შეფასების საერთო კრიტერიუმის როლში შეიძლება გამოვიდეს **სს**-ის მიერ ინფორმაციის დამუშავებისათვის შესრულებული ოპერაციების მოცულობა-**W** შეფარდებული სისტემის ფლობის მთლიან ღირებულებასთან – **C_{TCO}**.

$$\Xi = W / C_{TCO}$$

საინტერესოა **სს**-ის შექმნის ორი ვარიანტის – შეძენილისა და საკუთარი ძალებით შექმნილის – შედარება. თუ ეს ორი ვარიანტი მიღებული კრიტერიუმების მიხედვით ერთნაირად ეფექტურია, მაშინ შესრულება პირობა $\Xi_{შეძ} = \Xi_{საკ}$ ამ პირობის გათვალისწინებით, ადგილი ექნება:

$$\begin{aligned} W_{შედ} / C_{Tcoშედ} &= W_{საკ} / C_{Tcoსაკ} \\ W_{საკ} / W_{შედ} &= C_{Tcoსაკ} / C_{Tcoშედ} \end{aligned}$$

თუ ეს პირობა სრულდება, მაშინ ეს ორი ვარიანტი, მოცემული კრიტერიუმების მიხედვით, ექვივალენტურია. ამ პირობას გააჩნია შემდეგი აზრი: **სს**-ის შექმნა საკუთარი ძალებით შეიძლება ეკვივალენტური იყოს მზა სისტემის შეძენის, თუ მისი ფლობის მთლიანი ღირებულება იმდენჯერ ნაკლებია შეძენილი **სს**-ის ფლობის მთლიან ღირებულებაზე, რამდენჯერაც საკუთარი ძალებით დამუშავებული ინფორმაციის მოცულობა ნაკლებია შეძენილი სისტემით დამუშავებული ინფორმაციის მოცულობაზე.

საკუთარი ძალებით შექმნილი **სს**-მა შეიძლება უფრო მიმზიდველი იყოს მოცემული კრიტერიუმების მიხედვით, თუ მისი შექმნის დანახარჯები შემცირდება. ეს შესაძლებლობა დღემდე იზიდავს არა მარტო ბანკის ხელმძღვანელებს, არამედ ინფორმაციის დარგის სპეციალისტებსაც, პირველ რიგში, იმიტომ, რომ საკუთარი ძალებით **სს**-ის შემქმნელი ბანკის მუშაკების ხელფასი გაცილებით დაბალია, ვიდრე გარე ორგანიზაციიდან მოწოდებული სისტემის სპეციალისტების ხელფასი. სხვა მდგენელი $C_{Tcoსაკ}$ შეიძლება იყოს დაბალი, ვიდრე **სს**-ის შეძენის, განსაკუთრებით მაშინ, თუ შეზღუდულია ფინანსების მოცულობა. თუმცა ეს მიმზიდველობა მოჩვენებითი აღმოჩნდება ხოლმე, როცა გაირკვევა რომ ასეთი სახის **სს**-ის მიერ შესრულებული სამუშაოს მოცულობა ბევრად ნაკლებია, ვიდრე შეძენილი **სს-ისა**. ამის საფუძველზე შეიძლება გამოვიტანოთ შემდეგი დასკვნა: იმ ბანკებმა, რომლებიც იმყოფებიან ინფორმატიზაციის პროცესების საწყის სტადიაზე, შეიძლება უპირატესობა მიანიჭონ **სს**-ის შექმნას საკუთარი ძალებით, თუმცა ამით ისინი ხელს უწყობენ თავიანთი ჩამორჩენილობის კონსერვაციას. თუ ბანკს გააჩნია სტრატეგიული მიზნები და მისთვის მნიშვნელოვანია **სს**-ის მიერ შესრულებული სამუშაოების და მომსახურების მოცულობა, მაშინ ბანკს არ რჩება ამორჩევის ვარიანტი, მიუხედავად ფულადი საშუალებების მოჩვენებითი ეკონომიისა, მან უპირატესობა უნდა მიანიჭოს **სს**-ის ფორსირებულ შექმნას და დანერგვას, ანუ მის შეძენას.

განხილული მოდელის საფუძველზე დგება დანახარჯების მართვის ამოცანა, ე. ი. უნდა განისაზღვროს საუკეთესო ან დასაშვები დანახარჯების მნიშვნელობები. ასეთი ამოცანების დასახვისას აუცილებელია დანახარჯების დეტალური აღწერა და მათი განაწილება სს-ის სიცოცხლის ციკლის ეტაპების მიხედვით.

ნებისმიერი ბანკის ხელმძღვანელობა პერიოდულად მიდის იმ დასკვნამდე, რომ ბანკში არსებული ავტომატიზებულ საინფორმაციო სისტემა (ასს) ვერ უზრუნველყოფს ბანკის თანამედროვე მოთხოვნებს და ლეზულობს გადანყვეტილებას ახალი, პერსპექტიული სისტემის დანერგვის შეახებ. პრობლემა ამ შემთხვევაში მდგომარეობს იმაში, თუ როგორ მიიღოს აუცილებელი და საკმარისი ინფორმაცია დასმული პრობლემის გადასაწყვეტად. მან უნდა გაითვალისწინოს, რომ ახალი ავტომატიზებული სისტემის დანერგვა არ გაინელოს დროში, არ მოხდეს ბიუჯეტის გადახარჯვა, შეძლოს რისკების მინიმიზაცია და სასურველი შედეგის მიღწევა.

როგორც წესი, პროექტის დანერგვის მიზანშეწონილობა და მისი განხორციელების აუცილებლობა წარმოადგენს ნებისმიერი პროექტის საწყის სტადიას როგორც პროექტის საკუთარი ძალეობით შემუშავებისას, ასევე მისი შეძენისას, აუცილებელია, ასეთი ანალიზი ჩატარდეს ეკონომიკური, ტექნიკური, ტექნოლოგიური და სოციალურიდან გამომდინარე. ბანკმა პროექტის შემუშავების დაწყებამდე პასუხი უნდა გასცეს შემდეგ კითხვებზე:

- რა დროის განმავლობაში უნდა მოხდეს ავტომატიზებული საინფორმაციო სისტემის ამორჩევა, შემუშავება, ექსპლუატაცია;

- ახალი საბანკო საინფორმაციო სისტემის (სსს-ის) დანერგვა მართლა ნაკარნახევია თუ არა ბიზნესის მოთხოვნებიდან გამომდინარე და რომელი ალტერნატიული ვარიანტები არსებობს მის გადასაწყვეტად;

- არსებობს თუ არა ინფორმაციული ტექნოლოგიების ბაზარზე ისეთი გადანყვეტილება (სისტემა), რომელიც სრულყოფილად დააკმაყოფილებს ბანკის მოთხოვნებს;

- დაახლოებით რა ელირება საკუთარი ძალებით და გარე ორგანიზაციის მიერ შემუშავებული სსს;

- რამდენად შეესაბამება შემოთავაზებული სსს ბანკის სტრატეგიულ მიზნებს;

- როგორი იქნება ძირითადი რისკები ამა თუ იმ სისტემის დანერგვისას.

ეკონომიკური მიზანშეწონილობის დასაბუთება მოიცავს შესაძლო დანახარჯების შედარებას იმ სარგებელთან, რასაც შემოთავაზებული სსს მისცემს ბანკს. ამ შემთხვევაში უნდა გაანალიზდეს ისეთ მაჩვენებლები, როგორიცაა: სისტემის გამოსყიდვის პერიოდი, რენტაბელობის ნორმა, ფლობის მთლიანი ღირებულება და ა. შ.

ტექნიკურად განხორციელების შესაძლებლობის განსაზღვრისას ვლინდება, თუ რამდენად ადეკვატურია ბაზარზე არსებული ტექნიკური და ტელესაკომუნიკაციო სისტემები შემოთავაზებული სისტემისთვის;

ტექნოლოგიური და ოპერაციული მიზანშეწონილობის განსაზღვრა მოიცავს იმ შესაძლო დადებითი მხარეების შეფასებას, რომელთა საფუძველზეც შეიძლება განხორციელდეს მომსახურების ხარისხის გაუმჯობესება, პროდუქტების სპექტრის გაფართოება და ბანკის ბიზნესის სხვა მოთხოვნების დაკმაყოფილება;

სოციალური მოთხოვნები მოიცავს, თუ რამდენად მზადაა მომხმარებელი შემოთავაზებული გადანყვეტილებების ექსპლუატაციისთვის (დატვირთვის გაზრდა, ახალი პროდუქტების ექსპლუატაციისთვის პროფესიული დონის ამაღლება, კადრების გადამზადება).

ზემოთ ჩამოთვლილი შეგროვებული ინფორმაციის ანალიზის საფუძველზე ბანკის ხელმძღვანელობა ღებულობს გადანყვეტილებას სსს-ის შეძენის ან საკუთარი ძალებით შემუშავების შესახებ.

შემდეგ ნაბიჯს სსს-ის შერჩევაში წარმოადგენს მომავალი სისტემისთვის წაყენებული ფუნქციური მოთხოვნების ჩამოყალიბება. ასეთი მოთხოვნები უნდა ჩამოაყალიბოს ბანკის თანამშრომლებისგან შემდგარმა სპეციალურმა გუნდმა ან კონსულ-

ტანტებმა, ბანკის ქვეგანყოფილებების სპეციალისტებთან ურთიერთობის საფუძველზე. ამ გუნდს უნდა უხელმძღვანელოს ბანკის მაღალი დონის ხელმძღვანელობის (ბანკის გამგეობა) ერთ-ერთმა წევრმა. ეს ეტაპი მოიცავს შემდეგ ნაბიჯებს:

- ბანკის ბიზნეს განყოფილებების ხელმძღვანელებისა და წარმომადგენლებთან ინტერვიუს აღებას;
- ბიზნეს-პროცესების არსებული და დაგეგმილი ტექნოლოგიების, თავისებურებების და ინფორმაციული ნაკადების გაცნობას;
- ბანკის ორგანიზაციული სტრუქტურის, სტრატეგიისა და მიმართულებების განვითარების შეფასება და მათი ზემოქმედება სსს-ის ამორჩევაზე;
- გამოყენებული სისტემის დეტალურ ანალიზს;
- სისტემის ტექნიკური მახასიათებლებისათვის (ოპერაციების მოცულობა, ოპერატიულობა, მონაცემების დაცულობა) მოთხოვნების განსაზღვრას, შეთანხმებას და დამტკიცებას;
- იმ ბიზნესპროცესების განსაზღვრაც, დაზუსტებაც და დამტკიცებაც, რომელთა ავტომატიზაცია უნდა განხორციელდეს;
- დაბოლოს, სისტემისადმი მოთხოვნების განსაზღვრას და დამტკიცებას. შესრულებულმა სამუშაოებმა ასახვა უნდა ჰპოვოს დოკუმენტში „მოთხოვნები სისტემისადმი“.

განვიხილოთ სსს-ადმი წაყენებული მოთხოვნები:

- სისტემა დაფუძნებული უნდა იყოს თანამედროვე ტექნოლოგიებზე და თანამედროვე პლატფორმაზე (ოპერაციული სისტემები, მონაცემთა ბაზების მართვის სისტემები), რომლებიც საბოლოოდ უზრუნველყოფენ სისტემის მოქნილობას, გახსნილობას, მასშტაბურობას;
- სისტემამ უნდა უზრუნველყოს გადაწყვეტილების მიღების ოპერატიულობა, ინტეგრირებულობა;

- მას ასევე უნდა გააჩნდეს სტატისტიკური მონაცემების ერთიანი ბაზა, არსებულ სისტემებთან და მოდულებთან ინტეგრაციის შესაძლებლობა;

- კანონმდებლობის შეცვლის გამო ბანკის მოთხოვნებიდან გამომდინარე, უნდა გააჩნდეს გაფართოებისა და ფუნქციური შესაძლებლობების თანდათანობით ზრდის შესაძლებლობა;

- დასამუშავებელ ტრანზაქციების, ან კლიენტების რაოდენობის გაზრდის შესაძლებლობა;

- სსს-ში შესაძლებელი უნდა იყოს ელექტრონული დოკუმენტბრუნვის მეშვეობით ოპერაციების შეყვანა და დამუშავება;

- სისტემამ უნდა შეძლოს ბანკის პროდუქტებისა და კლიენტების მიხედვით ანალიზური გარიგებების ფორმირება;

- სისტემას უნდა შეეძლოს გამოყენების დონეზე მომხმარებელთა მხრიდან სისტემაზე ზემოქმედება, კონტროლის განხორციელება და მისი შემდგომი ანალიზი;

- სისტემას უნდა შეეძლოს გარე დანართებიდან მონაცემების იმპორტირება;

- სისტემამ უნდა უზრუნველყოს საქმიანი ინფორმაციის კონფიდენციალობა, მთლიანობა და წვდომის შესაძლებლობა;

- სისტემის ანგარიშგების გენერატორი საშუალებას უნდა იძლეოდეს, განვსაზღვროთ ანგარიშგებების და მონაცემების გარე სახე, რომელთა საფუძველზეც უნდა მოხდეს ანგარიშგებების ფორმირება, მონაცემთა დახარისხების და ამორჩევის წესის განსაზღვრა;

- სისტემას უნდა შეეძლოს მომხმარებლის ან გაცვლის ინტერფეისის მიერ შეტანილი მონაცემების ლექსიკური, სინტაქსური და სემანტიკური შემოწმება;

- სისტემას უნდა შეეძლოს ყველა შესრულებული ოპერაციის დაფიქსირება ოქმის სახით და მასთან ხელმისაწვდომობა უსაფრთხოების ადმინისტრატორისთვის, უნდა გააჩნდეს წვდომის შეზღუდულობა;

- სისტემას უნდა შეეძლოს მომხმარებელთა კლასიფიკაცია, სხვადასხვა კატეგორიის მომხმარებლისთვის სისტემასთან და მონაცემებთან წვდომის სხვადასხვა დონის ორგანიზება. გარდა ზემოთ აღნიშნული მოთხოვნებისა, სისტემას შეიძლება წაეყენოს მრავალი სპეციფიკური მოთხოვნა (მაგ., კლიენტის ანგარიშიდან თანხის ჩამონერამდე შეამოწმოს მის ანგარიშზე არსებული ფულადი საშუალებები, ლიმიტების ნაშთები და სხვ).

მას შემდეგ, რაც დასაბუთდება სისტემის შექმნა და განისაზღვრება მისთვის წაყენებული მოთხოვნები, შეიძლება გადავიდეთ უშუალოდ სისტემის ამორჩევაზე.

სსს-ის ამორჩევის ძირითადი ეტაპებია: სისტემის ამოსარჩევად ტენდერის ჩატარება და კონტრაქტის გაფორმება.

10.6 ტენდერის ჩატარება

სსს-ის ამოსარჩევად არსებობს ტენდერის ჩატარების ორი ფორმა: ღია და დახურული [67].

ტენდერის ჩატარების ღია ფორმა გულისხმობს ტენდერის ჩატარების შესახებ ოფიციალური განცხადების გაკეთებას, რაც იმას ნიშნავს, რომ მასში მონაწილეობის მიღება შეუძლია ყველა დაინტერესებულ ფირმას. დახურული ტენდერის ჩატარება კი გულისხმობს, რომ ტენდერში მონაწილეთა წრეს განსაზღვრავს თვითონ ბანკი იმ ორგანიზაციებს, რომლებიც ვერ მოხვდებიან ამ ჩამონათვალში, ტენდერში მონაწილეობის მიღების უფლება არ აქვთ. ჩვეულებრივ, **სსს-ის** ამორჩევისთვის იყენებენ ტენდერის ჩატარების მეორე ფორმას, თუმცა ზოგიერთ შემთხვევაში შეიძლება გამოიყენონ პირველი ფორმაც. დახურული წესით ტენდერის ჩატარება დაკავშირებულია **სსს-ის** პროგრამული უზრუნველყოფის სპეციფიკასთან, სახელდობრ, ცნობილი ფირმების რაოდენობა შეზღუდულია.

ტენდერის ჩატარება შეიძლება ორ ეტაპად. ტენდერის ჩატარების პირველ ეტაპზე წარმოებს ტენდერის ჩასატარებლად მოსამზადებელი სამუშაოების ორგანიზება, რაც მდგომარეობს

შემდეგში: სატენდერო დოკუმენტების მომზადება, ტენდერის ჩატარების პირობებისა და წესების განსაზღვრა და დამტკიცება.

ტენდერის ჩატარებისთვის მინიმალურ დოკუმენტაციას მიეკუთვნება:

1. ტენდერის ჩატარების წესი (მეთოდика) და შედეგების შეჯამება.

2. ტენდერში მონაწილეთა მოწვევა (მოსაწვევის გაგზავნა).

3. ტენდერში მონაწილის ანკეტა, რომელიც ტენდერში მონაწილემ, უნდა შეავსოს და უკან დაუბრუნოს დამკვეთს.

მეორე ეტაპზე უშუალოდ უნდა განხორციელდეს: ტენდერში მონაწილეთა სიის შედგენა და მათთვის შეტყობინებების გაგზავნა. ტენდერში პოტენციური მონაწილეების დასადგენად უნდა განიხილებოდეს ის ფირმები, რომლებიც უშვებენ **სსს**-ის პროგრამულ უზრუნველყოფას და მიზანშეწონილია თუ არა მათი მონაწილეობა ტენდერში.

ტენდერში მონაწილე ფირმისთვის გაგზავნილი მოწვევა უნდა შეიცავდეს შემდეგი სახის ინფორმაციას: საერთო ინფორმაცია, ტენდერის პირობები, ტენდერის ჩატარების წესი, ჩატარების ვადები, საკონტაქტო ინფორმაცია და კონფიდენციალობა. ტენდერში მონაწილის ანკეტაში მითითებული უნდა იყოს: კომპანიის შესახებ საერთო ინფორმაცია (საკონტაქტო ინფორმაცია, წარმოდგენილი სისტემის დასახელება, შექმნის წელი, თანამშრომელთა და კლიენტთა რაოდენობა, წარმომადგენლობები და პარტნიორები).

სისტემის შესახებ საერთო ინფორმაცია მოიცავს:

დანერგილი სისტემების რაოდენობას როგორც მოცემულ ქვეყანაში, ასევე საზღვარგარეთ, ტექნიკურ პლატფორმას (მონაცემთა ბაზები, ოპერაციული სისტემა), მოთხოვნებს სერვერებისა და მუშა სადგურებისადმი, არქიტექტურას, დამატებით პროგრამულ უზრუნველყოფაზე ლიცენზიებს;

ფუნქციურობა. (მულტივალუტობა, ქვეყნის ეროვნული ბანკის ინსტრუქციებთან საბუღალტრო აღრიცხვის შესაბამისობა, რამდენიმე ანგარიშთა გეგმისა და აღრიცხვის საერთაშორისო სტანდარტების გამოყენების შესაძლებლობა);

გახსნილობა. (გარე სისტემებიდან მონაცემების იმპორტის შესაძლებლობა, ურთიერთობა გარე სისტემებთან). დანერგვისთვის საჭირო საშუალო დრო, მიახლოებითი ღირებულება, სისტემის თანხლების ორგანიზება.

მესამე ეტაპი. გაცნობის მიზნით ყველაზე საუკეთესო სისტემების ამორჩევა. იმ კომპანიებს, რომლებიც მოხვდნენ ტენდერში შესაძლო მონაწილეთა სიაში და რომლებმაც განაცხადეს ტენდერში მონაწილეობის სურვილი, ეგზავნებათ დოკუმენტი სისტემისადმი წაყენებული მოთხოვნების შესახებ. შემდეგ წარმოებს თითოეული სისტემის გაცნობა. მონაწილეებს ეძლევათ გარკვეული დრო იმის გასარკვევად, თუ რამდენად პასუხობს ტენდერში მონაწილე სისტემა ბანკის მიერ წაყენებულ მოთხოვნებს. ტენდერში მონაწილე ფირმის საანკეტო მონაცემების გაცნობის საფუძველზე და დანვრისათვის გაცნობის მიზნით, წარმოებს ყველაზე პერსპექტიული სისტემების შერჩევა. საბოლოოდ, ტენდერში შემდგომი მონაწილეობისთვის შეირჩევა 3-4 სისტემა – მეტი რაოდენობის დატოვება ტენდერში შემდგომი მონაწილეობისათვის არაა სასურველი, რადგან გაზრდის სისტემის ამორჩევის დროს.

მეოთხე ეტაპი. სისტემების დეტალური გაცნობა და სისტემის შერჩევა. მას შემდეგ, რაც დადგინდება შემდგომ ეტაპზე მონაწილე სისტემები, უნდა დაიგეგმოს მათთან შეხვედრა, შედგეს შეხვედრების გრაფიკი. მათ მიერ წარმოდგენილი სისტემების დეტალური განხილვისთვის, გაცნობის მსვლელობისას შეიძლება ე. წ. ტესტური დავალების გამოყენება. ეს უკანასკნელი გულისხმობს ბანკში შერჩეული პროცედურების სისტემის მიერ შესრულებას. ზოგჯერ მომწოდებელი წინასწარ უნდა გააფრთხილოს აღნიშნულის შესახებ, რათა მან შეძლოს სისტემის მომზადება აღნიშნული პროცედურების შესასრულებლად, რაც საბოლოოდ გამოიწვევს სისტემის გაცნობისთვის საჭირო დროის შემცირებას. შემდეგ წარმოებს მომწოდებლის მიერ წარმოდგენილი წინადადებების ანალიზი და სისტემის შეფასება. შეფასება წარმოებს შემდეგი კრიტერიუმების მიხედვით:

- სისტემების დეტალური გაცნობა, ბანკის ბიზნესმოთხოვნებთან შესაბამისობა;

- სისტემების დეტალური გაცნობა შემოთავაზებული სისტემის მოდიფიკაციისა და საბოლოოდ დამუშავების აუცილებლობა;

- სისტემების დეტალური გაცნობა, სისტემის ღირებულება, მხარდაჭერისა და მომსახურების ღირებულება;

- სისტემების დეტალური გაცნობა და სისტემის ფარული დანახარჯები, სისტემის გამოყენების შედეგად მიღებული სარგებელი;

- სისტემების დეტალური გაცნობა და სისტემის მომწოდებლის საიმედოობა და რეპუტაცია.

წარმოდგენილი სისტემების შეფასება და ანალიზი. საბოლოო შედეგი როგორც ოპტიმალური ვარიანტი უნდა აისახოს შედგენილ ანგარიშში და მიეცეს რეკომენდაცია. მომზადებული ანგარიშის საფუძველზე, რომელშიც მითითებულია განხილული სისტემების დადებითი და უარყოფითი მხარეები, ბანკის ხელმძღვანელობამ უნდა გააკეთოს არჩევანი რაც, როგორც წესი, უნდა მოხდეს ბანკის გამგეობის სხდომაზე, სადაც გაცხადდება ბანკის სხვადასხვა ქვეგანყოფილებების წარმომადგენლის შეფასება და კომენტარი წარმოდგენილი სისტემების შესახებ.

შეიძლება აირჩეს არა მარტო ერთი ოპტიმალური ვარიანტი, არამედ მეორეც – ე.წ. სადაზღვევო ვარიანტი. იმ შემთხვევაში, თუ აღმოცენდა პრობლემები შერჩეულ მომწოდებელთან, მაგალითად, კონტრაქტის გაფორმების სტადიაზე, მაშინ მოლაპარაკება დაიწყება მეორე მომწოდებელთან. აღნიშნული სიტუაცია უნდა ეცნობოს ორივე კომპანიას, რაც საბოლოოდ სასარგებლო იქნება ბანკისთვის.

კონტრაქტის გაფორმება. სისტემის საბოლოოდ შერჩევის შემდეგ იწყება შეთანხმებისა და კონტრაქტის გაფორმების სტადია. კონტრაქტის გაფორმებისას ბანკი უნდა იყოს ფრთხილად. ყველა ნიუანსი უნდა აისახოს დოკუმენტურად. კონტრაქტში დაუფიქსირებელი სიტყვიერი შეთანხმება მომწოდებელმა შეიძლება არ შეასრულოს. ბანკმა უნდა გაითვალისწინოს, რომ:

- მომწოდებელი კომპანია შეასრულებს მხოლოდ იმას, რაც კონტრაქტშია ასახული;

- კონტრაქტის გაფორმებისას გასათვალისწინებელია ყველაზე ნეგატიური სცენარიც, აქედან გამომდინარე, აუცილებელია კონტრაქტის ანალიზი;

- აუცილებელია კონტრაქტში ასახული ტერმინების ახსნა. მაგ., ადაპტაცია, საბოლოო შემუშავება, გამართვა, კონვერტირება და ა.შ. კონტრაქტში უნდა განისაზღვროს პროექტის ძირითადი სტადიები (საცდელი და სამრეწველო ექსპლუატაცია, სამომხმარებლო ტესტირება, მიღება, პროგრამული უზრუნველყოფის მოწოდება და ა. შ.). კონტრაქტში, სადაც კი ეს შესაძლებელია, უნდა ჩაირთოს მოთხოვნა, რომ კომპანია-მომწოდებლის მოქმედება შეთანხმებული იყოს ბანკთან;

- კონტრაქტში მითითებული უნდა იყოს სანქციები მომწოდებლის მხრიდან პროექტის ადაპტაციისა და დანერგვის ვადების დარღვევისთვის;

- კონტრაქტში უნდა აისახოს აგრეთვე ძველი სისტემის გაუქმების პროცედურა;

- კონტრაქტში ასევე უნდა მიეთითოს, რომ იმ შემთხვევაში, თუ პროექტის მენეჯერი არა რის საკმარისად კვალიფიცირებული ან არ შეუძლია სათანადო ურთიერთობების დამყარება ბანკის თანამშრომლებთან, ის უნდა შეიცვალოს;

- სასურველია, განისაზღვროს პროექტის ზღვრული ღირებულება და ვადები;

- კონტრაქტში უნდა ჩაიწეროს აგრეთვე დავებისა და კონფლიქტური სიტუაციების გადაწყვეტის პროცედურები;

- აღნიშნული ფაქტორების გათვალისწინება მნიშვნელოვნად შეამცირებს სისტემის არჩევის რისკებს.

კითხვები თვითშემოწმებისთვის

1. როგორ გაიანგარიშება სს-ის ფლობის მთლიანი ღირებულება?

2. რა დადებითი მხარეები გააჩნია სს-ების გარე ორგანიზაციებიდან შეძენის მოდელს?

3. რა უარყოფითი მხარეები გააჩნია სს-ების საკუთარი ძალებით შემუშავების მოდელს?

4. როგორ ხდება სს-ების შექმნის ვარიანტების შედარება?

5. როგორია სს-ების ფლობის მთლიანი ღირებულების დანახარჯების სტრუქტურა?

6. რატომ გამოიყენება ტენდერი და როგორია მისი ჩატარების თანამიმდევრობა?

თავი 11. საბანკო საინფორმაციო სისტემის თაობების განვითარება და შიქმინის ხერხები

11.1. საბანკო საინფორმაციო სისტემის თაობების განვითარება

დღეისათვის საბანკო საინფორმაციო სისტემების შემმუშავებლები, საბანკო საქმიანობის ავტომატიზაციის მიზნით კლიენტებს სთავაზობენ საინფორმაციო სისტემებს, რომლებიც უზრუნველყოფენ მათ საქმიანობას და გადავიდნენ სისტემებზე, რომლებიც დაფუძნებულია მონაცემთა ცენტრალიზებულ და შეგროვილი მონაცემების ანალიზის ინსტრუმენტებზე. წარმოებს ღრმა ანალიზი, რომელი მეთოდი უფრო მისაღებია მოცემული ბანკისთვის საინფორმაციო სისტემის საკუთარი ძალებით შემუშავება, თუ გარე ორგანიზაციის მიერ შემუშავება.

მიმდინარე პერიოდისთვის ბანკისათვის მიწოდებულ საინფორმაციო სისტემებს შეუძლიათ მუშაობა სხვადასხვა მონაცემთა ბაზების მართვის სისტემებთან, რაც ბანკებს საშუალებას აძლევს, **ფასი/მწარმოებლობა**, კრიტერიუმიდან გამომდინარე აირჩიონ მონაცემთა ბაზების მართვის სისტემები. საბანკო საინფორმაციო სისტემების შეცვლა წარმოებს ისეთი მიზეზის გამო როგორიცაა:

- კომპანია შემუშავებლისადმი უნდობლობა;
- ფინანსური ანგარიშგებების საერთაშორისო სტანდარტებზე გადასვლა;
- არადამაკმაყოფილებელი თანხლება;
- პლატფორმის მოთხოვნებთან შეუსაბამობა;
- დაბალი მწარმოებლურობა;
- კანონმდებლობის შეცვლა;
- სისტემის მოძველება;
- არასაკმარისი ფუნქციური შესაძლებლობები და სხვ.

საბანკო ინფორმაციის დამუშავების ავტომატიზაციისთვის შეიძლება გამოყენებულ იქნეს არასპეციალიზებული პროგრამული პროდუქტები. მაგ., **MS Excel**.

ბანკში საინფორმაციო სისტემების განვითარება ხდებოდა ე.წ. თაობების მიხედვით.

პირველი თაობა:

- სამუშაოების შესრულება ხდებოდა პერსონალური კომპიუტერების სისტემების გამოყენებით;
- არარსებობდა კავშირი კომპიუტერებს შორის;
- პროგრამების და მონაცემების შენახვა წარმოებდა ცალკეულ ლოკალურ კომპიუტერებზე;
- მონაცემების გაცვლა წარმოებდა მაგნიტურ მატარებლებზე ჩანერილი ინფორმაციის საშუალებების გაცვლის გზით;
- კონსოლიდირებული ანგარიშების შედგენა წარმოებდა ერთ გამოყოფილ კომპიუტერზე, ცალკეული კომპიუტერებიდან მიღებული ინფორმაციის საფუძველზე;
- არ არსებობდა ტრანზაქციის მხარდამჭერი რაიმე მექანიზმი;
- შეუძლებელი იყო ინფორმაციის მთლიანობის შენარჩუნება;
- გართულებული იყო მონაცემების არასანქცირებული წვდომისაგან დაცვა;
- ადგილი ჰქონდა საბოლოო მომხმარებლის კომპიუტერზე არსებული ინფორმაციის არალეგალურად კოპირებას და მიტაცებას.

მეორე თაობა:

- სამუშაოების შესრულება ხდებოდა პერსონალური კომპიუტერების სისტემების გამოყენებით;
- კომპიუტერები გაერთიანებული იყო ლოკალურ ქსელებში;
- დაინერგა მომხმარებლის მომსახურების „ფაილ-სერვერული სისტემა“;
- საბანკო საინფორმაციო სისტემის მომხმარებლებისთვის შეიქმნა მონაცემთა ერთიანი ფაილები;

- გამოიყენებოდა ავტომატიზაციის პროგრამული პროდუქტების ქსელური ვერსიები;
- ჯერ კიდევ არ ხდებოდა ტრანზაქციების სრული მხარდაჭერა;
- იმის გამო, რომ ფაილის მონაცემები განთავსებული იყო ერთიან სერვერზე და მოიცავდა არა მარტო კონკრეტული თანამშრომლის ინფორმაციას, არამედ სხვა თანამშრომლების ინფორმაციასაც, გართულებული იყო ინფორმაციის დაცვა არასანქცირებული შეღწევისაგან;
- ერთობლივად გამოიყენებოდა ინდექსირებული ფაილები.

მესამე თაობა:

- სამუშაოების შესრულება ხდებოდა პერსონალური კომპიუტერების სისტემების გამოყენებით;
- კომპიუტერები გაერთიანებული იყო ლოკალურ ქსელებში;
- გამოიყენებოდა ჩანაწერების მენეჯერი – *trieve*;
- მთელი სისტემის მიხედვით შეზღუდვას ადგენს ჩანაწერის მენეჯერი *trieve*;
- მონაცემებთან მუშაობა იყო დაბალ დონეზე;
- სისტემა *Novel-ში*, ტრანზაქციის კონტროლის მექანიზმი – *Transaction Tracing system (TTS)*, არ იყო ორიენტირებული ჩანაწერზე, როგორც ეს მონაცემთა ბაზების მართვის სისტემებშია, რაც ქმნიდა პრობლემებს ინფორმაციის მთლიანობის შესაძლო დარღვევების აღმოცენებაში.

მეოთხე თაობა:

- სისტემის ცენტრალურ რგოლს წარმოადგენდა მაღალმწარმოებლური დანართების სერვერი;
- გამოყენებული იყო სრულფასოვანი მონაცემთა ბაზების მართვის სისტემები;
- გამოყენებული იყო მონაცემების მანიპულირების სპეციალური ენები, მაგ., როგორიცაა *SQL*;
- სრულად იყო რეალიზებული ტრანზაქციის მექანიზმი;

- მონაცემების მართვის სისტემის ბირთვის დონეზე, მართვის მთლიანობის მხარდაჭერა უზრუნველყოფდა მონაცემების არანინალმდეგობრიობას;
- მონაცემებთან წვდომის უფლებები იყო შეზღუდული;
- დაპროექტების ავტომატიზაციის საშუალებების გამოჩენა სისტემების შემუშავებლებს სისტემის ფუნქციონირების დონეზე აძლევდა კონცენტრაციის საშუალებას;
- გამოყოფილი სერვერის დანართის საფუძველზე, დიდი იყო სისტემის მწარმოებლურობა;
- მაღალი იყო საბანკო საინფორმაციო სისტემების დაცულობა და უსაფრთხოება;
- მონაცემების რეზერვირების ჩაშენებული მექანიზმი აიოლებდა მონაცემების კოპირების ამოცანას;
- არ ხდებოდა მონაცემთა ბაზების მართვის სისტემის მონაცემებთან პირდაპირი წვდომა. წვდომა ხორციელდებოდა გამოყენებითი ინტერფეისის მეშვეობით.

მეხუთე თაობა:

- განაწილებული მონაცემთა ბაზების გამოყენება იძლევა მონაცემების ერთიან ბაზაში დამუშავების საშუალებას;
 - კლიენტის დანართისთვის მნიშვნელობა არ აქვს, ფიზიკურად სად იმყოფება მონაცემები;
 - მრავალმომხმარებლიანი ოპტიმიზებული სამუშაო რეჟიმი იძლევა, მონაცემების განვითარებული ტრანზაქციის საშუალებას;
 - შესაძლებელია საბანკო საინფორმაციო სისტემებში ნებისმიერი პლატფორმის გამოყენება.
- საბანკო საქმიანობის ავტომატიზაციის პრაქტიკაში არ არსებობს ბანკის საინფორმაციო სისტემის რომელიმე სტანდარტი, რომლის გამოყენებაც შესაძლებელია ყველა ბანკში. აღნიშნული დამოკიდებულება რიგ ფაქტორებზე:
- მთლიანად ბანკის ორგანიზაციულ სტრუქტურაზე და იმ განყოფილებებზე, რომელთა ავტომატიზაცია უნდა განხორციელდეს;

- ბანკის შიგნით საქმიანობის არსებულ გარემოსა და ბანკის თანამშრომლების საერთო მიზნებით დაინტერესებაზე;
- მართვის პერსონალის აქტიურობასა ან პასიურობაზე;
- ბანკის პერსონალის მომზადების დონეზე, შესასრულებელი ტექნოლოგიური ოპერაციების ცოდნასა და თანამშრომლების კომპიუტერული განათლების დონეზე;
- ბანკში არსებული ინფორმაციული ტექნოლოგიების ინფრასტრუქტურაზე;
- ბანკის ხელმძღვანელობის მზაობაზე, შეიძინოს საჭირო ტექნიკური და პროგრამული საშუალებები.

11.2. საბანკო საინფორმაციო სისტემის შექმნის ხერხები

შეძენილ საინფორმაციო სისტემას გააჩნია როგორც დადებითი, ისე უარყოფითი მხარეები.

დადებითი მხარეები:

- ბანკი მაშინვე ღებულობს შემომწებულ პროგრამას, შესაბამის დოკუმენტებთან ერთად;
- მხარდაჭერა და თანხლება ხორციელდება შემმუშავებელი კომპანიის მიერ, რაც უზრუნველყოფს სამუშაოების ხარისხიან შესრულებას;
- შემმუშავებელ კომპანიას დიდი გამოცდილება გააჩნია სხვა ბანკებში შემოთავაზებული საინფორმაციო სისტემების დანერგვის, რაც იძლევა გარანტიას, რომ გარე სპეციალიზებული ორგანიზაციის მიერ შემმუშავებული საინფორმაციო სისტემა იქნება მაღალი ხარისხის და კონკურენტუნარიანი;
- სისტემის განახლების თაობაზე ბანკი შემმუშავებლისგან ღებულობს გარანტიას;
- საინფორმაციო სისტემის შემუშავება და დანერგვა შეძენილ საინფორმაციო სისტემის მეშვეობით საკუთარი ძალებით, შემუშავებასთან შედარებით, მცირე დროს საჭიროებს.

უარყოფითი მხარეებია:

- ერთჯერადი კაპიტალური დანახარჯების დიდი მოცულობა;
- შემოთავაზებული ინფორმაციული ტექნოლოგიები შეიძლება წინააღმდეგობაში მოვიდეს არსებულთან, რაც გარკვეულ უთანხმოებას იწვევს კოლექტივში;
- ვინაიდან საინფორმაციო სისტემის დანერგვა ხორციელდება ინტენსიურად მოკლე დროის განმავლობაში, საჭირო ხდება სპეციალისტების ოპერატიული გადამზადება;
- თუ საჭირო გახდა ცვლილებების შეტანა შემუშავებულ საინფორმაციო სისტემაში, ეს შემუშავებული კომპანიის მხრიდან გამოიწვევს ხარჯების გაზრდას;
- ვინაიდან შემოთავაზებული სისტემა ტირაჟირებადია, ბანკს არ ექნება რაიმე უპირატესობა სხვა კონკურენტებთან შედარებით;
- ვინაიდან შემოთავაზებული სისტემა არ წარმოადგენს ბანკის საკუთრებას, ამიტომ ბანკის გაფართოვების შემთხვევაში მას მოუწევს მისი თავიდან შეძენა

საკუთარი ძალებით საინფორმაციო სისტემის შემუშავება.

დადებითი მხარეები:

- ბანკის თანამშრომლები ღებულობენ ისეთ სისტემას, როგორიც მათ სურთ;
- ბანკი არ არის დამოკიდებული გარე კომპანიაზე და ბაზარზე მის მდგომარეობაზე;
- სისტემის ბოლომდე შემუშავება შესაძლებელია საკუთარი ძალებით ან კონსალტინგის გზით, რაც ბანკს სისტემის მუდმივად განვითარებისა და სრულყოფის საშუალებას აძლევს;
- არ საჭიროებს ადაპტაციის პერიოდს;
- ერთჯერადად გასაღები ხარჯების მოცულობა შეიძლება არ იყოს დიდი;

- ბანკის ინფორმაციზაციის სპეციალისტები ყოველთვის იმყოფებიან ადგილზე და შეუძლიათ დახმარება აღმოუჩინონ ბანკის თანამშრომლებს;

- ბანკის ინფორმაციზაციის სპეციალისტებმა კარგად იციან ბანკის სპეციფიკა.

უარყოფითი მხარეები:

- ავტომატიზაციის თითოეული ფუნქციისთვის საჭიროა ტექნიკური დავალების შედგენა;

- ბანკში უნდა შეიქმნას სპეციალური ჯგუფი, რომელმაც უნდა უზრუნველყოს ისეთი სისტემის შემუშავება, რომელიც ხელს შეუწყობს მმართველობითი გადაწყვეტილებების შემუშავებასა და რეალიზებას;

- საინფორმაციო სისტემის შემუშავებისა და დანერგვის დრო გაცილებით დიდია, ვიდრე გარე შემსრულებლის შემთხვევაში;

- შემუშავებული საინფორმაციო სისტემის ფლობის მთლიანი ღირებულება შეიძლება მეტი ან ტოლი აღმოჩნდეს შეძენილთან შედარებით;

- პრობლემები შეექმნება ბანკს, თუ დამპროექტებელთა ჯგუფი დაიშალა ან მისი ხელმძღვანელი (მთავარი პროგრამისტი) წავიდა ბანკიდან;

- არ არის გამორიცხული, რომ საკუთარი ძალებით საინფორმაციო სისტემის შემუშავება მიყვანილი იქნება ბოლომდე და პროექტი იქნება დასრულებული;

- შეუძლებელი ხდება სახელმწიფო ორგანოების მიერ მოთხოვნების დროული ასახვა შემუშავებულ პროექტში;

- შემუშავებული საინფორმაციო სისტემის ხარისხი დაბალია გარე ორგანიზაციის მიერ შემუშავებულ სისტემასთან შედარებით, რაც გამოწვეულია საკუთარი სპეციალისტების არასაკმარისი ცოდნითა და გამოცდილებით.

საინფორმაციო სისტემის ბაზური ნაწილის შეძენა.

აღნიშნულ მეთოდს გააჩნია შემდეგი დადებითი მხარეები:

- სისტემის ბირთვი მზადაა და ტესტირებულია,
- შეიძლება მისი შეძენა და გამოყენება;
- მზა სისტემისა და არსებულ მონაცემთა ბაზების ფარგლებში შესაძლებელია პრინციპულად ახალი დანართების შემუშავება;
- საკუთარი ძალებით საინფორმაციო სისტემის შემუშავების ფოკუსირება წარმოებს არა საბაზისო ფუნქციებზე, არამედ ბიზნესის თავისებურებების გათვალისწინებით.

**შემოთავაზებულ მეთოდს გააჩნია
უარყოფითი მხარეები:**

- ახალი დანართების შემუშავება შეზღუდულია შეძენილი საინფორმაციო სისტემის ბირთვის ჩარჩოთი;
- საჭიროა განისაზღვროს ის საკითხები, რომლებიც პრინციპულ ზეგავლენას იქონიებს ბანკის საერთო საქმიანობაზე. კერძოდ, ბაზარზე ბანკის კონკურენტიანობაზე.

საჭიროა პასუხის გაცემა შემდეგ კითხვებზე:

- როგორი ტექნოლოგია უნდა იქნეს გამოყენებული ინფორმაციის შესანახად და გამოსაყენებლად;
- შესაძლებელია თუ არა კლიენტების მომსახურება ფილიალების გარეშე;
- როგორ შეიძლება ბანკის საქმიანობის გაანალიზება;
- როგორი მოცულობისა და მასშტაბის იქნება შესაგროვებელი ინფორმაცია და რა მოთხოვნები წაყენება მონაცემთა ბაზების მართვის სისტემას.

ბანკის მთლიანი ავტომატიზაციის შესაძლო ორგანიზაცია

აღნიშნული განვიხილოთ საბანკო საინფორმაციო სისტემის ბოლო თაობის მაგალითზე.

პროგრამულ-ტექნიკური საშუალებების ტექნოლოგიის ორგანიზაცია დამყარებული იქნება ყველა მომხმარებლის მიერ ერთიანი მონაცემთა ბაზით სარგებლობაზე.

ბანკის მთლიანი ავტომატიზაციის შესაძლო ორგანიზაციისათვის საჭიროა:

- ამ ვარიანტით სარგებლობისას ყველა პროცესის შესრულება უნდა მოხდეს ერთიანი მონაცემთა ბაზის მართვის სისტემის გამოყენებით;
- აღნიშნული ვარიანტის მიხედვით, მთელი ინფორმაცია უნდა განთავსდეს მონაცემთა ბაზების ცენტრალურ სერვერზე;
- უნდა იყოს შესაძლებელი ცენტრალური ბაზის რეპლიკაცია დამხმარე და სარეზერვო სერვერებზე.

აღნიშნულის შესრულების შემდეგ:

- გაიოლდება ყველა ქვეგანყოფილების მართვის ორგანიზება;
- გაიოლდება მონაცემთა ბაზების მართვის სისტემის სერვერის მომსახურება;
- დაშორებულ ქვეგანყოფილებებს არ ექნებათ კომერციული სახის ინფორმაცია;
- დაშორებულ ქვეგანყოფილებებს არ დასჭირდებათ მომსახურება;
- ბანკის ყველა ოპერაციის შესრულება შესაძლებელი გახდება ონლაინრეჟიმში;
- შეიქმნება კლიენტების ერთიანი ბაზა. ადგილი არ ექნება არასაჭირო ანგარიშების დუბლირებას.

განხილულ ვარიანტს გააჩნია უარყოფითი მხარეები:

- მაღალია მოწყობილობების შეძენისა და პროგრამული უზრუნველყოფის დაყენების საწყისი ღირებულება;

- მთელი კვირის განმავლობაში უზრუნველყოფილი უნდა იყოს სერვერის 24-საათიანი შეუფერხებელი მუშაობა;

- უზრუნველყოფილი უნდა იყოს საკომუნიკაციო ქსელის შეუფერხებელი მუშაობა;

- საინფორმაციო სისტემამ ხელი უნდა შეუწყოს ბანკს, იმუშაოს სხვადასხვა დროით ზონაში.

თუ ბანკს არ გააჩნია საკომუნიკაციო სისტემების ნორმალურად ფუნქციონირების ხარჯები, იგი თანახმაა, გარკვეული თანხები ჩადოს სისტემის ექსპლუატაციის პროცესების განსახორციელებლად. შესაძლებელია აგრეთვე ბანკის რეგიონული ოფისების გამოთვლითი ცენტრების აღჭურვა შედარებით ნაკლები სიმძლავრის ტექნიკური საშუალებებით, ცენტრალური ოფისის ტექნიკურ საშუალებებთან შედარებით. ამ შემთხვევაში ადგილი აქვს ინფორმაციის განაწილებულ შენახვას და გადაამუშავებას. რეგიონულ ოფისების გამოთვლით ცენტრებში ინახება მთავარი ოფისის მთელი ინფორმაციის ასლი.

ასევე შესაძლებელია, რეგიონულ ოფისების მონაცემთა ბაზების მართვის სისტემებში ნორმატიულ-საცნობარო და ბიზნესის შესახებ მთლიანი ინფორმაცია შენახვა. მაგ., კლიენტების ბარათები და მათი ანგარიშების ნაშთის შესახებ ინფორმაცია, რეგიონულ და მოთავე ოფისებში შესრულებული ოპერაციების დეტალიზებული ინფორმაციის გარეშე. ცენტრალურ სერვერს გადაეცემა რეგიონულ ოფისში შესრულებული ოპერაციების შესახებ დეტალური ინფორმაცია, ან კონსოლიდირებული ანგარიშგებების მისაღებად საშუალო ინფორმაცია.

აღნიშნულ ვარიანტს გააჩნია შემდეგი დადებითი თვისებები:

- მთელი სისტემის მაღალი საიმედოობა და დაცვა (რამდენიმე სერვერზე ინახება ერთი და იმავე მონაცემების ასლები);

- საკომუნიკაციო საშუალებებს რეპლიკაციისთვის წაყენება ნაკლები მოთხოვნები, ვიდრე ონლაინრეჟიმში ინფორმაციის გაცვლისას;

- ინფორმაციის განაწილებული დამუშავების ორგანიზების შესაძლებლობა (რეგიონულ სერვერზე ახლად გახსნილი მეანობ-რეების ანგარიშების მიხედვით პროცენტების გაანგარიშება და მოთავე ორგანიზაციაში შედეგების გადაცემა);

- მცირდება პირველადი კაპიტალდაბანდებების მოცულობა (კერძოდ, კავშირის არხებისთვის).

უარყოფითი მხარეებია:

- ექსპლუატაციის მაღალი ღირებულება წინა ვარიანტთან შედარებით;

- როგორც მთავარი, ისე რეგიონული ოფისების მომსახუ-რების აუცილებლობა;

- 24X7 დროის განმავლობაში რეგიონული გამოთვლითი ცენტრების შეუფერხებელი მუშაობისთვის საჭირო ხარჯები;

- მასშტაბების გაზრდის შემთხვევაში იზრდება პროგრამულ უზრუნველყოფაზე განეული დანახარჯები.

კითხვები თვითშემოწმებისთვის

1. დაახასიათეთ ბანკის სს-ების თაობები.

2. რა დადებითი მხარეები გააჩნია სს-ების გარე ორგანი-ზაციებიდან შეძენის მოდელს?

3. რა უარყოფითი მხარეები გააჩნია სს-ების გარე ორგა-ნიზაციებიდან შეძენის მოდელს?

4. რა დადებითი მხარეები გააჩნია საკუთარი ძალებით საინ-ფორმაციო სისტემის შემუშავებას?

5. რა უარყოფითი მხარეები გააჩნია სს-ების საკუთარი ძა-ლებით შემუშავების მოდელს?

6. რა დადებითი მხარეები გააჩნია საინფორმაციო სისტემის ბაზური ნაწილის შეძენას?

7. რა უარყოფითი მხარეები გააჩნია საინფორმაციო სის-ტემის ბაზური ნაწილის შეძენას?

თავი 12. საბანკო საინფორმაციო სისტემების შემფუძვანელი კომპანიების დახასიათება

12.1. ავტომატიზებული საბანკო საინფორმაციო სისტემის სტრუქტურა

საბანკო სისტემების ფუნქციების გაფართოება დაკავშირებულია ქვეყანაში საბანკო საქმიანობის განვითარების თავისებურებაზე. თუ იზრდება ბანკის სხვადასხვა მომსახურებებზე მოთხოვნები, მაშინ ავტომატიზებული საბანკო სისტემების ბაზარზე ჩნდება ახალი საბანკო დანართები, საბანკო ტექნოლოგიების ახალი სახეები.

ავტომატიზებული საბანკო სისტემის საბაზო კომპლექტი საშუალებას იძლევა, მოემსახუროს კლიენტებს ფართო სპექტრით. სისტემის ძირითადი ფუნქციური მოდულები ახდენენ შემდეგი ამოცანების რეალიზებას:

- იურიდიული პირების საანგარიშსწორებო-საკასო მომსახურება;
- ბანკ-კორესპონდენტის ანგარიშების მომსახურება;
- კერძო პირების ნებისმიერი ანაბრის და მათზე შესრულებული ოპერაციების საკრედიტო, სადეპოზიტო და სავალუტო მომსახურება;
- საფონდო ოპერაციები;
- ანგარიშსწორება პლასტიკური ბარათების გამოყენებით;
- საბუღალტრო აღრიცხვის ფუნქციები;
- ანალიზი, გადანყვეტილების მიღება, მენეჯმენტი, მარკეტინგი და ა. შ.

მეოთხე თაობის ავტომატიზებული საბანკო საინფორმაციო სისტემები დაფუძნებულია „კლიენტ-სერვერულ“ ტექნოლოგიაზე და იყენებს აგებისა და ფუნქციონირების ერთიან პრინციპებს.

უკანასკნელ პერიოდში დიდ ყურადღებას უთმობენ ფინანსური ანალიზის და ბიზნესის მართვის საკითხებს. სათანადო დონეზე ჯერ-ჯერობით არ არის ფინანსური რისკების კონტროლის

სისტემები, რესურსების მართვის ოპერაციების მომგებიანობის ანალიზი.

ბანკში საინფორმაციო სისტემის შექმნა დამოკიდებულია ბანკში დასამუშავებელი ინფორმაციის მოცულობაზე, შესრულებული ოპერაციების რაოდენობასა და ბანკის მოთხოვნებზე, გაიმარჯვოს კონკურენტულ ბრძოლაში. ბანკის საინფორმაციო სისტემის აგება უნდა ეფუძნებოდეს შემდეგ პრინციპებს: კომპლექსურობის, ეკონომიკური ეფექტიანობის და მოდულობის. კომპლექსურობის პრინციპი გულისხმობს, რომ ბანკში გადასაწყვეტი ყველა ამოცანა ერთმანეთთან უნდა იყოს დაკავშირებული, რაც თავიდან აგვაცილებს ინფორმაციის დუბლირებას. ბანკში ინფორმაციული ტექნოლოგიების აგება და, შესაბამისად, საინფორმაციო სისტემის შემუშავება უნდა განხორციელდეს მოდულური პრინციპით. ბანკში მოდულების გამოყოფა უნდა წარმოებდეს შესრულებული ფუნქციების საფუძველზე. მაგ., სალაროსა და სააღრიცხვო ოპერაციების მოდული, ფასიანი ქაღალდების საბირჟო ოპერაციათა აღრიცხვის მოდული. ტექნოლოგიების აგება შესაძლებელია ობიექტების მიხედვით. ამ შემთხვევაში გამოყოფენ: მთავარი ოფისის, ფილიალების, განყოფილებების და წარმომადგენლობის მოდულებს.

გარდა ზემოთ მითითებული მოდულებისა, ფუნქციური დანიშნულების მიხედვით შეიძლება შემუშავდეს შემდეგი მოდულები: კრედიტების დისტანციური მომსახურების, **S.W.I.F.T.**-ის საშუალებით შესრულებული ოპერაციების, კლიენტების დისტანციური მომსახურების, დეპოზიტების აღრიცხვის, კომერციული კრედიტების აღრიცხვის, პლასტიკურ ბარათებთან მუშაობის, ფასიანი ქაღალდებით არასაბირჟო ვაჭრობის და სხვ.

12.2. საბანკო საინფორმაციო სისტემების შემუშავებელი კომპანიების დახასიათება

კომპანია „Диасофт“. კომპანია „Диасофт“ საფინანსო ორგანიზაციებისთვის პროგრამული უზრუნველყოფის შემუშავებასა და დანერგვაში ლიდერი და მსხვილ მიმწოდებელია. 1991 წლიდან მუშაობს რუსეთის საბანკო ბაზარზე. კომპანია ქმნის კორპორა-

ციული და საცალო მომსახურების, საფინანსო ბაზარზე ოპერაციების, სამეურნეო საქმიანობის მართვის კომპლექსური ავტომატიზაციის სისტემებს. ის ახდენს მსხვილი საფინანსო სტრუქტურების ბიზნესის, სადაზღვევო კომპანიების, სახელმწიფო საპენსიო ფონდების მართვის საინფორმაციო-ანალიზური სისტემების შემუშავებას.

კომპანიის ძირითად საქმიანობაში შედის: საწარმოებისა და ორგანიზაციების კომპლექსური ავტომატიზაცია; ინფორმაციული ტექნოლოგიების კონსალტინგი; მაღალმწარმოებლური ტექნიკური საშუალებებისა და პროგრამული უზრუნველყოფის მიწოდება.

ის არის ფინანსური ბაზრის ყველა მიმართულების ინფორმაციული ტექნოლოგიების დარგში ინფორმაციული გადაწყვეტილებების მიმწოდებელი. კომპანიაში დასაქმებულია 1600-მდე თანამშრომელი. გააჩნია 300-ზე მეტი კლიენტ-ფინანსური ორგანიზაცია. მათ შორის 55 რუსეთის ბანკია.

კომპანია „**Диасофт**“ ერთ-ერთი პირველი საბანკო პროგრამული უზრუნველყოფის შემმუშავებელია, რომელიც შეყვანილია **Leades ანგარიშში Magic Quadrant for International Retail Core Bankkind Systems Garter-ის** კომპანიაში. გააჩნია საერთაშორისო სერთიფიკატი **CMMI for gevelopment level**, შეყვანილია ინფორმაციული ტექნოლოგიების კომპანიების **Software 500-ის** რეიტინგში. დღეისათვის ბანკის საინფორმაციო სისტემების ბაზარზე წამყვანი პოზიციები უკავიათ შემდეგი ფირმების შემუშავებულ საინფორმაციო სისტემებს: „**Диасофт**“ – 31%, „**R-Stile**“ – 26%, „**ПрограмБанк**“ – 10%.

„**Диасофт**“-ი უზრუნველყოფს:

- ფუნქციურ სიახლეს – ადვილად წარმოებს ბანკის ახალი მოთხოვნების დაკმაყოფილება, რადგან გააჩნია ახალი მოდულების შემუშავების საკუთარი ინსტრუმენტარი;

- მასშტაბურობას – სისტემის უნარს მოახდინოს ადაპტირება, გაფართოება მოთხოვნებისა და გადასაწყვეტი ამოცანების რაოდენობის გაზრდის შემთხვევაში: ავტომატიზებული სამუ-

შაოა ადგილებისა და დასამუშავებელი დოკუმენტების რაოდენობა;

- კომპლექსურ მიდგომას – კომპლექსური საინფორმაციო სისტემების არსებობა, რომელიც ხელს უწყობს ბანკის სხვადასხვა საქმიანობის ინტეგრაციას;

- სისტემის გამართულობას – მობილურობა და დინამიურობა. სისტემის ზოგიერთი პარამეტრი შეიძლება ადაპტირებული იქნეს კონკრეტული ბანკის მოთხოვნებთან და პირობებთან;

- სისტემის ცენტრალური მართვას – რაც გულისხმობს სისტემის ფუნქციონირების გამართვას საბოლოო მომხმარებლის არა სამუშაო ადგილიდან, არამედ ერთ-ერთი სპეციალური მოდულის საშუალებით;

- მუშაობა რეალური დროის რეჟიმში – სისტემის რეაქცია მმართველ ზემოქმედებაზე შეესაბამება პროცესის მიმდინარეობის სისწრაფეს;

- უსაფრთხოებას – ინფორმაციასთან წვდომის უფლების დაყოფა და დოკუმენტებთან შეღწევის უფლების შეცვლა მისი სიცოცხლის პროცესში.

კომპანია „Диасофт“-ის მიერ შემუშავებული საბანკო საინფორმაციო სისტემა მოიცავს შემდეგ ქვესისტემებს:

- საბალანსო დოკუმენტები;
- სალაროს დოკუმენტები;
- ბანკთაშორისი დოკუმენტები;
- არასაბალანსო დოკუმენტები;
- ვალუტაშორისი დოკუმენტები;
- ბანკთაშორისი ოპერაციები;
- ბანკის ოპერაციები;
- ანგარიშთა გეგმა;
- ბანკის ანგარიშგებები და ანგარიშგებების გენერატორი;
- ბანკის კლიენტები;

კომპანია R-stile. კომპანია **R-stile** წარმოადგენს რუსეთის სისტემურ ინტეგრატორს და მიმწოდებელს კორპორაციული ინფორმაციული გადანაცვეტილებების შემუშავებაში. შეიქმნა

1991 წელს. მისი ფილიალები განთავსებულია რუსეთის ფედერაციის მრავალ ქალაქსა და ოლქში. ეწევა შემდეგი სახის მომსახურებას:

- საწარმოებისა და ორგანიზაციების კომპლექსური ავტომატიზაცია;
- ინფორმაციული ტექნოლოგიების და ბიზნეს პროცესების კონსალტინგი;
- სერვისის მხარდაჭერა და აუტსორსინგი;
- ინფორმაციული ტექნოლოგიების სფეროში პროექტების მართვა;
- ბიზნესსისტემების დანერგვა;
- ინფორმაციული უსაფრთხოების სისტემების შემუშავება და დანერგვა;
- მაღალტექნოლოგიური მოწყობილობებისა და პროგრამული უზრუნველყოფის მიწოდება;
- ინფრასტრუქტურული ინტეგრაცია;
- ტელესაკომუნიკაციო მომსახურება;
- ინფორმაციული ტექნოლოგიების სფეროში კადრების მომზადება;
- სხვა ინფორმაციული ტექნოლოგიების მომსახურება.

R-style Softlab რუსეთის საბანკო საინფორმაციო სისტემების შემუშავებაში ლიდერია, რომლის მიერ შემუშავებული პროგრამული უზრუნველყოფა გამოიყენება რუსეთის ფედერაციული რესპუბლიკის ყოველ მესამე ბანკში. მის მიერ შემუშავებულ საბანკო პროდუქტებს მიეკუთვნება: **ABCRS-Bank pervasive, SQL, Oracle** და სხვ. ნებისმიერი ყველა ტექნოლოგიური რგოლის კომპლექსურ ავტომატიზაცია. **RS-DataHouse** საინფორმაციო ანალიზური სისტემაა, ემყარება მონაცემთა ცენტრალიზებულ საცავს და რომელიც მოიცავს როგორც დინამიკურ, ისე სტატიკურ ანალიზის საშუალებებს. მის მიერ შემუშავებული **InterBank** სისტემა მომსახურებას უწევს როგორც იურიდიულ, ისე ფიზიკურ პირებს.

R-stile Softlab-ის მიერ შემუშავებულია საბანკო საინფორმაციო სისტემების შემდეგი პროგრამული უზრუნველყოფა:

- **RS-Retail** – საცალო მომსახურების კომპლექსური ავტომატიზაციის სისტემა;

- **RS-loans** – იურიდიული და ფიზიკური პირების დაკრედიტების პროცესების ავტომატიზაცია;

- **RS-Incounting** - ბანკის სამეურნეო საქმიანობის ავტომატიზაცია;

- **RS-Payments** გადახდების განხორციელების ავტომატიზებული სისტემა.

R-stile Softlab კომპანიაში დასაქმებულია ათასამდე მაღალკვალიფიცირებული თანამშრომელი.

კომპანია „ПрограмБанк“. კომპანია „ПрограмБанк“ შეიქმნა 1989 წელს, როგორც სამეურნეო ანგარიშზე მყოფი მოსკოვის ბანკების კავშირის საწარმო. ბანკების საინფორმაციო სისტემების შემუშავებში მას ერთ-ერთი წამყვანი ადგილი უკავია. „ПрограмБанк“-ის მუშაობა პირდაპირ კავშირშია საბანკო სისტემის შემუშავებასა და განვითარებასთან. მისი შვილობილი კომპანიაა „Новая-Афина“, ლიდერი საბანკო სეგმენტში. იგი რამდენიმე ათეული წელია ეწევა საბანკო საინფორმაციო სისტემების ტექნოლოგიების შემუშავებას. ინფორმაციული ტექნოლოგიების დანერგვის მიმართულებით, ემსახურება 200-ზე მეტ ორგანიზაციას. როგორც ზემოთ აღვნიშნეთ, ბანკის საინფორმაციო სისტემების ბაზარზე გარკვეული წარმატება აქვს ფირმა – „ПрограмБанк“-ს, რომლის მიერ შემუშავებულია საბანკო საქმიანობის ავტომატიზაციის ორი მოდული: „Центавр Дельта“ და „Гефест“.

კომპანია „Инверсия“. კომპანია „Инверсия“ შეიქმნა 1990 წელს. მის მიერ შემუშავებული ბანკის საქმიანობის ავტომატიზაციის პროგრამული უზრუნველყოფა მოიცავს:

- 1) ცენტრალიზებულ ავტომატიზებულ საბანკო სისტემას – „БАНК21-БЕК“;

2) ფაქტორინგული ბიზნესის ავტომატიზაციის სისტემას - „**Факторинг**“;

3) კლიენტების აღრიცხვის ავტომატიზაციის სისტემა - „**Бизнес Досье**“;

4) ფიზიკური პირების დაკრედიტების ავტომატიზაციის სისტემა - „**Involan**“;

5) კლასიკური ბანკ-კლიენტი სისტემას „**CBSAQ**“.

6) სისტემას ინტერნეტბანკინგი ფიზიკური და იურიდიული პირებისთვის - „**CBSNT**“;

7) ფულადი საშუალებების სწრაფი გზავნილების სისტემა - „**INVOPAY**“;

8) მონაცემთა საგნობრივ-ორიენტირებულ საცავს - „**Интеллектуальный Банк**“ და სხვ.

განვიხილოთ ფირმა „**Инверсия**“-ს მიერ შემუშავებული ავტომატიზებული საბანკო საინფორმაციო სისტემის ძირითადი ქვესისტემები.

ბანკის „ოპერაციული დღე“, როგორც პროგრამულ-ტექნოლოგიური კომპლექსი, უზრუნველყოფს შრომატევადი საბანკო ოპერაციების აღრიცხვის ავტომატიზაციას. კლიენტების პირადი ანგარიშების მიხედვით, ყველა ოპერაციის განხორციელება წარმოებს საგადამხდელო დოკუმენტების საფუძველზე. სისტემა უზრუნველყოფს ფულადი საშუალებების ფაქტობრივი და გეგმური მოძრაობის კომპლექსურ რეალიზაციას. პირადი ანგარიშების მიხედვით დოკუმენტები კონტროლდება და, შეცდომების არარსებობის შემთხვევაში, დგება ჩამონათვალი, ფორმირდება საანგარიშსწორებო-საკასო ცენტრში გასაგზავნი ფაილი. სალაროს დოკუმენტების მოძრაობას გააჩნია თავისებურებები, რომელთა შორის მთავარია ბანკის სხვა სამსახურებთან კავშირი.

ბანკის კომპლექსს „ოპერაციული დღე“ გააჩნია მულტივალუტური თვისება. ფილიალების საქმიანობის აღრიცხვის კომპლექსის დანიშნულებაა ბუღალტერიაში სამუშაო ადგილებისა და ფილიალების სხვა განყოფილებების მუშაობის ავტომატიზაცია. „ბანკ-ფილიალების“ დონეზე ავტომატიზაცია ხდება ფილი-

აღებიდან შემოსული ინფორმაციის შეგროვების, დამუშავების და ანალიზის საფუძველზე. ფილიალთა ურთიერთქმედებების ორგანიზება წარმოებს პირდაპირ, ცენტრალური ბანკის განყოფილების მეშვეობით. ფილიალების ფარგლებში კომპლექსი მოიცავს სავალუტო და სალაროს ოპერაციებს. ფილიალების მიხედვით წარმოებს ბალანსის გაანგარიშება.

ხელშეკრულებების ქვესისტემა მუშაობს საკრედიტო, სადეპოზიტო და ბანკთაშორის ოპერაციებზე, ახორციელებს სავალუტო დილინგს. ხელშეკრულების ჟურნალში აისახება მონაცემები მიმდინარე, დამთავრებული, ვადაგადაცილებული და იმ ხელშეკრულებების შესახებ, რომელთა გადახდის ვადაც დადგა.

ფირმა „**ინვერსიის**“ პროგრამულ-ტექნიკური კომპლექსით – ფირმის დეპოზიტები, რეალიზდება შემდეგი ფუნქციები:

1. კლიენტების სიების ფორმირება და მათი ტიპის განსაზღვრა (ინვესტორი, დილერი, ემიტენტი დეპოზიტორი, საცავი).
2. დეპოზიტორების საბალანსო ანგარიშების და ანგარიშგებების ფორმირება.
3. ფასიანი ქაღალდების გამოშვება.
4. ფასიან ქაღალდებზე ოპერაციების (მიღება, აღრიცხვიდან მოხსნა, მფლობელისა და შენახვის ადგილის ცვლილების ასახვა. დეპონანგარიშის მიხედვით ამონაწერი) შესრულება.
5. ოპერაციების კატალოგის წარმოება, ფასიანი ქაღალდების განთავსება.
6. კრებსითი ანგარიშგებების მომზადება.

ფირმა „**Инверсия**“-ს მიერ შემუშავებული პროგრამულ-ტექნოლოგიური კომპლექსი „საბირჟო ოპერაციები“ ახორციელებს ვალუტის ყიდვა-გაყიდვის შესახებ კონტრაქტებისა და განაცხადების რეგისტრაციის ავტომატიზაციას; სავალუტო გადახდებისა და მაჩვენებლების კონტროლსა და ანალიზს; ვალუტით ვაჭრობის სტატისტიკას, ანგარიშგებითი ფორმების გენერაციას.

კომპლექსი „ოპერაციები სახელმწიფო მოკლევადიანი ობლიგაციების ბაზარზე“ უზრუნველყოფას უკეთებს შემდეგი ფუნქციების რეალიზებას:

- ფასიანი ქაღალდების შემოსავლიანობის ანალიზი. ბანკი დილერის, მისი კლიენტებისა და ფილიალებისათვის ანგარიშდევოს შექმნა;
- ფასიანი ქაღალდების შესყიდვა-გაყიდვის ოპერაციების აღრიცხვა, ოპერაციების მიხედვით საკომისიოსა და გადასახადების აღრიცხვა;
- ვაჭრობის შედეგების მიხედვით ფასიანი ქაღალდების პორტფელის გადაფასება;
- ბანკისა და მისი კლიენტების შემოსავლების გაანგარიშება;
- გატარებებისა და ოპერაციების ჟურნალის ფორმირება, მიღება, ანგარიშების ამონაწერების გაკეთება სხვადასხვა მაჩვენებლების მიხედვით.

ავტომატიზებული საბანკო საინფორმაციო სისტემის ყველაზე გავრცელებული ქვესისტემებია: კლიენტ-ბანკი, მუშაობა პლასტიკურ ბარათებთან, ვალუტის გაცვლის პუნქტების ოპერაციები.

ფირმა „Инверсия“-ს მიერ შემუშავებული კლიენტ-ბანკის პროგრამულ-ტექნოლოგიური კომპლექსი შედგება შემდეგი მოდულებისაგან: „ბანკი“ და „კლიენტი“, რომელთა დაყენება წარმოებს ბანკისა და კლიენტის პერსონალურ კომპიუტერზე, რაც კლიენტს აძლევს, შესაძლებლობას თავისი სამუშაო ადგილიდან (ოფისიდან) განახორციელოს სტანდარტული საბანკო ოპერაციები. კომპლექსი ასრულებს საგადამხდელო დოკუმენტების გაგზავნისა და მიღების ფუნქციებს, ანგარიშების მიხედვით ამონაწერის მიღებას, ვალუტის ყიდვა-გაყიდვის შეკვეთებს, ოპერაციებს ფასიან ქაღალდებზე.

კლიენტების მომსახურების ეფექტური ფორმაა პლასტიკური ბარათების გამოყენება.

კომპანია „Кворум“-ი. კომპანია „Кворум“-ი – საბანკო საინფორმაციო სისტემების და საბანკო სექტორისთვის სპეციალიზებული პროდუქტების შემმუშავებელია. 2006 წლის სექტემბრიდან გაერთიანებულია „Компьюлинк“-ი კომპანიების ჯგუფში, არის რუსეთის ბანკების ასოციაციის წევრი და მსოფლიოს წამყვანი ვენდორების – **Oracle (Certified Partner)** და **IBM-ის (advanced Business Partner)** სერტიფიცირებულ პარტნიორი.

კომპანიის მისიაა საწარმოებისათვის ძირითადი ბიზნეს პროცესების ავტომატიზაციის კორპორაციული საინფორმაციო სისტემების შემუშავება, დანერგვა და თანხლება. კომპანიის კლიენტებია სახელმწიფო და კომერციული ორგანიზაციები. კომპანიის ძირითადი კომპონენტებია:

1. საბანკო ტექნოლოგიების, წინასაპროექტო გამოკვლევების ჩატარების მეთოდების და დაკვეთების მთლიანი სამუშაო ციკლის ექსპერტიზა.
2. ავტომატიზებული საბანკო სისტემების, გადავადების საინფორმაციო სისტემების შემუშავება და დანერგვა, რომელთა ანალოგები საინფორმაციო სისტემების ბაზარზე არ არსებობს.

„**Кворум**“-ის მიერ შემუშავებულ ინტეგრირებული გადაწყვეტილების პროექტებს საფუძვლად უდევს შემდეგი ტექნოლოგიები: კორპორაციული პორტალების, პროგრამული უზრუნველყოფის შუალედური შრეების ინტეგრაციის, შეტყობინებების მიწოდების გარანტირებული სისტემების, გამჭოლი ბიზნეს პროცესების ავტომატიზაციის, საწარმოებისა და ორგანიზაციებისთვის ერთიანი ცნობარების აგების, საინფორმაციო სისტემების ტექნიკური მომსახურებისა და მხარდაჭერის, რომელიც მოიცავს დღე-ღამის განმავლობაში „ცხელი ხაზის“ მხარდაჭერას, დამკვეთის ტერიტორიაზე პროფილაქტიკური და ტექნიკური სამუშაოების განხორციელებას, ავტონომიურ ტესტირებას, დამკვეთის ტერიტორიაზე სპეციალისტების მუდმივად ყოფნას.

საბანკო სისტემა „**Quorum.Бланк**“ ერთიანი საბანკო სისტემაა, რომელიც ემყარება კომპონენტურ სტრუქტურას და გამოიყენება ბანკის ოპერაციული, სააღრიცხვო და მმართველობითი საქმიანობის ავტომატიზაციისათვის. „**Quorum.Бланк**“-ის პლატფორმის არქიტექტურა საშუალებას იძლევა, კლიენტმა ამოირჩიოს მხოლოდ ის კომპონენტები, რომელიც საჭიროა ბანკის საქმიანობის ორგანიზებისა და იმისათვის, რომ შემდგომში პლატფორმას თავისუფლად დაამატოს საჭირო კომპონენტები, სისტემას გააჩნია სხვადასხვა კომპონენტები:

„**სააღრიცხვო ბირთვი**“ – იძლევა შემდეგი 5 სახის ფუნქციის რეალიზაციის საშუალებას: „პიროვნებები და კლიენტები“, რომ-

ლითაც ხორციელდება კლიენტების შესახებ მთლიანი ინფორმაციის აღრიცხვა და წარმოება;

„მთავარი წიგნი“ - ქვეყნის საბუღალტრო აღრიცხვის დებულებების შესაბამისად ახდენს საბანკო ოპერაციების აღრიცხვას, ღირებულებით და ნატურალურ მაჩვენებლებში;

„საბუთბრუნვა“ – ელექტრონული საბუთბრუნვის სისტემაა, რომელიც უზრუნველყოფს ბანკის შიდა და გარე დოკუმენტების დამუშავებას;

„ფინმონიტორინგი“ – უზრუნველყოფს დანაშაულებრივი გზით შემოსავლების მიღების ლეგალიზაციისა და ფინანსური ტერორიზმის წინააღმდეგ ბრძოლის განხორციელებას;

„ვალუტის კონტროლი“ - ახორციელებს არარეზიდენტი ანგარიშებისა და იმ დოკუმენტების კონტროლს, რომლებიც შეიცავენ სავალუტო ოპერაციებს.

„ოპერაციული მომსახურება“. ოპერაციული მომსახურების დანიშნულებაა ხელშეკრულებების წარმოების, კლიენტების მიმდინარე და ანგარიშსწორების ანგარიშების მომსახურების, უნაღდო ანგარიშსწორების, სალაროს ოპერაციების, კომუნალური გადასახადების მომსახურების პროცესების ავტომატიზაცია.

„ანგარიშსწორების ცენტრი“. ანგარიშსწორების ცენტრის დანიშნულებაა რუსეთის ბანკების მეშვეობით განხორციელებული ანგარიშსწორების, ფილიალებს შორის ანგარიშსწორების პროცესების ავტომატიზაცია, ბანკის მეშვეობით გადახდების მიღებისა და გადაგზავნის პროცესების ავტომატიზაცია.

„დეპოზიტები და ანაბრები“. დეპოზიტების და ანაბრების დანიშნულებაა იურიდიული და ფიზიკური პირებისგან თავისუფალი ფულადი საშუალებების მოზიდვის პროცესების ავტომატიზაცია და მოიცავს პლასტიკური ბარათების გამოყენებით შესრულებული ოპერაციების, კომუნალური გადასახადების, კონვერსიული ოპერაციების შესრულების ავტომატიზაციას. ბანკის ელექტრონული სისტემის საშუალებით ფულის გადაგზავნის ოპერაციების ავტომატიზაციას.

„დაკრედიტება“. დაკრედიტების დანიშნულებაა იურიდიული პირებისთვის სესხის გამოყოფისა და ფიზიკურ პირებზე კრედიტების გაცემის ოპერაციების შესრულების ავტომატიზაცია.

„საბანკო ბარათები“. საბანკო ბარათების დანიშნულებაა იმ საბანკო პროცესების კომპლექსური ავტომატიზაცია, რომლებიც დაკავშირებულია საემისიო და საინვესტიციო საქმიანობასთან.

„სალაროს ოპერაციები“. სალაროს ოპერაციების დანიშნულებაა ნაღდი ფულის მიღებისა და გაცემის, კრეხითი ანგარიშგებების მიღების ოპერაციების ავტომატიზაცია.

„სავალუტო დილინგი“. სავალუტო დილინგის დანიშნულებაა კონტრაგენტებთან ხელშეკრულებების გაფორმების ავტომატიზაცია, გარიგებების აღრიცხვა, განხორციელებული სადილინგო ოპერაციების მიხედვით ანგარიშგებების მიღების ავტომატიზაცია.

„გადასახადების აღრიცხვა“. გადასახადების აღრიცხვის დანიშნულებაა საგადასახადო კოდექსის მიხედვით კომერციულ ბანკებში აღრიცხვის წარმოების ავტომატიზაცია.

კითხვები თვითშემოწმებისთვის

1. რომელი ამოცანების რეალიზაცია შეუძლია საბანკო საინფორმაციო სისტემის საბაზო კომპლექტს?

2. დაახასიათეთ კომპანია **„Инверсия“**-ს მიერ შემუშავებული ავტომატიზებული საბანკო საინფორმაციო სისტემის ძირითადი ქვესისტემები.

3. დაახასიათეთ კომპანია **„Диасофт“**-ის მიერ შემუშავებული საბანკო ავტომატიზებული სისტემა.

4. დაახასიათეთ კომპანია **„Кворум“**-ის მიერ შემუშავებული საბანკო ავტომატიზებული სისტემა.

5. დაახასიათეთ კომპანია **„ПрограмБанк“**-ის მიერ შემუშავებულ საბანკო ავტომატიზებული სისტემა.

თავი 13. საბანკო საინფორმაციო სისტემების უსაფრთხოების უზრუნველყოფა

13.1. საზოგადოების ახალი საფრთხეები

XXI საუკუნე იქნება მსოფლიო საზოგადოების ინფორმაციზაციის საუკუნე. ქვეყნების უმეტესობა ააშენებს ინფორმაციულ საზოგადოებას, ე. ი. ინდუსტრიული საზოგადოებიდან განხორციელდება ინფორმაციულ საზოგადოებაზე გადასვლა, რომლის მთავარი და განმსაზღვრელი რესურსი, შრომის ძირითადი საგანი იქნება ინფორმაცია.

კონკურენციულ ბრძოლაში მხოლოდ ის ქვეყნები გაიმარჯვებენ, რომლებსაც ყველაზე მეტი ინფორმაციული რესურსი ექნებათ დაგროვილი.

კაცობრიობის დასაბამიდან დღემდე, ადამიანმა ბევრი რამ გამოიგონა და აითვისა, რამაც სასიკეთოდ იმოქმედა საზოგადოების განვითარებაზე, მაგრამ ხშირად მის მიერ შექმნილი თუ აღმოჩენილი მისსავე საწინააღმდეგოდ იყო მიმართული (ბირთვული ენერგია, ქიმიური და ბაქტერიოლოგიური იარაღები და სხვ.). იშვიათად მოიძებნება ისეთი ახალი ტექნიკისა და ტექნოლოგიის მიღწევები, რომელთა დანერგვასაც დადებითთან ერთად თან არ ახლდეს უარყოფითი მოვლენებიც. ასეა საზოგადოების საყოველთაო ინფორმაციზაციის შემთხვევაშიც. კერძოდ, კომპიუტერული უსაფრთხოების პრობლემა გადასაჭრელია. ჯერ კიდევ ცნობილი მეცნიერი და კიბერნეტიკის ფუძემდებელი ნ. ვინერი გვაფრთხილებდა, რომ ახალი ინფორმაციული ტექნოლოგიების უკონტროლო დანერგვამ კაცობრიობას შეიძლება დიდი ზიანი მიაყენოს.

„გენური ინჟინერია“, ანუ ინფორმაციული ტექნოლოგიები – ეს არის მოსალოდნელი ქარიშხლის მოკრძალებული ხმები, თუმცა ვიცით რა ადამიანის თვითგანადგურების უნარი, ჩვენ კარგად უნდა წარმოვიდგინოთ ინფორმაციული აღმოჩენების გამოყენებისას ამ მოვლენის მრავალჯერ გაზრდილი საფრთხე, ვი-

ნაიდან, თუ ეს აღმოჩენები არ იქნება კონტროლის ქვეშ, შეიძლება გამოიწვიოს კაცობრიობისათვის ტრაგიკული „მიღწევები“.

საზოგადოების საყოველთაო კომპიუტერიზაციამ შეიძლება გამოიწვიოს სხვადასხვა სახის დანაშაული და უარყოფითი სოციალური შედეგები.

კაცობრიობის ძირითადი ამოცანაა ახალი ინფორმაციული ტექნიკისა და ტექნოლოგიის დანერგვის შედეგად გამოწვეული უარყოფითი სოციალურ-ეკონომიკურ შედეგებთან აქტიური ბრძოლა, რათა მთლიანად სამყაროში და, პირველ რიგში, ჩვენს პლანეტაზე მიღწეულ იქნეს ინფორმაციული წონასწორობა.

ინფორმაციული ტექნოლოგიის არასწორი, დაუსაბუთებელი, შეუზღუდავი გამოყენება დროთა განმავლობაში შეუმჩნევლად, თანდათან უარყოფითად იმოქმედებს ადამიანის პიროვნებაზე.

სამხედრო საქმეში კომპიუტერული ტექნიკა და მისი პროგრამული უზრუნველყოფა შეიძლება იყოს პირდაპირ ან არაპირდაპირ დამნაშავე, ასევე, შეიძლება გახდეს ეკონომიკური, სამეურნეო და სოციალური ცხოვრების სფეროში მომხდარი მრავალი ინციდენტის ან ავარიის მიზეზი.

ინფორმაციულ საფრთხეობაში იგულისხმება გამოთვლითი ტექნიკის, ან ავტომატიზებული სისტემებით ინფორმაციის დამუშავებისას შიგა და გარე საფრთხეებიდან ინფორმაციის დაცვის მდგომარეობა. მოკვლევებით დადგინდა, რომ კომპიუტერების დაუსაბუთებელ უკონტროლო გამოყენებას შეიძლება მოჰყვეს პიროვნების ინიციატივის შესუსტება, მისი, როგორც პიროვნების, საზოგადოებიდან განკერძოება. წარმოების რობოტიზაცია და კომპიუტერიზაცია ადამიანში ადამიანურის ჩაკვლას იწვევს. მეცნიერების მიერ დამტკიცებულია, რომ პიროვნებას, რომელიც დროის დიდ ნაწილის კომპიუტერთანა ტარებს, სხვადასხვა უარყოფითი თვისებები უვითარდება. მაგალითად, მეგობრებთან ურთიერთობების განწყვეტა, მძიმე ხასიათი, დაქვეითებული ემოციები, ადამიანური სიტბოს ნაკლებად გამოყვანების უნარი და ოჯახის წევრებთან მიმართებაში სიტყვაძუნწობა. ასეთ ადამიანებს დასავლეთში ტექნოცენტრულ ადა-

მიანებს უწოდებენ. მათ, პირველ რიგში, კომპიუტერის საშუალებით ინფორმაციის მოძებნა და გაცვლა აინტერესებთ.

კომპიუტერი აძლიერებს ადამიანის აზროვნების შესაძლებლობებს. სასარგებლო იდეებს ის დადებითი ემოციებით ამარაგებს, ხოლო სახიფათოს კიდევ უფრო მეტ უარყოფითობას ანიჭებს.

კომპიუტერის არასწორად, უკანონოდ გამოყენების შემთხვევაში შეიძლება ადგილი ჰქონდეს: პიროვნების უფლებების შელახვას, პოლიტიკურ და ეკონომიკურ დანაშაულს, სახელმწიფოს უშიშროების შელახვას და სხვ.

საყოველთაო კომპიუტერიზაციის ერთ-ერთი უარყოფითი მოვლენაა ინტელექტუალური საკუთრების უფლებების დარღვევა, რაც თავის გამოხატულებას პოულობს ინტელექტუალური პროდუქტის არაკანონიერ მითვისებასა და საავტორო უფლებების დარღვევაში. პირველ რიგში, აღნიშნული ეხება პროგრამულ პროდუქტს, როგორც ინტელექტუალური საკუთრების ერთ-ერთ ობიექტს. საკმაოდ გავრცელებულია პროგრამული პროდუქტების არალიცენზირებული ტირაჟირება. პროგრამულ პროდუქტზე საავტორო უფლებების დარღვევას დიდი ზიანი მოაქვს ავტორისათვის. ჯერ ერთი, ეს ზიანი გამოიხატება დიდ მატერიალურ ზარალში და, მეორეც, პროგრამისტს ახალი პროგრამების შექმნის ხალისს უკარგავს.

პროგრამული პროდუქტის არალიცენზირებული გამრავლება გამონეულია რიგი მიზეზებით:

- ხშირ შემთხვევაში მასობრივ მომხმარებელს არა აქვს ფინანსური შესაძლებლობა, კანონიერი გზით შეიძინოს იგი;
- დაბალია მომხმარებლის ინფორმაციული კულტურა;
- ფირმებისა და ორგანიზაციების ხელმძღვანელებს არა აქვთ დიდი სურვილი, შეიძინონ პროგრამული უზრუნველყოფა, რადგან ნაკლებად წარმოებს მათი, როგორც ძირითადი საშუალებების აღრიცხვა.

განსაკუთრებით საყურადღებოა პიროვნების შესახებ ინფორმაციის საიდუმლოების დარღვევა. არსებობს პროგრამები, რომლებიც უზრუნველყოფენ პიროვნების შესახებ ინფორმაციის

გადაცემას იმ პირებისათვის, რომლებიც უფლებამოსილი არ არიან, ისარგებლონ ასეთი ინფორმაციით. ინფორმაციის ასეთი სახით ამოღებას არსების „გახსნას“ უწოდებენ. რამდენადაც პიროვნების შესახებ ინფორმაცია ელექტრონული სახით განთავსებულია მონაცემთა ბაზებში, პიროვნების ინფორმაციის არასრულყოფილი დაცვის შემთხვევაში იზრდება ადამიანის პირადულ ცხოვრებაში შეჭრის საფრთხე. კომპიუტერის საშუალებით ბევრ ქვეყანაში წარმოებს სატელეფონო საუბრების მოსმენა, რაც ადამიანის უფლებების დარღვევაა.

საზოგადოების ინფორმატიზაციის პროცესს გარკვეული ზომით თან ახლავს ქვეყნის უშიშროების კონტროლის გართულება. დღეისათვის მსოფლიოში შექმნილია მრავალი გლობალური კომპიუტერული ქსელი, რომელთა დახმარებითაც შესაძლებელია ინფორმაციის გადაცემა დედამიწის ნებისმიერ წერტილში. თითქმის შეუძლებელია ასეთი ინფორმაციის ოპერატიული გაკონტროლება. მაგალითად, ზემოთაღნიშნული გლობალური კომპიუტერული ქსელი **Internet**, რომლითაც დღეისათვის სარგებლობს 5.56 მილიარდზე მეტი მომხმარებელი [68].

ასეთ შემთხვევაში ძნელია, გაკონტროლდეს აღნიშნულ ქსელში გადაცემული ინფორმაცია.

ნებისმიერ პიროვნებას, რომელსაც აქვს პერსონალური კომპიუტერი, მოდემი და მობილური ტელეფონი, შეუძლია ჩაერთოს ქსელში და გადასცეს ნებისმიერი სახის ინფორმაცია. იზრდება იმის ალბათობა, რომ გლობალური ქსელები შეიძლება გამოიყენონ ჯაშუშობისთვის, ქვეყნის საიდუმლო ინფორმაციის გადასაცემად.

კომპიუტერული ტექნოლოგიის გამოყენებისას ერთ-ერთი საშიშროებაა კომპიუტერული ქსელის საშუალებით პორნოგრაფიული ინფორმაციის გავრცელება, რომელიც უარყოფითად მოქმედებს საზოგადოების მორალურ სახეზე და, განსაკუთრებით, ახალგაზრდა თაობაზე.

ინფორმაციულ საზოგადოებაში კომპიუტერი შეიძლება გამოიყენონ ძალაუფლების ხელში ჩაგდების ინსტრუმენტად, დემოკრატიის საწინააღმდეგოდ და ძალაუფლების ცენტრალიზაციის გაძლიერების მიზნით. მაგალითად, როგორც აშშ-ის სოცი-

ოლოგების გამოკვლევები გვიჩვენებს, კომპიუტერის საშუალებით არჩევნების შედეგების პროგნოზირების სისტემამ შეიძლება ზემოქმედება იქონიოს არჩევნების მსვლელობის კამპანიაზე. ამის ნათელი მაგალითია 1984 წელს აშშ-ში საპრეზიდენტო არჩევნების შედეგების კომპიუტერული პროგნოზის გამოცხადება ტელევიზიით საარჩევნო უბნების დახურვამდე. უარყოფითად უნდა ჩაითვალოს აგრეთვე არჩევნების მსვლელობისას შედეგების ინფორმირება.

საზოგადოების ინფორმატიზაცია, ერთი მხრივ, იწვევს ახალი პროფესიების აღმოცენებას და, შესაბამისად, ახალი სამუშაო ადგილების შექმნას, თუმცა ახლად შექმნილი სამუშაო ადგილების რაოდენობა გაცილებით ნაკლებია გამოთავისუფლებულ მომუშავეთა რაოდენობაზე, ე. ი. ადგილი აქვს უმუშევართა რაოდენობის ზრდას.

ინფორმატიზაციის პროცესი მოითხოვს გამოთავისუფლებულ მომუშავეთა გადამზადებას საზოგადოების ინფორმატიზაციის მოთხოვნების შესაბამისად, რაც დაკავშირებულია დიდი ოდენობის ფულადი სახსრების გაღებასთან, რისი გაკეთებაც, რა თქმა უნდა, არ სურთ სხვადასხვა საწარმოების და ორგანიზაციების ხელმძღვანელებს. იზრდება დაპირისპირება წარმოების მფლობელებსა და დაქირავებულთა შორის, მოქალაქეებსა და სახელმწიფოს შორის, ირღვევა უშუალო კონტაქტები მუშებსა და დამქირავებლებს შორის, რასაც საბოლოოდ სოციალურ უთანასწორობამდე, შემოსავლების უსამართლო განაწილებამდე მივყავართ. მუშების გადამზადების პროცესი გაცილებით რთულია, ვიდრე მოძველებული, დაბალმწარმოებლური დაზგის შეცვლა მაღალმწარმოებლურით.

ინფორმაციული ტექნოლოგიების დანერგვის შედეგად იზრდება მონოპოლისტური ტენდენციების განვითარება, რაც კლავს თავისუფალ კონკურენციას, როგორც თავისუფალი საბაზრო ეკონომიკის საფუძველს.

ახალი ინფორმაციული ტექნოლოგიების დანერგვამ შეიძლება უარყოფითად იმოქმედოს ადამიანის ჯანმრთელობაზე. საზღვარგარეთის სპეციალისტების შეფასებით, კომპიუტერული ტექნიკის ინტენსიურმა დანერგვამ შეიძლება გამოიწვიოს სხვადას-

ხვა პროფესიული დაავადებები. პუბლიკაციების მიხედვით თუ ვიმსჯელებთ, მონიტორთან ხანგრძლივი მუშაობა უარყოფითად მოქმედებს ფეხმძიმობის მიმდინარეობაზე. ცხოველებზე ჩატარებული ცდების მიხედვით დამტკიცებულია, რომ 60-ჰერციანი სიხშირის მაგნიტური ველი უარყოფითად მოქმედებს ცოცხალ ორგანიზმზე.

ავსტრალიაში ჩატარებული გამოკვლევები მიუთითებს კომპიუტერთან მომუშავე ოპერატორების დაავადებების ზრდაზე. აღნიშნული დაავადება ცნობილია, როგორც განმეორებადი დაძაბულობით გამოწვეული „მოშლილობა“. ასეთი დაავადებით არიან შეპყრობილი კომპიუტერთან მომუშავე ოპერატორების 20-30%. ეს დაავადება, ორგანიზმში ხანგრძლივი სტატიკური დაძაბულობის გამო, იწვევს ფუნქციონალურ ცვლილებებს: კუნთების, ბეჭების, ხელების, კისრის დაავადებებს. ჯერ კიდევ ბოლომდე არ არის შესწავლილი მონიტორთან ხანგრძლივი მუშაობით გამოწვეული დაავადებები. დადგენილია მხოლოდ ის, რომ მონიტორთან დიდხანს მუშაობა ადამიანში იწვევს თავის ტკივილებსა და სტრესულ რეაქციას, ასევე, შრომისუნარიანობის მოშლას ან მის დაქვეითებას. ძირითადად ავადდებიან ის პირები, როლებიც მთელი დღის განმავლობაში მუშაობენ კომპიუტერთან. მაგალითად, აშშ-ის გაზეთების რედაქტორების 30-40%-ს კომპიუტერთან ხანგრძლივი მუშაობის გამო მოშლილი აქვს ხელის მტევნისა და მაჯის ნორმალური ფუნქციონირება. კომპიუტერთან ხანგრძლივი მუშაობის შედეგად ზიანდება მხედველობა, თვალი სწრაფად იღლება, რაც იწვევს თვალის ქრონიკულ დაავადებებს.

კომპიუტერიზაციის ზემოთ აღნიშნული უარყოფითი მოვლენების აღმოფხვრის მიზნით, საჭიროა გაფართოვდეს მეცნიერული კვლევა ინფორმაციზაციის ტექნიკურ საშუალებათა გამოყენებით გამოწვეული დაავადებების გამოსავლენად, რაც საშუალებას მოგვცემს, გარკვეული მოთხოვნები ნავუყენოთ ტექნიკური საშუალებების დამპროექტებელ და გამომშვებ წარმოება-ორგანიზაციებს. აღნიშნულ საქმეში დადებითი როლის შესრულება შეუძლია ინფორმაციულ პროდუქტებზე საერთაშორისო სტანდარტების შემუშავებას, დამპროექტებელი და გამომშვები წარმოება-დანესებულების მიერ აღნიშნული სტანდარტე-

ბის დაცვას. კომპიუტერის ბოროტად გამოყენებამ, არასწორად შედგენილმა პროგრამულმა უზრუნველყოფამ, გამოთვლით სისტემაში შეცდომით ინფორმაციის შეტანამ, ზოგიერთი პირის თაღლითურმა მოქმედებამ, მომხმარებლის დაბალმა კვალიფიკაციამ და უყურადღებობამ შეიძლება დიდი მატერიალური და მორალური ზიანი მიაყენოს პიროვნებას, ორგანიზაციას, ან მთლიანად სახელმწიფოს, გამოიწვიოს ეკოლოგიური კატასტროფები, ომის დაწყება, ქვეყნის ეკონომიკის მოშლა.

კომპიუტერი თვითონ არ სჩადის დანაშაულს, მას ადამიანი-დამნაშავე იყენებს. ხშირად დანაშაულს გართობის მიზნით სჩადიან და არა ინფორმაციის მითვისების გამო. ადამიანი, ამონებს რა თავის პროფესიულ შესაძლებლობებს, არ ითვალისწინებს დანაშაულის შედეგებს. მაგალითად, ჰაკერები ადგენენ ვირუსულ პროგრამებს, რომელთა მოქმედება არღვევს მომხმარებლის პროგრამების მთლიანობას, მწყობრიდან გამოჰყავს პერსონალური კომპიუტერი ან მთლიანად გამოთვლითი ქსელი.

პირველი კომპიუტერული ვირუსები გაჩნდა გასული საუკუნის 60-იან წლებში. 1962 წელს ინჟინერებმა ვ. ა. ვისოტსკიმ, გ. დ. მაკელორმა და რობერტ მორისმა შექმნეს კომპიუტერული თამაში „დარვინი“. თამაშის არსი მდგომარეობდა იმაში, რომ შედგენილ პროგრამას უნდა გაენადგურებინა მოწინააღმდეგის ყველა პროგრამა და ხელში ჩაეგდო ბრძოლის ველი. ამ უწყინარმა თამაშმა საფუძველი ჩაუყარა თანამედროვე კომპიუტერული ვირუსების ეპოქას. გარკვეული დროის გასვლის შემდეგ კაცობრიობამ გაიგო, რომ თამაშის ძირითადი იდეის გამოყენება შეიძლება არა მარტო გართობის მიზნით, არამედ საზოგადოებისათვის სხვა მრავალი ზიანის მისაყენებლადაც.

დღევანდელი კომპიუტერული ვირუსები მეტისმეტად „ნიჭიერები“ არიან. ისინი აგროვებენ ინფორმაციას და გადასცემენ პატრონს. ვირუსების მოქმედება არღვევს კომპიუტერის მუშაობას, მათი მეშვეობით შესაძლებელია სხვისი ფულადი სახსრებისა და ინფორმაციის მითვისება და სხვა მრავალი კომპიუტერული დანაშაულის ჩადენა. ამ პრობლემას შევეხებით მოგვიანებით.

1988 წელს აშშ-ში კორნელსკის უნივერსიტეტის დამამთავრებელი კურსის 23 წლის სტუდენტმა რობერტ ტაპან მორისმა

კომპიუტერულ ქსელ-**ARPANET**-ში შეიყვანა პროგრამა, – კომპიუტერული ვირუსის იშვიათ სახეობა, ე. წ. „ქსელურიჭია“. რის შედეგადაც მთლიანად ან ნაწილობრივ დაბლოკა საერთო ნაციონალური კომპიუტერული სისტემები. კერძოდ: **Internet, CSNet, NSFnet, BNnet, ArpaNet და სხვ.**, დაავადდა **Internet**-ის 1 200 ქსელი, 85 200 საკვანძო კომპიუტერი. ამ „იერიშის“ შედეგად მიყენებულმა საერთო ზარალმა 100 მილიონი დოლარი შეადგინა.

რ. მორისი ჩადენილი დანაშაულისათვის უნივერსიტეტიდან გარიცხეს, ერთი წლის შემდეგ აღდგენის უფლებით, 270 ათასი დოლარით დააჯარიმეს და სამი თვით პატიმრობა მიუსაჯეს.

კომპიუტერი მასში შეტანილი არასწორი ინფორმაციის საფუძველზე იღებს გადაწყვეტილებას, რომლის რეალიზაციის შედეგად საზოგადოებას დიდი ზარალი ადგება. მაგალითად, 1983 წელს აშშ-ის სამხრეთ-დასავლეთ ნაწილში მოხდა წყალდიდობა, რომლის მიზეზიც იყო კომპიუტერში შეტანილი არასწორი ინფორმაცია ამინდის პროგნოზის შესახებ. კომპიუტერმა შეტანილი ინფორმაციის საფუძველზე გასცა ბრძანება მდინარე კოლორადოს რაბით გადაკეტვის შესახებ. მოსალოდნელი კარგი ამინდის ნაცვლად, წამოვიდა ნიაღვარი, რომელმაც დიდი ზიანი მიაყენა ქვეყანას.

კომპიუტერის არასწორი მუშაობის შედეგად 1986 წელს კატასტროფა განიცადა ამერიკულმა თანამგზავრულმა ხომალდმა **Challenger**-მა. კომპიუტერის არასწორი მუშაობის შედეგად რამდენჯერმე წარმოიშვა საავარიო სიტუაცია კოსმოსურ სადგურ „**MIR**“-ზე. ალგორითმულ ენა ადაზე შედგენილ პროგრამაში დაშვებული შეცდომის გამო, 1996 წლის ზაფხულში კატასტროფა განიცადა თანამგზავრმა **Cluter**-მა, რომელიც ორბიტაზე უნდა გაეყვანა რაკეტამატარებელ **Arian5**-ს, რომლის შექმნაზე 8 მილიარდი დოლარი დაიხარჯა და რომლის გაშვების ძირითადი მიზანი დედამიწაზე მზის აქტივობის ზეგავლენისა და კლიმატის ფორმირების პრობლემების გლობალური გამოკვლევა იყო. ჩერნობილის ატომურ სადგურში მომხდარი ავარია შეტანილია ეკოლოგიური კატასტროფების გინესის წიგნში, გამოწვეული იყო კომპიუტერის არასწორი მუშაობით.

რადგან სამხედრო ტექნიკის მართვა ძირითადად კომპიუტერის საშუალებით ხორციელდება, იქმნება მესამე მსოფლიო ომის დაწყების გარკვეული საშიშროება. ეს შეიძლება მოხდეს მაშინ, თუ კონტინენტთაშორისი რაკეტების მართვის პროგრამა ხელში ჩაუვარდებათ ექსტრემისტებს.

კომპიუტერული ინფორმაციის გაყალბებამ შეიძლება დიდი ზიანი მიაყენოს საზოგადოებას. მაგალითად, 1971 წელს ნიუ-იორკის რკინიგზაზე დაიკარგა 352 ვაგონი. დამნაშავემ ისარგებლა იმ გამოთვლითი ცენტრის ინფორმაციით, რომელიც მართავდა რკინიგზის მუშაობას. მან შეცვალა ვაგონების საბოლოო პუნქტში მისვლის მისამართი. მიყენებულმა ზარალმა ერთ მილიონ დოლარზე მეტი შეადგინა.

კომპიუტერული ინფორმაციის გაყალბება შეიძლება არჩევნებისა და რეფერენდუმის ხმის მიცემის, ანდა კომპიუტერებით მათი რეგისტრაციისა და დათვლის დროს.

საბანკო სისტემაში „ელექტრონული ფულის“ დანერგვა, ე.ი. უნაღდო ანგარიშსწორების შემოღება, ზოგიერთ თაღლითს საშუალებას აძლევს, აკრძალული ხერხების გამოყენებით შეაღწიოს ბანკის მონაცემთა ბაზაში და უკანონო გზით მიითვისოს ფულადი თანხები. მოვიყვანთ მხოლოდ რამდენიმე მაგალითს.

1989 წელს ჩიკაგოს ბანკ „ფერსტ ნეშალ ბანკის“ თანამშრომლებმა – არმანდ მურმა და მისმა თანამზრახველებმა – აღნიშნული ბანკის „კომპიუტერული დაყაჩაღება“ განახორციელეს. მათ ბანკის ელექტრონულ სისტემას მოარგეს კოდი, რის საშუალებითაც ჩიკაგოს ბანკიდან ავსტრიაში, ვენის ორ ბანკში, გადაგზავნეს 69 მილიონი დოლარი. შემდეგ ისინი შეეცადნენ ეს ფული ამერიკაში თავიანთ ანგარიშებზე ჩაერიცხათ. სწორედ ამ მომენტში გამომჟღავნდა მათი საქმიანობა. არმანდ მურს ჩადენილი დანაშაულისათვის მიესაჯა 10 წლით პატიმრობა.

მოვიყვანოთ მაგალითები რუსეთის ფედერაციული რესპუბლიკისთვის კიბერთავდასხმების შედეგად მიყენებული ზარალის შესახებ 2019-0224 წლებში:

2024 წელი. წლის განმავლობაში ნოვოსიბირსკის ოლქში, IT დანაშაულებიდან მიღებული ზარალი 36%-ით გაიზარდა და 3,8 მილიარდ რუბლი შეადგინა. კიბერდანაშაულის ზარალი ნიჟნი

ნოვგოროდის რეგიონში 3,8 მილიარდ რუბლამდე გაიზარდა. ვორონეჟის რეგიონში IT დანაშაულების ზარალმა წლის განმავლობაში 2,4 მილიარდ რუბლს გადააჭარბა.

კიბერკრიმინალებმა ტვერის რეგიონის მცხოვრებლებს 1 მილიარდი რუბლი მოპარეს. ლენინგრადის რეგიონის შინაგან საქმეთა სამინისტრომ IT დანაშაულთან ბრძოლის შედეგები შეაჯამა და აღნიშნა, რომ რუსეთში კიბერთაღლითობის შედეგად მიყენებული ზარალი წელიწადში 36%-ით გაიზარდა და 200 მილიარდ რუბლს მიაღწია.

თათარსტანში 2024 წლის განმავლობაში 32 ათასი IT დანაშაული დაფიქსირდა, ზარალმა 5,7 მილიარდი რუბლი შეადგინა. „სბერბანკის“ მონაცემებით კიბერკრიმინალებმა 3 წელიწადში რუსებს 350 მილიარდ რუბლზე მეტი მოპარეს.

2023 წელი. რუსეთის პრეზიდენტი ვლადიმერ პუტინი: „IT დანაშაულებიდან მიღებულმა ზარალმა წელიწადში 156 მილიარდ რუბლს გადააჭარბა“. სანქტ-პეტერბურგში IT დანაშაულებიდან მიყენებულმა ზარალმა 13 მილიარდ რუბლს მიაღწია. რუსეთის შსს-ის მონაცემების მიხედვით ჰაკერებმა შექმნეს 1000-ზე მეტი ყალბი ვებსაიტი და 3 თვეში რუსეთისა და დსთ ქვეყნების მომხმარებლებისაგან მოიპარეს 5 მილიონი დოლარის კრიპტოვალუტა. ცენტრალურმა ბანკმა გამოავლინა კიბერთაღლითების მიერ რუსებისგან მოპარული თანხა პირველ კვარტალში – 4,55 მილიარდი რუბლი. კომპანიები რუსეთში ქსელის აღჭურვილობის კონტროლის ყოველი ინციდენტისთვის 18 მილიონ რუბლს კარგავენ.

2022 წელი. FBI-მა გამოაქვეყნა ყველაზე პოპულარული ონლაინდანაშაულებისა და მათგან ამერიკელებისადმი მიყენებული ზარალის სია. ტანსაცმლისა და საცვლების ამერიკულმა მწარმოებელმა sBrands-მა კიბერშეტევის გამო 100 მილიონი დოლარი დაკარგა.

2021 წელი. რუსეთში ყველაზე „აგრესიული“ გამოსასყიდი ვირუსები დასახელდა. დანაკარგების ოდენობა აშშ-ში ყველაზე გავრცელებული კიბერდანაშაულიდან 4 მილიარდ დოლარს შე-

ადგენს. რუსული კომპანიები სულ უფრო ხშირად ყიდულობენ საკუთარ მონაცემებს ჰაკერებისგან.

რუსეთის საგარეო საქმეთა სამინისტროს მონაცემებით კი-ბერდანაშაულებისგან მიყენებულმა გლობალურმა ზარალმა შეიძლება 6 ტრილიონ დოლარს მიაღწიოს.

შინაგან საქმეთა სამინისტრო: ეკონომიკური დანაშაულებიდან მიყენებულმა ზარალმა 450 მილიარდ რუბლს მიაღწია.

2019 წელი. რუსეთში ჰაკერების თავდასხმების შედეგად მიყენებულმა ზარალმა დაახლოებით 2,5 ტრილიონი რუბლი შეადგინა. მსოფლიო ეკონომიკა ჰაკერების გამო წელიწადში 1 ტრილიონ დოლარს კარგავს [69].

დამნაშავე ბევრ შემთხვევაში კომპიუტერს იყენებს მიზნის მისაღწევად. ის სწავლობს ფირმაში არსებულ აღრიცხვა-ანგარიშგების მდგომარეობას, ცდილობს, აღმოაჩინოს აღრიცხვის არსებულ სისტემაში „სუსტი წერტილები“ და გამოიყენოს ისინი საკუთარი მიზნების განსახორციელებლად, თუნდაც ფულადი თანხის მისათვისებლად. იგი ადგენს რა შემავალი ინფორმაციის საფუძველზე ამოცანის ამოხსნის მათემატიკურ მოდელს, რომელიც გამოიყენება დანაშაულის ჩადენის პირობად, დამნაშავე მას კომპიუტერზე „გათამაშებს“. კომპიუტერის მიერ მიღებული გამოსავალი ინფორმაცია სარეკომენდაციო ხასიათისაა. კომპიუტერი დამნაშავეს დანაშაულის ჩადენის რამდენიმე ვარიანტიდან ამოურჩევს ყველაზე ოპტიმალურს – დანაშაულის ჩადენის უსაფრთხოებისა და მითვისებული თანხის ოდენობის შესახებ.

აშშ-ის კალიფორნიის შტატის სანაოსნო კომპანიის ერთ-ერთმა თანამშრომელმა, რომელიც ბუღალტრად მუშაობდა აღნიშნულ კომპანიაში და, იმავდროულად, იყო კომპიუტერული მომსახურების მფლობელი, შეამჩნია აღნიშნული კომპანიის სარეგიონო სამსახურის საქმიანობაში სუსტი ადგილები და გადაწყვეტა, ესარგებლა ამით. მან კომპანიის საბუღალტრო აღრიცხვის მოდელირება და შედგენილი მოდელის კომპიუტერზე ამოხსნის შედეგად დაადგინა, თუ რა რაოდენობის ფალსიფიცირებული ანგარიშის გახსნა იყო საჭირო და რა ოპერაციები უნდა შეესრულებინა ფულის მისატაცებლად. აღნიშნული კომპანია ეწეოდა ხილბოსტნეულის გადაზიდვას. მან 17 ფიქციურ მომწოდებელ კომპა-

ნიას გაუხსნა ანგარიშები და დაიწყო ფულადი ოპერაციების შესრულება. შემუშავებულმა საბუღალტრო აღრიცხვის მოდელმა უჩვენა, რომ სარევიზიო სამსახურის ფარგლებში არსებული ხარვეზი მას საშუალებას აძლევდა მონაცემების 5%-ით დამახინჯების შემთხვევაში, მის მიერ ჩადენილი დანაშაული არ გამოჟღავნებულიყო. აღნიშნული საქმიანობა იმდენად წარმატებული აღმოჩნდა, რომ მაქინაციის დანყების პირველ წელს მან მიიტაცა 250 ათასი დოლარი. თავისი განზრახვით მას არ დაურღვევია კომპანიის საფინანსო საქმიანობა. კომპანიის ხელმძღვანელობა ბოლოს და ბოლოს მიხვდა, თუ სად იყო დამარხული „ძაღლის თავი“, მაგრამ ამ მომენტისათვის დამნაშავეს უკვე მითვისებული ჰქონდა ერთი მილიონი დოლარი.

2008 წლის აგვისტოში, რუსეთ-საქართველოს ომის პერიოდში, და 2014 წლის იანვარში ჰაკერებმა განახორციელეს თავდასხმა საქართველოს სახელმწიფო საიტებზე. პირველ შემთხვევაში გაითიშა ყველა სამთავრობო საიტი, რამაც გამოიწვია ქვეყნის ინფორმაციული იზოლაცია გარე სამყაროსგან.

2014 წელს ჰაკერებმა გაანადგურეს საქართველოს პარლამენტის მონაცემთა ბაზაში არსებული ფაილები, რომლებშიაც ასახული იყო პარლამენტის 17-წლიანი მუშაობის შესახებ ინფორმაცია.

13.2. კომპიუტერული დანაშაულებების კლასიფიკაცია

ინტერნეტის მომხმარებელთა რაოდენობის ზრდას თან ახლავს კომპიუტერული დანაშაულებების ზრდა. ეკონომიკური საქმიანობის სფეროში ქსელური დანაშაული მომხმარებლის, ბიზნესის, სახელმწიფოსა და საზოგადოებისათვის მნიშვნელოვან საფრთხეს წარმოადგენს.

საერთაშორისო ვაჭრობის პალატის ექსპერტების მონაცემების მიხედვით, ჩადენილი დანაშაულებების რაოდენობა იზრდება მომხმარებელთა რაოდენობის ზრდის პარალელურად. ინტერნეტის კრიმინალიზაციას ხელს უწყობს დამნაშავეს ანონიმურობა, რომელიც მისი მსხვერპლიდან რამდენიმე ათას კილომეტრზე იმყოფება.

რაც უფრო მეტად ვითარდება ინფორმაციული ტექნოლოგიები, მით უფრო იზრდება კომპიუტერული დანაშაულების რაოდენობა, უფრო საშიში ხდება ჰაკერების მიერ შექმნილი ვირუსული პროგრამები.

კომპიუტერული დანაშაულების პროფილაქტიკის, გახსნისა და დამნაშავის კანონის ფარგლებში დასჯის მიზნით საჭიროა, პირველ რიგში, გაიკვეს კომპიუტერული დანაშაულის არსი, მოქმედების ადგილი, დანაშაულის განხორციელების შედეგად მიყენებული მატერიალური და მორალური ზარალი, დანაშაულის ჩადენის მიზანი.

კომპიუტერულ დანაშაულებებს მიეკუთვნება:

1. ინფორმაციის გაჟონვა, დამახინჯება, დაფარვა, ინფორმაციის გაყალბება.
2. ინფორმაციაზე არასანქცირებული მიმართვა.
3. კომპიუტერისთვის ზიანის მომტანი პროგრამების შემუშავება, გამოყენება, გავრცელება. მაგალითად, კომპიუტერული ვირუსები.
4. ინფორმაციის ბლოკირება.

ინფორმაციაზე არასანქცირებულ მიმართვას მაშინ აქვს ადგილი, როცა კომპიუტერში კანონით გათვალისწინებულ შენახულ ინფორმაციაზე ავტორის, მისი მფლობელის ნებართვის გარეშე წარმოებს ინფორმაციის მოპოვება, ინფორმაციის მფლობელის შანტაჟი, კომერციული საიდუმლო ინფორმაციის მიღება ან მოპარული ინფორმაციის საფუძველზე მისთვის საჭირო ამოცანების გადაწყვეტა.

კომპიუტერული ვირუსები მცირე ზომის პროგრამებია (რამდენიმე ასეულიდან რამდენიმე ათასი ბაიტის სიგრძის). მათთვის ძირითადად დამახასიათებელია ის, რომ, მომხმარებლის ნების გარეშე ხდება ამ პროგრამების ავტომატური გამრავლება და მისი მიერთება სხვა სასარგებლო პროგრამებთან ან ინფორმაციულ ფაილებთან. ვირუსული პროგრამების გავრცელება წარმოებს ჯაჭვური რეაქციით, დაავადებული დისკები და ფაილები, თავის მხრივ, ვირუსების მატარებლები ხდებიან და სხვა დისკებსა და ფაილებს ავაადებენ. ზოგიერთ კომპიუტერულ ვირუსს მწყობრიდან გამოჰყავს კომპიუტერი.

„ვირუსის“ სახელწოდება ვირუსულმა პროგრამამ მიიღო მისი ანალოგიური ბიოლოგიური პროტოტიპისაგან. ბიოლოგიური ვირუსის ზემოქმედება, როგორც ცნობილია, იწვევს იმ ინფორმაციის განადგურებას, რომელიც ჩადებულია ცოცხალი უჯრედის კოდში. ვირუსი უზრუნველყოფს ორგანიზმში მის თავისუფალ გამრავლებას, რაც იწვევს მთლიანად ორგანიზმის დაავადებას. პროგრამული ვირუსი ანადგურებს, სპობს იმ ინფორმაციას, რომელსაც შეიცავს პროგრამული კოდი. ვირუსით დაავადების შემთხვევაში ირღვევა კომპიუტერის გამართული მუშაობა. ვირუსული პროგრამა შეიძლება შექმნას პროფესიონალმა ან მოყვარულმა. ყველაზე საშიშია პროფესიონალის მიერ შექმნილი ვირუსული პროგრამები, რადგან წინასწარ განზრახული მიზნის განსახორციელებლადაა მოფიქრებული. ვირუსული პროგრამების გავრცელება ყველაზე მასშტაბურია ისეთ ქვეყნებში, სადაც დაბალია ინფორმაციული კულტურა და, ძირითადად მოპარულ პროგრამებს იყენებენ. მათ გავრცელებას ხელს უწყობს ისიც, რომ პერსონალური კომპიუტერის გამოყენება ხშირად ხდება კოლექტიურად, რამდენიმე ერთეული ან ათეული მომხმარებლის მიერ.

გავრცელების მიხედვით, კომპიუტერული ვირუსებია: ფაილური, ქსელური და სისტემური ანუ ჩამტვირთავი. ქსელური ვირუსები ვრცელდება კომპიუტერულ ქსელში, ფაილური კი – შესასრულებელ ფაილებში. ჩამტვირთავი კომპიუტერული ვირუსი მოთავსებულია დისკის იმ ნაწილში, სადაც ჩამტვირთავი პროგრამის მოდულია. განასხვავებენ რეზიდენტულ და არარეზიდენტულ ვირუსულ პროგრამებს. რეზიდენტული ვირუსი მოთავსებულია ოპერატიულ მეხსიერებაში და აქტიურ მდგომარეობაში იმყოფება მაშინაც კი, როცა კომპიუტერი გამორთულია ან მიმდინარეობს სისტემის გადატვირთვა. არარეზიდენტული ვირუსული პროგრამები კი აქტიურია მხოლოდ გარკვეული დროით და არ იწვევს კომპიუტერის მეხსიერების დაავადებას.

როგორც აღინიშნა, დანიშნულების მიხედვით, ვირუსული პროგრამები მრავალგვარია. განვიხილოთ რამდენიმე მათგანი:

პროგრამა „ლოგიკური ბომბი“. აღნიშნული პროგრამა მოქმედებას იწყებს გარკვეული დროის გავლის ან პირობის შესრუ-

ლების შემდეგ. ხშირად ამ პროგრამას უწოდებენ ბომბს საათის მექანიზმით. მისი ამოქმედება იწვევს კომპიუტერული სისტემის ნორმალური მუშაობის მოშლას. აღნიშნული ვირუსის მოქმედება განსაკუთრებით საშიშია, თუ იგი მოხვდა ოპერაციულ სისტემაში.

პაროლების გახსნის პროგრამა. აღნიშნული პროგრამა თანმიმდევრულად ახორციელებს პაროლების ყველა შესაძლო ვარიანტების გენერაციას მანამ, სანამ აღმოჩენილი არ იქნება რეალური პაროლი. ანალოგიური დანიშნულებისაა პაროლების ხელში ჩაგდებისა და მიღების პროგრამები. პაროლების ხელში ჩაგდების პროგრამების საშუალებით შესაძლებელია კომპიუტერული სისტემის შეფერხების იმიტაციის შექმნა, რაც მომხმარებლისაგან სისტემაში იდენტიფიკაციისა და პაროლის ხელმეორედ შეტანას მოითხოვს. აღნიშნული იდენტიფიკაციისა და პაროლის მიღების შემდეგ, ბოროტმოქმედი იყენებს მას ნამდვილი მომხმარებლის სახელით სხვადასხვა მონაცემთა ბაზებში შესასვლელად, ე. ი. სისტემაზე არასანქცირებული მიმართვისათვის. ვირუსული პროგრამების შემდგენელ დამნაშავეებს **ჰაკერები** ეწოდებათ, ხოლო იმ დამნაშავეებს, რომლებიც იმგვარ პროგრამებს ადგენენ, რომელთა მეშვეობითაც ხორციელდება კონფიდენციალური მონაცემების მიღება ან სისტემაში არსებული მონაცემების მთლიანობის დარღვევა **კრაკერები** ეწოდებათ (კრაკერი ინგ. Crack – გატეხვა). ისეთი სახის ვირუსული პროგრამების შემდგენელ პირებს რომლებიც შედიან კავშირგაბმულობის (როგორც სადენიან, ისე უსადენო) ქსელში და უფასოდ სარგებლობენ არხებით **ფრიკერები** ეწოდებათ.

იმ საწარმოებსა და ორგანიზაციებს, რომლებიც ინფორმაციის დასამუშავებლად იყენებენ კომპიუტერებს, მიუხედავად იმისა, ამ კომპიუტერების გამოყენება წარმოებს ავტონომიურად თუ ქსელში, ინფორმაციის დამუშავებაში ყოველთვის შეექმნებათ პრობლემები, თუ ისინი არ არიან დაცული ვირუსული პროგრამებისაგან. კომპიუტერებში მათ აუცილებლად ექნებათ ამა თუ იმ მოქმედების კომპიუტერული ვირუსი, რომელიც გარკვეული დროის გასვლის შემდეგ იჩენს თავს, – „გაიღვიძებენ“ და დაიწყებენ ინფორმაციის ან კომპიუტერის დაზიანებას.

ადრე გავრცელებული ვირუსები იყო **Win 95.CIN**, **Win 32.F-unlove** და **Win32.Elken**. თუმცა აღნიშნული ვირუსები ახლა ნაკლებად „პოპულარულია“. ხშირად კომპიუტერის დაავადება გამოწვეულია ვირუსით „ჩერნობილი“ **WinCin** ვირუსით. ვირუსული პროგრამები იქმნება როგორც ინფორმაციის დასაზიანებლად, ასევე ოპერაციული სისტემების მწყობრიდან გამოყვანის მიზნით. მაგ., ათობით ათასი ვირუსია შექმნილი ოპერაციული სისტემა **MS DOS**-ის დასაზიანებლად. ამ ვირუსების დიდი ნაწილი **Windows**-ის ვერსიებში აღარ არსებობს. თუმცა დროდადრო შეიძლება მოხდეს მათი გააქტიურება, რაც დიდ ზიანს მიაყენებს ოპერაციულ სისტემას.

Adware არის არასასურველი, მაგნე პროგრამა, რომელიც აჩვენებს რეკლამებს თქვენს ეკრანზე, ყველაზე ხშირად თქვენს ბრაუზერში. ის, როგორც წესი, იყენებს მზაკვრულ მეთოდს, რათა შენიღბოს ლეგიტიმური პროგრამული უზრუნველყოფა ან ჩამოტვირთოს სხვა პროგრამასთან ერთად, რათა მოატყუოს და დააინსტალიროს იგი თქვენს კომპიუტერზე, ტაბლეტზე ან მობილურ მოწყობილობაზე.

Spyware არის მაგნე პროგრამა, რომელიც ფარულად, ნებართვის გარეშე აკონტროლებს კომპიუტერის მომხმარებლის საქმიანობას და გადასცემს ინფორმაციას პროგრამის ავტორს.

ტროას ცხენი, მაგნე პროგრამის ერთ-ერთი ყველაზე საშიში სახეობაა. როგორც წესი, ისინი მომხმარებლის მოწყუების მიზნით თავს წარმოაჩენენ როგორც სასარგებლო და სისტემაში შესვლის შემდეგ, თავდამსხმელები იღებენ უნებართვო წვდომას კომპიუტერზე. ამ მომენტიდან მოყოლებული, ისინი შეიძლება გამოყენებულ იქნას ფინანსური ინფორმაციის მოსაპარად ან მაგნე პროგრამების სხვა ფორმებით, ხშირად გამოსასყიდის პროგრამების დასაყენებლად.

Ransomware არის მაგნე პროგრამის ტიპი ბლოკავს თქვენს მოწყობილობას და/ან შიფრავს თქვენს ფაილებს, შემდეგ კი გაიძულებთ გადაიხადოთ გამოსასყიდი წვდომის აღსადგენად. გამოსასყიდი პროგრამის კოდი ადვილად ხელმისაწვდომია ონლაინკრიმინალური ბაზრების საშუალებით და მისგან დაცვა

ძალიან რთულია. მიუხედავად იმისა, რომ გამოსასყიდი პროგრამების შეტევები ფიზიკურ პირებზე ამ დროისთვის შემცირდა, ბიზნესებზე თავდასხმები გაიზარდა 365 პროცენტით. ამის მაგალითია **Ryuk** გამოსასყიდი პროგრამა, რომელიც კონკრეტულ მიზნად ისახავს მაღალი დონის ორგანიზაციებს, რომლებსაც აქვთ დიდი გამოსასყიდის გადახდის მეტი შანსი.

Rootkit არის მავნე პროგრამა, რომელიც თავდამსხმელს ინფიცირებულ სისტემაზე ანიჭებს წვდომის ადმინისტრაციულ უფლებებს. ეს პროგრამა, ცნობილია როგორც **"Root"** წვდომა. ეს პროგრამა ასევე შექმნილია იმისთვის, რომ დარჩეს დამალული მომხმარებლისგან, სისტემის სხვა პროგრამული უზრუნველყოფისგან და თავად ოპერაციული სისტემისგან.

Keylogger არის მავნე პროგრამის ნაწილი, რომელიც მომხმარებლის ყველა მოქმედებას კლავიატურაზე ჩანერს, ინახავს და უგზავნის თავდამსხმელს, რომელიც ეძებს მგრძნობიარე ინფორმაციას, როგორიცაა: მომხმარებლის სახელები, პაროლები ან ინფორმაცია საკრედიტო ბარათის შესახებ.

Mavnen kriptomaining არის პროგრამა, რომელსაც ზოგჯერ უწოდებენ დისკზე მაინინგს ან კრიპტოჯაკინგს, არის გავრცელებული მავნე პროგრამა. ის საშუალებას აძლევს გარეშე პიროვნებას თქვენი კომპიუტერის ენერგიის ხარჯზე გამოიყენოს თქვენი კომპიუტერი კრიპტოვალუტების ბიტკოინის ან მონეროს მოსაპოვებლად. მაინერები მონეტებს აგზავნიან საკუთარ ანგარიშზე და არა თქვენს ანგარიშზე. არსებითად, მავნე კრიპტომაინერი ფულის საშოვნელად იპარავს თქვენს რესურსებს.

ექსპლოიტები არის მავნე პროგრამის ტიპი, რომელიც სარგებლობს სისტემის შეცდომებით და დაუცველობით, და თავდამსხმელს აძლევს თქვენს სისტემაზე წვდომის უფლებას. სისტემაში ყოფნისას, თავდამსხმელს შეუძლია მოიპაროს თქვენი ინფორმაცია ან დააინსტალიროს მავნე პროგრამა [70].

ინტერნეტჭიები. უკანასკნელ პერიოდში ყველაზე გავრცელებულია ინტერნეტჭიები. სწორედ ამ სახის ვირუსები უქმნიან დიდ საფრთხეს ინტერნეტის მომხმარებლებს. ინტერნეტჭიების

დიდი ნაწილი არის საფოსტო ჭია, ნაწილი კი არ მიეკუთვნება ამ ჯგუფს. მაგ., **IISWorm.CodeRed, CodeBlue, Worm.SQL.Helken.**

საფოსტო ჭიებს ყოფენ ორ ქვეკლასად: ჭიები, რომელთა გამავებაც ხდება მომხმარებლის ნების გარეშე, თუ მომხმარებელი გახსნის წერილთან მიერთებულ ფაილს. პირველი სახის ჭიები იყენებენ საფოსტო კლიენტის შეცდომებს, რომელიც მოთავსებულია საფოსტო კლიენტ **Outlook**-ში, უფრო სწორად, ინტერნეტბრაუზერში **Internet Explorer**-ში. იყენებს რა შესაბამის კოდს, ვირუსს შეუძლია წერილის დათვალიერებისას დისკზე ავტომატურად შეინახოს წერილთან მიერთებული ფაილი და შემდეგ გაუშვას იგი. ამ სახის ყველაზე გავრცელებულ ვირუსებია **I-Worm.Klez, I-Worm.Avron, I-Worm. Frethem.** მეორე სახის საფოსტო ჭიის პროგრამას, რომელიც მიერთებულია წერილთან, მომხმარებელი რაღაც მოსაზრების გამო, თვითონ უშვებს (ინფიცირებულ ფაილს). სხვადასხვა ფსიქოლოგიური ზემოქმედებით ამისკენ მას უბიძგებს ჭიის შემმუშავებელი. ყველაზე გავრცელებული ხერხია მომხმარებელს ფაილი წარმოუდგინოს, როგორც საჭირო დოკუმენტი, სურათი ან პროგრამა. ჭია ყოველთვის იყენებს „ორმაგ გაფართოებას“. ამ შემთხვევაში, ფაილის სახელია „**Doc1.Do-cpif**“, „**pict.jpg.com.**“ მოცემული პრინციპი გათვლილია იმაზე, რომ საფოსტო კლიენტები არ მიმართავენ ფაილის სრული სახელის ასახვას (თუ ეს სახელი ძალიან გრძელია), ამიტომ მომხმარებელი ვერ ხედავს მეორე გაფართოებას, რეალურს, ანუ მომხმარებელი ფიქრობს, რომ ეს ფაილი არის დოკუმენტი ან სურათი, სინამდვილეში კი ის წარმოადგენს საშემსრულებლო ფაილის ერთ-ერთ გაფართოებას: **EXE, COM, PIF, SCR, BAT, CMD**, და ა. შ. თუ ასეთ ფაილს გავხსნით ჭია, გააქტიურდება. გარდა იმისა, რომ ჭია მრავლდება, მასში შეიძლება ჩაიდოს სხვადასხვა მოქმედების „ბომბი“. მაგ., კომპიუტერზე დააყენოს ტროიანის პროგრამა ან დაფარული ადმინისტრირების უტილიტი, შეატყობინოს ჭიის შემქმნელს კომპიუტერის მისამართი. საბოლოოდ შეიძლება ინფორმაცია განადგურდეს ან შეუძლებელი გახდეს კომპიუტერზე მუშაობა. მაგ., ჭია **I-Worm.Magistr** ასრულებს იმავე მოქმედებებს, რასაც

ცნობილი ვირუსი **WinCIN**-ი შლის **Flash Bios**-ზე ან მყარ დისკზე მოთავსებულ მონაცემებს.

მაკროვირუსები. გავრცელებულ ვირუსებს შორის მეორე ადგილზეა მაკროვირუსები. აღნიშნული ვირუსები წარმოადგენენ მაკროსებს, რომლებიც მოთავსებულია პროგრამული უზრუნველყოფის გარე ფაილში (**Microsoft Office**-ის, **Autocad**-ის, **CorelDRAW**-ის დოკუმენტებში), დოკუმენტის გახსნისას მათი შესრულება წარმოებს მოცემული პროგრამების შიდა ინტერპრეტატორებით. მათი ფართო გავრცელება ხდება **Visual Basic**-ის ინტერპრეტატორის ფართო შესაძლებლობების გამო, რომელიც ინტეგრირებულია **Microsoft Office**-ში. მაკრო ვირუსები უმეტესად გავრცელებულია დიდი მოცულობის დოკუმენტბრუნვის ოფისებში. ასეთი სახის ოფისების მომხმარებლებს (ოპერატორები, მდივნები, ბუღალტრები), დიდი დატვირთულობის გამო, აღარ რჩებათ დრო, ყურადღება დაუთმონ კომპიუტერულ ვირუსებს. ოფისში წარმოებს დოკუმენტების გადაგზავნა ერთი კომპიუტერიდან მეორეში, ვირუსებზე ყოველგვარი შემოწმების გარეშე, განსაკუთრებით მაშინ, როცა კომპიუტერები ჩართულია ლოკალურ ქსელში. ხშირ შემთხვევაში, ადამიანები სათანადო ყურადღებას არ აქცევენ მაკროვირუსებს, რომლებსაც შეუძლიათ დიდი ზიანი მიაყენონ მომხმარებელს. ეს ვირუსები დაწერილია **VBA**-ზე. მათი ინტეგრირება ხდება **Excel**-ის ან **Word**-ის დოკუმენტებში. მათ შეუძლიათ ვინჩესტერის ფორმატიზება, ანუ მასზე მოთავსებული ინფორმაციის წაშლა, ფაილის ან პაროლის მოპარვა და მისი გადაგზავნა ელექტრონული ფოსტით ვირუსის შემქმნელისათვის. ფაქტობრივად, ამ ტიპის ვირუსებს შეუძლიათ ოფისის მუშაობის პარალიზება.

ვირუსული პროგრამების ავტორები დაწვრილებით სწავლობენ ანტივირუსულ პროგრამებს და, შესაბამისად, ახდენენ ვირუსული პროგრამების მოდიფიკაციას მანამ, სანამ არ მიაღწევენ ისეთ შედეგს, რომ არსებულმა ანტივირუსულმა პროგრამებმა ვერ შეძლონ მათი აღმოჩენა და განადგურება. იმისათვის, რომ შემუშავდეს ანტივირუსული პროგრამა, საჭიროა, ვირუსული პროგრამა მოხვდეს იმ ცენტრში, სადაც წარმოებს ანტივირუსუ-

ლი პროგრამების შემუშავება. მხოლოდ ამის შემდეგ ხდება შესაძლებელი, არსებულ ანტივირუსულ პროგრამას დაემატოს ისეთი ფუნქციები, რომლებიც მოახდენენ ვირუსული პროგრამების დედექტირებას, გაუვნებელყოფას.

უკრაინის ანტივირუსული ცენტრის სპეციალისტებისათვის ცნობილია ვირუს **Makro.Word97**-ის 100-მდე და **Makro.W97M/-Marker**-ის 200-მდე მოდიფიკაცია. ეს მოდიფიკაციები ერთმანეთისაგან მნიშვნელოვნად განსხვავდება, რის გამოც საჭიროა, ანტივირუსულ პროგრამებს დაემატოს დეტექტირებისა და მკურნალობის მოდულები. ტროიანის ვირუსული პროგრამები განსხვავდება სხვა ზემოთ განხილული პროგრამებისაგან – არ ახასიათებთ თვითგამრავლება, ერთხელ მოხვდებიან რა კომპიუტერში, ხანგრძლივი დროის განმავლობაში (როგორც წესი, მათ აღმოჩენამდე ან რაიმე მიზეზით ოპერაციული სისტემის გადაყენებამდე) ასრულებენ თავიანთ ფუნქციებს. ამასთან ერთად, მათ არ შეუძლიათ დამოუკიდებელი გადაადგილება სხვა კომპიუტერში. აღნიშნული ვირუსული პროგრამები მაქსიმალურად შეუმჩნეველია და „სასარგებლო“. ხშირად ეს პროგრამები წარმოადგენენ ქსელური და საფოსტო ჭიების თანამგზავრებს. მაგ., საფოსტო ჭია **I-Worm.Lovgate**, მოხვდება რა კომპიუტერში, აყენებს სისტემაში **backdoor** მოდულს, რომელიც შესაძლებლობას აძლევს მას, შეაღწიოს კომპიუტერში და გაუგზავნოს ვირუსული ჭიის შემქმნელს წერილი, რომელშიაც მითითებული იქნება მომხმარებლისა და კომპიუტერის სახელი, დაავადებული კომპიუტერის ქსელური მისამართი.

ტროიანის ვირუსული პროგრამები, მათ მიერ შესრულებული მოქმედებების მიხედვით, იყოფა სამ ჯგუფად:

ლოგიკური (დროითი) „ბომბები“. აღნიშნული ვირუსული პროგრამები პროგრამაში ინფორმაციის მოდიფიკაციას ახდენენ მითითებულ დროს ან ჩადებული პირობის შესრულებისას;

BackDoor პროგრამები. ამ პროგრამების საშუალებით შესაძლებელია კომპიუტერების შორიდან მართვა ან ბოროტმზრახველებისაგან ბრძანებების მიღება (ლოკალური ან გლობალური ქსელების საშუალებით, ელექტრონული ფოსტით). ტროიანის ვირუსული პროგრამების სამივე სახეობა მეტად საშიშია. თითო-

ეულ მათგანს შეუძლია, გაანადგუროს მონაცემები ან მოიპაროს სასარგებლო ინფორმაცია.

უნდა აღინიშნოს, რომ ტროიანის პროგრამების განახლება წარმოებს ხშირად, უშვებენ ახალ-ახალ მოდიფიკაციებს. ამიტომ საჭიროა ანტივირუსული პროგრამული პროდუქტების რეგულარულად განახლება. უკრაინის ანტივირუსული ცენტრი **UNA** ყოველდღიურად უშვებს ანტივირუსულ პროგრამებს. თუ თქვენ ხართ ინტერნეტის აქტიური მომხმარებელი, მაშინ ანტივირუსული პროგრამების განახლებას უნდა მიმართოთ მინიმუმ, კვირაში ერთხელ. კარგი იქნება, თუ ამას გავაკეთებთ ყოველდღიურად.

ვირუსები დესტრუქციული მოქმედებების მიხედვით იყოფა სამ ჯგუფად:

- ინფორმაციული ვირუსები;
- აპარატურული ვირუსები;
- ფსიქოტროპული ვირუსები.

ინფორმაციული ვირუსები, რომლებსაც პირველი თაობის ვირუსებსაც უწოდებენ, დღეისათვის ყველაზე გავრცელებული ვირუსებია. მათი ძირითადი დანიშნულებაა ინფორმაციის განადგურება, მოდიფიკაცია ან მოპარვა.

ანტიაპარატურულ ვირუსებს (მეორე თაობის ვირუსები) შეუძლიათ მწყობრიდან გამოიყვანონ კომპიუტერის აპარატურული ნაწილი. მაგ., ნაშალონ **BIOS** ან გააფუჭონ მყარი დისკის ლოგიკური სტრუქტურა ისე, რომ შემდგომში შეუძლებელი გახდეს ფორმატიზაციის გარეშე მისი გამოყენება. ამ ტიპის ვირუსებიდან ყველაზე საშიშია „ჩერნობილი“ - **Win95.CIH**. თავის დროზე ამ ვირუსმა მწყობრიდან გამოიყვანა მილიონობით კომპიუტერი, გაანადგურა მყარ დისკზე არსებული ინფორმაცია ისე, რომ შეუძლებელი გახდა მისი აღდგენა. ასეთი ვირუსებისაგან თავდაცვის მიზნით, დედა პლატაზე შესაძლებელია სპეციალური ჯამპერების დაყენება, რომლებიც დაბლოკავენ **BIOS**-ზე ინფორმაციის ჩანერას.

ფსიქოტროპული ვირუსები (მესამე თაობის ვირუსები). ასეთ ვირუსებს შეუძლიათ ადამიანის მოკვლა. ინვეეს რა განსაზღვრული სიხშირის ბგერების განმეორებას, ან ეკრანზე სხვადასხვა ფერების ციმციმს, ფსიქოტროპულ ვირუსს ეპილეფსიით დაავადებულ ადამიანებში შეუძლია გამოიწვიოს ეპილეფსიური შეტევა, გულის გაჩერება, ტვინში სისხლის ჩაქცევა. ბევრი სპეციალისტი მათ არსებობას ეჭვქვეშ აყენებს, თუმცა დიდი ხანია გამოგონილია ადამიანზე ზემოქმედებისათვის ფსიქოტროპული ტექნოლოგია – განსაზღვრული მეთოდით ბგერებით ან გამოსახულებით ზემოქმედება (ეს განსხვავდება 25-ე კადრისაგან).

ზომბები (Zombie) – ეს არის ვირუსული პროგრამები, რომლებიც ქსელში ჩართულ კომპიუტერში მოხვედრისას გარედან იმართებიან და გამოიყენებიან ბოროტმოქმედის მიერ სხვა კომპიუტერზე იერიშის მისატანად.

ქსელში გაერთიანებული დაავადებული კომპიუტერის მეშვეობით, ელექტრონული ფოსტით იგზავნება დიდი მოცულობის არასასურველი მონაცემები, ვირუსები და სხვა პროგრამები. მაგ., იაპონიაში მულტფილმ „პოკემონები“-ს ერთ-ერთი სერიის ჩვენების შემდეგ ასობით ბავშვი მოხვდა საავადმყოფოში, მათ აღენიშნებოდათ ძლიერი თავის ტკივილი და ტვინში სისხლის ჩაქცევები, ზოგიერთი მათგანი გარდაიცვალა კიდევ. მულტფილმში ჩადებული იყო პალიტრის ნათელი ფერების გენერაციის კადრები. ეს იყო გარკვეული თანმიმდევრობის წითელი აფეთქებები შავ ფონზე. აღნიშნული შემთხვევის შემდეგ ამ მულტფილმის ჩვენება იაპონიაში აიკრძალა. კიდევ ერთი მაგალითი: რუსეთისა და იაპონიის ნაკრებების თამაშის შემდეგ მაყურებლები ამსხვრევდნენ ირგვლივ ყველაფერს. აღნიშნული მოქმედებისაკენ მათ უბიძგა თამაშის ტრანსლაციის დროს ნაჩვენებმა რგოლმა, რომელშიც ასახული იყო, თუ როგორ ამსხვრევენ ადამიანები საცემი ჯოხებით მანქანებს.

ჯაშუშური პროგრამები (Spyware) არის პროგრამული პროდუქტი, რომელიც კომპიუტერში ხვდება მისი მფლობელის სურვილის გარეშე. ამ პროგრამის მიზანს წარმოადგენს კომპიუტერში არსებულ კონფიდენციალურ მონაცემებთან შეღწევა. ეს პროგრამები კომპიუტერებში ხვდება ქსელის ჭიისგან ტროიანის

პროგრამის მეშვეობით, როგორც თითქოს ეს სარეკლამო (**ad-ware**) ხასიათის ინფორმაციაა. პროგრამა-ჯაშუშები – ეს ისეთი ვირუსული პროგრამებია, რომლებსაც შეუძლიათ შეაგროვონ ინფორმაცია (სახელები, პაროლები), დაალაგონ და მასალები ელექტრონული ფოსტიდან სხვა მეთოდებით გადასცენ პროგრამის შემმუშავებლებს. ჯაშუშური პროგრამის ერთ-ერთ სახეობას წარმოადგენს ფიშინგგამგზავნები.

ფიშინგი (Phishing) – ეს პროგრამა არის საფოსტო გამგზავნი, რომლის მიზანიც კონფიდენციალური ფინანსური ინფორმაციის მიღებაა. ასეთი წერილი, როგორც წესი, მოიცავს საიტზე მიმართვას, რომელიც წარმოადგენს ინტერნეტბანკის ზუსტ ასლს, ან სხვა ფინანსურ დაწესებულებას. მომხმარებელი ამ შემთხვევაში ვერ ხვდება, რომ იმყოფება ყალბ საიტზე, ხშირად აწვდის ბოროტმზრახველებს ინფორმაციას თავისი ანგარიშის, საკრედიტო ბარათისა და პაროლის შესახებ.

ფარმინგი ფიშინგის შენიღბული ფორმაა, რომლის მიხედვითაც მომხმარებელი, ნაცვლად იმისა, რომ შევიდეს ინტერნეტბანკის ან სხვა ორგანიზაციის ნამდვილ საიტზე, ვირუსული პროგრამის საშუალებით ავტომატურად გადასამისამართდება ყალბ საიტზე, რომლის გარჩევაც ოფიციალური საიტისაგან მეტად ძნელია. ფარმინგის ძირითად მიზანს წარმოადგენს, ხელში ჩაიგდოს მომხმარებლის პირადი ფინანსური ინფორმაცია.

კომპიუტერული სისტემების დანერგვისას და სხვადასხვა ობიექტების მართვისას, მომხმარებელს ხშირად სთავაზობენ ისეთ პროგრამულ უზრუნველყოფას, რომელსაც სათანადო ექსპერტიზა არ გაუვლია. პროგრამულ პროდუქტში დაშვებულმა შეცდომებმა შეიძლება თავი იჩინოს პრაქტიკული ამოცანების რეალიზაციის დროს, ისეთი სიტუაციების წარმოშობისას, რომელიც არ იყო გათვალისწინებული პროგრამული უზრუნველყოფის შემუშავებისას. ასეთი პროგრამული უზრუნველყოფით სარგებლობამ მომხმარებელს შეიძლება მიაყენოს დიდი ეკონომიკური და მორალური ზარალი და მრავალი პრობლემა გაუჩინოს. არასასურველი შედეგი შეიძლება მივიღოთ მაშინაც, როცა პროგრამული პროდუქტი არასწორადაა გამოყენებული, რაც შეიძლება მომხმარებლის დაბალმა კვალიფიკაციამ გამოიწვიოს.

საზოგადოების საყოველთაო ინფორმატიზაცია უთუოდ გამოიწვევს კომპიუტერულ დანაშაულებათა ახალი სახეობების აღმოცენებას, ამიტომ აუცილებელია მომზადდეს იურისტთა ისეთი კატეგორია, რომელიც ღრმად გაერკვევა კომპიუტერულ დანაშაულებათა არსში და, სათანადო საკანონმდებლო აქტების არსებობის პირობებში, წარმატებით განახორციელებს აღნიშნულ დანაშაულებათა პროფილაქტიკას, გამოძიებასა და დამნაშავის სათანადო დასჯას. ასეთი სახის ინფორმატიკოს-იურისტების მომზადება საჭიროა საქართველოშიც, პირველ რიგში, თბილისის სახელმწიფო უნივერსიტეტში.

დღეისათვის ასეთ დამნაშავეთა წინააღმდეგ ბრძოლის სიძნელე იმაში მდგომარეობს, რომ ამ პროცესში მონაწილე იურისტებს, ხშირ შემთხვევაში, არ ესმით საკითხის სპეციფიკურობა, ამიტომაც მათ არ შეუძლიათ სწორი კვალიფიკაცია მისცენ ჩადენილ დანაშაულს. ხშირად ისინი უარს ამბობენ კომპიუტერული დანაშაულის გამოძიებაზე. კომპიუტერული დანაშაულის გახსნას ხელს უშლის ისიც, რომ დამნაშავეები არ ტოვებენ რაიმე ხელშესახებ კვალს, ხშირ შემთხვევაში, ძნელია აღმოაჩინო დანაშაულის დამამტკიცებელი მატერიალური ფაქტი და, შესაბამისად, დაამტკიცო იგი სასამართლო პროცესზე. აღნიშნულს ისიც ემატება, რომ უმეტეს შემთხვევაში, დაზარალებული (მაგალითად, ბანკის მფლობელი) არ მიმართავს სასამართლო ორგანოებს, ეშინია, ამათ არ გამოიწვიოს კომერციული ნდობის დაკარგვა კლიენტებში.

კომპიუტერულ სისტემებთან დაკავშირებული დანაშაულებები შეიძლება შემდეგნაირად დავაჯგუფოთ: ფიზიკური, ტექნიკური და ინტელექტუალური.

ფიზიკურ კომპიუტერულ დანაშაულებებს მიეკუთვნება: კომპიუტერული სისტემების მოტაცება, ყაჩაღური თავდასხმა, ფიზიკური განადგურება, ტერორისტული აქტების განხორციელება, ხანძრისა და წყალდიდობისას კომპიუტერული სისტემების მწყობრიდან გამოყვანა და სხვა საგანგებო სიტუაციები.

ტექნიკურ კომპიუტერულ დანაშაულს მიეკუთვნება: კომპიუტერულ სისტემაში არსებული ინფორმაციის დამახინჯება, მისი განადგურება, ინფორმაციის გაყალბება და სხვ.

ინტელექტუალურ კომპიუტერულ დანაშაულს მიეკუთვნება:

თაღლითური ოპერაციების წარმოება, მოვალეობის შეუსრულებლობა, ფსიქოლოგიური ზემოქმედება, აგენტური დაზვერვა, სისტემაში არსებულ ინფორმაციაზე არასანქცირებული მიმართვა და ა.შ.

კომპიუტერული სისტემის მწყობრიდან გამოყვანისა და სისტემის რესურსებით უკანონოდ სარგებლობის მიზნით, დამნაშავემ უნდა განახორციელოს სხვადასხვა კანონსაწინააღმდეგო აქტები: გამორთოს ან შეცვალოს სისტემის დაცვის მექანიზმი, სისტემაში შევიდეს რეალური მომხმარებლის სტატუსით, ისარგებლოს სისტემის დაცვის მექანიზმში არსებული ხარვეზებით. ხშირ შემთხვევაში, ბოროტმოქმედნი სხვადასხვა გზით ადგენენ მომხმარებლის პაროლს (მაგალითად, ჩადებული პროგრამების საშუალებით. ეს ისეთი პროგრამებია, რომლებიც კლავიატურიდან შეტანილ პაროლებს ინახავს მისთვის განკუთვნილ ადგილას) – ან პაროლის შეტანის პროგრამის გამორთვით, ან კიდევ მომხმარებლის მიერ კლავიატურაზე პაროლის აკრეფის მომენტში მისი დაფიქსირებით და შემდეგ მისი სახელით ახერხებენ ამ სისტემაში შესვლას.

კომპიუტერული დამნაშავეები, დანაშაულის ჩადენის მიხედვით, შეიძლება დავაჯგუფოთ, როგორც ჰაკერები-გამდიდრების მიზნით დანაშაულის ჩამდენები და ექსტრემისტული და ტერორისტული დაჯგუფებები. გამდიდრების მიზნით დანაშაულის ჩამდენი ცდილობს მიიღოს ან კომერციული ინფორმაცია, ან მოახერხოს დისტანციური შესვლა საბანკო სისტემაში და მიითვისოს ფულადი თანხები. შესაძლებელია, კონკურენტებთან ბრძოლის მიზნით, კომპიუტერულ სისტემაში სხვადასხვა ორგანიზაციებმა და სტრუქტურებმა განახორციელონ სამრეწველო შპიონაჟი.

კომპიუტერული დანაშაული, აღმოცენების ხასიათის მიხედვით, შეიძლება იყოს განზრახული და არა-განზრახული; სახეების მიხედვით – პროგრამული და არა-პროგრამული; აღმოცენების ადგილის მიხედვით – კომპიუტერული სისტემის ფარგლებში და გარეთ; აღმოცენების მიზეზის მიხედვით – უწესრიგობა სისტემის ფიზიკურ ნაწილში, შეცდომები პროგრამულ უზრუნველ-

ყოფაში, საარქივო ინფორმაციის არასწორი შენახვა, არასანქცირებული შეღწევა კომპიუტერულ სისტემებში.

პროგრამული გზით დანაშაულის ჩადენას ბოროტმოქმედი აღწევს სხვადასხვა ფუნქციური დანიშნულების პროგრამების გამოყენების საფუძველზე. აღნიშნულის გარდა, განვიხილოთ კიდევ რამდენიმე მათგანი:

ტრაფიკის ანალიზის პროგრამა აანალიზებს მომხმარებლის სისტემასთან მიმართვის მეთოდებსა და სიხშირეს. ამ გზით დანაშავე აღგენს მომხმარებლის სისტემასთან დაკავშირების წესს და ცდილობს, კანონიერი მომხმარებლის სახელით კავშირი დაამყაროს სისტემასთან.

მონაცემების ხელმეორედ გამოყენების პროგრამა სისტემიდან ამოგდებულ მონაცემებს აღადგენს და განმეორებით გამოიყენებს. აღნიშნულის ანალოგიურია პროგრამა, რომელსაც შეუძლია ე.წ. კომპიუტერული „ნაგვის“ შეგროვება, მისი ანალიზი და ანალიზის შედეგად იმის დადგენა, თუ რა საქმიანობას ეწევა მომხმარებელი. კერძოდ, დაადგინოს მომხმარებლის კომერციული ინფორმაცია.

მომხმარებლის მომსახურების შეწყვეტის პროგრამა. აღნიშნული პროგრამის გამოყენება ბოროტმოქმედს საშუალებას აძლევს, შეაწყვეტინოს სისტემას მომხმარებლის ამოცანის ამოხსნა, თავის ხელში აიღოს მანქანური რესურსები და ამოხსნას საკუთარი ამოცანები.

პროგრამა „სალიამის იერიში“ – ასეთი პროგრამით ხშირად სარგებლობენ ბანკის კომპიუტერული სისტემის თანამშრომლები. აღნიშნული პროგრამა დამნაშავის მიერ ფარულად გახსნილ სპეციალურ ანგარიშზე აწარმოებს ფულის მცირე საზომი ერთეულების მერამდენ ნაწილის დაგროვებას (მაგალითად, კაპიკის, ცენტის ან თეთრის მეათასედი ნაწილის დაგროვებას). ასეთი წესით შეიძლება დაგროვდეს საკმაოდ სოლიდური თანხა, რომელსაც შემდეგ ბოროტმოქმედი მიითვისებს.

პროგრამა რეპლიკატორი. ეს ისეთი პროგრამაა, რომელსაც შეუძლია სისტემაში შექმნას თავისი ასლები, რაც იწვევს მეხსიერების გადავსებას, სისტემის მუშაობის შეწყვეტას. ზოგიერთი

პროგრამა-რეპლიკატორი დამატებით სხვა ფუნქციებსაც ასრულებს.

კომპიუტერული დანაშაულის ჩადენა შეიძლება არა მარტო ინფორმაციის მიღების, არაკანონიერი გზით ფულის მითვისების, არამედ თვით კომპიუტერული სისტემის ხელში ჩაგდების მიზნითაც.

დღემდე, კომპიუტერული სისტემებით ინფორმაციის დამუშავების უსაფრთხოებას განსაკუთრებულ ყურადღებას უთმობენ მხოლოდ სამხედრო ორგანიზაციები და სამეცნიერო წრეები, რომელთა ინფორმაციის საიდუმლოების დაცვასაც ემსახურებიან სახელმწიფო სასამართლო ორგანოები. საბაზრო ეკონომიკის პირობებში, თითქმის დაუცველი აღმოჩნდა ფირმების, სახელმწიფო დაწესებულებებისა და კერძო პირთა ინფორმაცია.

დამატებით განვიხილოთ დღეისათვის არსებული ყველაზე საშიში ვირუსები:

Mydoom-ი საშინელი ვირუსია მის მიერ მიყენებული ზარალი სავარაუდოდ 38,5 მილიარი დოლარია. 2004 წლის იანვარში, **Mydoom**-ი სწრაფად გავრცელდა ელექტრონული ფოსტით. ზოგიერთი მონაცემის მიხედვით, 2004 წელს ხელწერილების 16-25% ვირუსით იყო გენერირებული. სპამის შეტყობინებების დიდმა მოცულობამ გადატვირთა კომპიუტერები. ზოგიერთი ბიზნესი იძულებული გახდა პრობლემების გადასაჭრელად რამდენიმე დღით დაეხურა ორი კომპანია, რომელმაც ყველაზე დიდი ზარალი განიცადა – **SCO Group** და **Microsoft**. 2004 წლის 1 თებერვალს გამოვიდა **Mydoom**-ის პირველი ვერსია, რომელიც შეიცავდა ბრძანებას **SCO** ჯგუფის სერვერზე **DoS** შეტევების შესასრულებლად. ორი დღის შემდეგ გამოვიდა მეორე ვერსია, რომელიც მიზნად ისახავდა **Microsoft**-ს. **Microsoft**-ზე თავდასხმის ეფექტი მინიმალური იყო, მაგრამ **SCO Group**-ი იძულებული გახდა წინასწარ დაეხურა ვებ-საიტი, რაც კომპანიის ძვირად დაუჯდა.

ვირუს **Sobig**-ის მიერ მიყენებულმა ზარალმა დაახლოებით 30 მილიარდი დოლარი შეადგინა. მისი გავრცელება მოხდა ელექტრონული ფოსტის სპამის მეშვეობით. მისმა ვერსიამ – **Sobig**-

მა გამორთო მასაჩუსეტის ტექნოლოგიური ინსტიტუტის ელექტრონული ფოსტის სერვერი. სადაც განთავსებული იყო მონაცემები კომპიუტერული და ელექტროინჟინერიის საბაკალავრო პროგრამების შესახებ.

ვირუსი **Klez**-ის მიერ მიყენებულმა ზარალმა დაახლოებით 20 მილიარდი დოლარი შეადგინა. სხვა ვირუსების მსგავსად იგი ვრცელდება ელექტრონული ფოსტით. მისი გავრცელება ხდება უბრალოდ ფოსტის გახსნის შედეგად. მან გავრცელება დაიწყო 2001 წლიდან.

ვირუსი **Conficket**. სავარაუდოდ ამ ვირუსის დაინფიცირების შედეგად მიყენებულმა ზარალმა 9 მილიარდი დოლარი შეადგინა. იგი 2008 წლის 21 ნოემბერს გამოჩნდა და 11 მილიონ კომპიუტერში ჩატვირთული ოპერაციული სისტემა Windows დააზიანა. ვირუსის გავრცელება მოხდა სხვადასხვა გზით, მათ შორის მოსახსნელი დისკების საშუალებით.

2000 წელს ვირუსმა რომანტიული სახელით **ILOV** დააინფიცირა 20 მილიონი კომპიუტერი. ვირუსი გავრცელდა ელექტრონული ფოსტით. წერილი სათაურით **ILOVEYOU** შეიცავდა ფაილს LOVE-LETTER-FOR-YOU.txt.vbs (ინგლისური – **"love letter for you"**). ნებისმიერი მომხმარებელი, რომელიც დაინტერესებული იყო იმის გასარკვევად, თუ ვინ გაუგზავნა მათ სასიყვარულო შეტყობინება, სწრაფად ხსნიდა ფაილს, რაც საკმარისი იყო კომპიუტერის დაინფიცირებისთვის. **ILOVEYOU** ვირუსი გავრცელდა ელექტრონული ფოსტით.

ვირუსი **Zeus**. ზევსი არის ტროას ბოტნეტის ვირუსი. ის ძირითადად ვრცელდება ელექტრონული ფოსტით, და დისკზე ჩამოტვირთვების საშუალებით, **Zeus**-ის ერთ-ერთი სამიზნეა ფინანსური ინსტიტუტები. როგორც კი კომპიუტერი დაინფიცირდება, ის ბოტნეტის ნაწილი ხდება. ყველა ინფიცირებული ბოტი დაუყოვნებლივ აძლევს „ბოტის მფლობელს“ უსაფრთხოების სისტემების გვერდის ავლით აკონტროლოს ბოტნეტის ყველა კომპიუტერი. საიტზე ასეთი წვდომით ჰაკერს შეუძლია განახორციელოს მასობრივი თავდასხმები: **DdoS**-ზე, განახორციე-

ლოს მასიური გატეხვები, მონაცემთა გაჟონვა, ქურდობა ონლაინბანკებიდან და სხვ.

ვირუსი **WannaCryptor**, ანუ მოკლედ **WannaCry**, ერთ-ერთი ყველაზე დამანგრეველი და დაუნდობელი ვირუსია. ეს არის გამოსასყიდი პროგრამა. როდესაც კომპიუტერი ინფიცირდება, ის შიფრავს ყველა ფაილს და ითხოვს გამოსასყიდს ბიტკოინებში. თუ მომხმარებელი უარს იტყვის გამოსასყიდის გადახდაზე, მას შეუძლია სამუდამოდ დაემშვიდობოს თავის მონაცემებს. მართალია, ვირუსი **WannaCry** არ იყო ჭკვიანი ვირუსი, თუმცა მან აირჩია სწორი სამიზნეები, რითაც მან მაქსიმალური ზიანი მიაყენა ქსელში ჩართულ კომპიუტერებს. ერთ მომენტში ფრანგული ავტომწარმოებელი – Renault-ი იძულებული გახდა საშინელი ვირუსის გავრცელების თავიდან ასაცილებლად დაეხურა თავისი ევროპული ქარხნები. **WannaCry**-ის მსხვერპლთა შორის იყვნენ საავადმყოფოები, ავიახაზები, ფინანსური ინსტიტუტები და მიწოდების წამყვანი საერთაშორისო კომპანია FedEx-ი [69].

13.3. კომპიუტერული დანაშაულებებისა და ინფორმატიზაციის უარყოფითი შედეგების აღმოფხვრის ღონისძიებები და საშუალებები

ვირუსებით კომპიუტერის დაავადების დროს მნიშვნელოვანია მათი დროული აღმოჩენა და შემდეგ განადგურება. საჭიროა ვიცოდეთ ის სიმპტომები, რომელიც დამახასიათებელია დაავადებული კომპიუტერისთვის:

- ხშირად ავტომატურად გადატვირთვა და „ჩამოკიდება“;
- ჩატვირთვისა და პროგრამის შესრულების შენელება;
- შესასრულებელი პროგრამების ზომების გაზრდა;
- ხელმისაწვდომი მეხსიერების მოცულობის შემცირება;
- კომპიუტერი არ ასრულებს კითხვა-პასუხების ოპერაციებს და ადგილი აქვს დისკმდების ნათურის ციმციმს.

კომპიუტერული სისტემების უსაფრთხოებისა და კომპიუტერული დანაშაულის წინააღმდეგ ღონისძიებები შეიძლება შემდეგნაირად დაჯგუფდეს:

- კომპიუტერული სისტემების კომპონენტების ფიზიკური უსაფრთხოების დაცვა;
- კომპიუტერული სისტემების კომპონენტების ლოგიკური უსაფრთხოების უზრუნველყოფა;
- კომპიუტერული სისტემების კომპონენტების სოციალური უსაფრთხოების დაცვა;
- კომპიუტერული სისტემების ეთიკური უსაფრთხოების დაცვა.

კომპიუტერული სისტემების ფიზიკური განადგურებისაგან უსაფრთხოების ღონისძიებები მოიცავს: კომპიუტერული სისტემების დაცვას წყალდიდობებისაგან, მოპარვისაგან, ხანძრისაგან, ელექტროენერგიის მომარაგებაში შეფერხებისა და სხვა სტიქიური უბედურებებისაგან.

ელექტროენერგიის მოკლე დროით გამორთვისას მონაცემების დაკარგვის თავიდან აცილების მიზნით, აუცილებელია შეუფერხებელი კვების წყაროს დამონტაჟება. უწყვეტი კვების წყაროს მოწყობილობები ერთმანეთისაგან განსხვავდებიან ტექნიკური მახასიათებლებით და სამომხმარებლო თვისებებით. მათ შეუძლიათ, დროებით დენით მოამარაგონ, როგორც ლოკალური გამოთვლითი ქსელები, ასევე ცალკეული კომპიუტერები და სერვერები. აღნიშნული მომხმარებელს საშუალება მისცეს, შეინახოს ინფორმაცია მაგნიტურ მატარებლებზე. საკმაოდ გავრცელებულია ამერიკული წარმოების შეუფერხებელი კვების წყაროები. მაგ., **Smart-UPS 2000**, ფირმა **APS (American Power Conversion)**, რომელსაც შეუძლია, ელექტროენერგიის გამორთვის შემთხვევაში, 3-4 საათის განმავლობაში უზრუნველყოს კომპიუტერი დენით. აუცილებელია აგრეთვე, ბანკს გააჩნდეს სარეზერვო ელექტროენერგიის კვების ხაზი.

კომპიუტერული სისტემების ლოგიკური უსაფრთხოების უზრუნველყოფაში შეიძლება გავაერთიანოთ: სისტემაში არა-

სანქცირებული მიმართვის დაცვის ღონისძიებები, ადამიანისა და პროგრამების მოქმედებაში განზრახ და უნებურად დაშვებული შეცდომები. ქსელის პროგრამული უზრუნველყოფის დონეზე შეიძლება ჰაკერების მხრიდან განხორციელდეს შემდეგი სახის იერიში: არხების მოსმენა, რაც შესაძლებელია ლოკალური ქსელის სეგმენტში განხორციელდეს. ჰაკერი ქსელში ქმნის ცრუ მარშრუტიზატორს, რისთვისაც ქსელში გზავნის განსაზღვრული სახის პაკეტს, რომლის შედეგადაც ჰაკერის კომპიუტერი ხდება მარშრუტიზატორი და მას ეძლევა შესაძლებლობა, განახორციელოს იერიში. ჰაკერს შეუძლია ქსელში გაგზავნოს ცრუ უკუმისამართი და ნამდვილი მომხმარებლის ნაცვლად ჩაერთოს ქსელში. ამ შემთხვევაში ჰაკერის უფლებამოსილება დაუკავშირდეს სერვერს იგივეა, რაც ნამდვილი მომხმარებლისა.

კომპიუტერული სისტემების კომპონენტების სოციალური უსაფრთხოების დაცვა გულისხმობს ისეთი საკანონმდებლო აქტების შემუშავებას, რომელიც ხელს ააღებინებს პიროვნებას დანაშაულის ჩადენაზე ან მისი დასჯის საფუძველს ჩადენილი დანაშაულისათვის.

კომპიუტერული სისტემების ეთიკური უსაფრთხოების უზრუნველყოფა გულისხმობს კომპიუტერზე მომუშავეთა მიერ წინასწარმედგენილი ეთიკური დისციპლინარული ნორმების დაცვას. აღნიშნული დისციპლინარული ნორმების მსგავსი „კოდექსი კომპიუტერული სპეციალისტების ქცევის შესახებ“ შემუშავდა აშშ-ის ნაციონალური სამეცნიერო ფონდის ექსპერტების მიერ. ამ კოდექსის მიხედვით არაეთიკურად ითვლება:

- კომპიუტერული სპეციალისტის წინასწარგანზრახული ან უნებლზე მოქმედება, რომელმაც გამოიწვია კომპიუტერული სისტემის ნორმალური ფუნქციონირების დარღვევა, მანქანური და სხვა სახის რესურსების დამატებითი ხარჯვა;
- კომპიუტერში შენახული ან დასამუშავებელი ინფორმაციის მთლიანობის დარღვევა;
- კანონიერი მომხმარებლის ინტერესების დარღვევა;
- სისტემის დარღვეული ნორმალური ფუნქციონირების აღსადგენად დაუგეგმავი დანახარჯების გაღება.

როგორც აღვნიშნეთ, კომპიუტერული სისტემების ნორმალურ მუშაობას დიდ ზიანს აყენებს მათი დაავადება ვირუსული პროგრამებით. ვირუსული პროგრამების ზრდის პარალელურად, მიმდინარეობს სამუშაოები ანტივირუსული პროგრამების შესამუშავებლად, კომპიუტერულ სისტემებში უკანონოდ შეღწევის აღმოსაფხვრელად. ჰაკერები ვირუსულ პროგრამებს ქმნიან ნინასწარგანზრახული მიზნების განსახორციელებლად, მაგალითად, ამა თუ იმ ოპერაციული სისტემის ნორმალური მუშაობის შესაფერხებლად. ასეთი ვირუსული პროგრამები შექმნილი იყო საკმაოდ ცნობილი ოპერაციული სისტემების **MS DOS, IBM OS/2, Windows-3.1, Windows-95** და მასთან თავსებადი ოპერაციული სისტემების მუშაობის შესაფერხებლად. მიუხედავად იმისა, რომ ოპერაციულ სისტემა **IBM OS/2**-ს სხვა ოპერაციული სისტემებისაგან განსხვავებით გააჩნია ვირუსულ პროგრამებში შესვლის მაღალი ეფექტური დაცვა, მაინც წარმოებს ამ სისტემაში შესაღწევად ვირუსული პროგრამების შემუშავება.

ქსელური ოპერაციული სისტემებიდან ყველაზე დაცულია სისტემა **Novel Net War**.

როგორც ყოფილ საბჭოთა კავშირის სივრცეში, ასევე საზღვარგარეთ, შექმნილია ფირმები, რომლებიც შეიმუშავებენ ანტივირუსულ პროგრამებს, მუშაობენ კომპიუტერული სისტემების უსაფრთხოების უზრუნველსაყოფად. მაგალითად, რუსეთში ფირმა - **АО-„Диалог Наука“** და მის მიერ შემუშავებული პროგრამები: **Aidstest, Dr. Web For, WinWor**; საზღვარგარეთული ფირმები: ფირმა **F Culasso**, პროგრამა **F-Prot v.1.14a**; ფირმა **Sophos Ltd**, პროგრამა - **Vacci-nev. 4.23.**; გარდა აღნიშნულისა ანტივირუსული პროგრამების შემმუშავებელი ფირმებია: **McAfee, Centra Point Panda, ESET, 3AO «კასპერსკის ლაბორატორია», IBM S@S International, Symantec** და სხვ. პრაქტიკაში ფართოდ გამოიყენება **OS/2** ოპერაციული სისტემისათვის შექმნილი ანტივირუსული პროგრამა.

მოქმედების მიხედვით ანტივირუსული პროგრამები შეიძლება დავაჯგუფოთ შემდეგ კატეგორიებად: პოლიფაგები, რევიზორები და ვაქცინები.

- პოლიფაგებს შეუძლიათ კომპიუტერული ვირუსების აღმოჩენა და განადგურება;
- რევიზორები მომხმარებლებს ატყობინებს კომპიუტერის ბოლო შემონმების შემდეგ ფაილების სტრუქტურასა და შინაარსში მომხდარ ცვლილებებს. ისინი არ ახდენენ ფაილების ტესტირებას ვირუსებზე და მათ მოსპობას;
- ვაქცინის (იმუნატორის) დანიშნულებაა, დაიცვას ფაილები განსაზღვრული სახის ფაილებისგან.

ანტივირუსული პროგრამების მუშაობის ეფექტიანობა შეიძლება გაიზომოს რამდენიმე პარამეტრით:

- მეხსიერებაში, ასევე, ფაილებში განთავსებული ვირუსების აღმოჩენა და იდენტიფიცირება;
- რამდენად ეფექტურია ვირუსების განკურნება, ანუ აღმოჩენილი ვირუსებიდან პროცენტულად რა რაოდენობის ვირუსებს სპობს იგი;
- რამდენი დროა საჭირო ტესტირებისათვის;
- როგორია მისი ფასი;
- რამდენად მარტივია მომხმარებლისათვის მისი გამოყენება;
- ახალი ვირუსების გავრცელების სიმარტივე და სიხშირე;
- გამავრცელებლების მხრიდან მომსახურების შესაძლებლობა;
- ლოკალურ ქსელში მუშაობის შესაძლებლობა;
- ტესტირების შედეგების ანგარიშის შედგენა;
- საჭირო მეხსიერების მოცულობა.

აღმოჩენა, იდენტიფიცირება, მოსპობა და ფაილების აღდგენა.

გასული საუკუნის ბოლოსთვის მომხმარებელი ყველაზე მეტად იყენებდა და ენდობოდა შემდეგი ფირმების მიერ შემუშავებულ ანტივირუსულ პროგრამებს: **Kaspersky-„kasperskis laboratoria“**; **Virex**-ფირმა **Microcom**; ანტივირუსული პროგრამა **Antivirus**, ფირმა **Centra lPoin tSoftWare** და პაკეტი **Norton Antivirus** ფირმა **Symantec**. **АО „Диалог Hayka“**-ს მიერ შემუშავებული

ანტივირუსული კომპლექტი: **Aidstest, Doctor Web , WinWor** და სხვ.

ანტივირუსული პროგრამების მიღება შეიძლება ანტივირუსული პროგრამების შემმუშავებელი ფირმებიდან ელექტრონული განცხადებების დაფის **BBS**-ის, **FTR**-სერვისის ან გლობალური ჰიპერტექსტური სისტემა **WWW**-ს საშუალებით.

კომპიუტერული ვირუსებით დაავადების თავიდან აცილების მიზნით, პროგრამული საშუალებების გამოყენების გარდა, საჭიროა გატარებულ იქნეს ორგანიზაციულ-პროფილაქტიკური ღონისძიებები:

- უნდა მოვერიდოთ საკუთარი დისკების სხვისთვის გადაცემას;

- არ უნდა მივცეთ უფლება სხვა პირებს თავიანთი დისკებით იმუშაონ ჩვენს კომპიუტერზე;

- არ დაუშვათ არალიცენზირებული გზით შეძენილი პროგრამების გამოყენება;

- კომპიუტერზე მუშაობის დაწყებამდე საჭიროა, ანტივირუსული პროგრამების გაშვება;

- საჭიროა დისკებზე ჩაწერილი პროგრამების გადანერა სხვა დისკებზე. აღნიშნულის განხორციელება საშუალებას მოგვცემს, სხვისთვის მიცემული დისკის დაბრუნების შემთხვევაში, მოვახდინოთ ამ დისკის ფორმატიზაცია და სარეზერვო დისკზე ჩაწერილი იმავე პროგრამის გადანერა;

- არ უნდა დავუშვათ სხვისი დისკების გამოყენება;

- თუ ანტივირუსული პროგრამების გამოყენების შემდეგ არ მოხერხდა „ვინჩესტერზე“ აღმოჩენილი ვირუსების მოსპობა, მაშინ აუცილებელია მყარი დისკის ფორმატიზაცია და მასზე სისტემების ხელმოწერა ჩაწერა.

თითქმის ყოველდღიურად წარმოებს ვირუსული პროგრამების შექმნა, ამიტომ აუცილებელია ანტივირუსული პროგრამების ოპერატიული განახლება, მუშაობის დაწყების წინ კომპიუტერის შემოწმება ვირუსზე.

სასარგებლო პროგრამული უზრუნველყოფის, ანტივირუსული პროგრამების განვითარებისა და სრულყოფის პარალელუ-

რად წარმოებს ვირუსული პროგრამების სრულყოფა და მათ მიერ შესრულებული ფუნქციების გაფართოება. ჯერჯერობით მსოფლიოში არ არსებობს ანტივირუსული პროგრამა, რომელიც შეძლებს დაიცვას ჩვენი კომპიუტერი, აღმოაჩინოს და გაანადგუროს ყველა სახის ვირუსი.

კომპიუტერული დანაშაულის თავიდან აცილების მიზნით, საჭიროა ტექნიკურ-ორგანიზაციული და სამართლებრივი ღონისძიებების გატარება, კომპიუტერული სისტემების რეზერვირება.

კომპიუტერული სისტემების რეზერვირება აუცილებელია ობიექტების მართვის რეალური დროის რეჟიმში ორგანიზებისას. მაგალითად, ატომური რეაქტორის, თვითმფრინავების ფრენისა და საბანკო სისტემის მართვა და მრავალი სხვ. ხანძრის გამოვლინებისა და ჩაქრობის მოწყობილობების დამონტაჟება, დივერსიის, მოპარვისა და აფეთქების საწინააღმდეგო ღონისძიებების გატარება.

ორგანიზაციულ ღონისძიებებს მიეკუთვნება: კადრების შერჩევა, იმ პირთა პასუხისმგებლობის გაზრდა, რომლებიც ვალდებული არიან უზრუნველყონ სისტემის უსაფრთხოების დაცვა; ისეთი პროექტების შემუშავება, რომელიც კომპიუტერული სისტემის მწყობრიდან გამოსვლის შემთხვევაში დახმარებას გაგვიწევს, აღვადგინოთ სისტემის ფუნქციონირება შედარებით მოკლე დროში.

სამართლებრივ ღონისძიებებს მიეკუთვნება: კომპიუტერული დანაშაულებისა და ინტელექტუალური საკუთრების შესახებ კანონების მიღება, კომპიუტერულ სისტემებში პორნოგრაფიული პროდუქციით სარგებლობის აკრძალვის შესახებ სათანადო საკანონმდებლო დოკუმენტების შემუშავება.

კომპიუტერული სისტემების უსაფრთხოების ამაღლების მიზნით საჭიროა, ქვეყნის ფარგლებში შეიქმნას კომპიუტერული უსაფრთხოების ცენტრი. აღნიშნულ ცენტრს უნდა დაევალოს შემდეგი სახის სამუშაოების შესრულება: სათანადო სტანდარტების მიხედვით შეამოწმოს შედგენილი პროგრამული უზრუნველყოფის ხარისხი, მისი მუშაობის საიმედოობა და ვარგისიანობა. კანონით აიკრძალოს ისეთი პროგრამული უზრუნველყოფის რე-

ალიზაცია, რომელსაც არ გაუვლია სათანადო ექსპერტიზა, ისე როგორც ნებისმიერ მატერიალურ საქონელს, და, მათ შორის წამლებს. თითოეულ ინფორმაციულ პროდუქტს უნდა ჰქონდეს გამოყენების ინსტრუქცია. მასში ნაჩვენები უნდა იყოს მომხმარებლის გაფრთხილება მისი გამოყენებისას შესაძლო მოსალოდნელი უარყოფითი შედეგების შესახებ.

13.4. კომპიუტერთან ხანგრძლივი მუშაობით გამონვეული შესაძლო დაავადებები

კომპიუტერთან ხანგრძლივად მუშაობა უარყოფითად მოქმედებს ადამიანის ჯანმრთელობაზე, იწვევს სხვადასხვა დაავადებას. კერძოდ: დატვირთვა თვალებზე, შეზღუდული პოზა, დატვირთვა ფსიქიკაზე და გამოსხივება.

თვალების დატვირთვა პირველი და მთავარი მავნე ფაქტორია. იწვევს თავის ტკივილს და თავბრუსხვევას, მხედველობის დაქვეითებას. აღნიშნულის თავიდან აცილების მიზნით, გამოიყენება თხევადკრისტალური მონიტორები, კომპიუტერზე ხანგრძლივად მუშაობისას აუცილებელია ხშირი შესვენება და ექიმების მიერ შემოთავაზებული თვალის ვარჯიშების შესრულება.

შეზღუდული პოზა კომპიუტერის მავნებლობის მეორე მთავარი ფაქტორია. კომპიუტერთან ხანგრძლივად მუშაობა იწვევს ადამიანის თითების, ხელის მტევნის, ბეჭების, კისრის შეზღუდულ მოძრაობას, რის შედეგადაც მას შეიძლება განუვითარდეს სხვადასხვა პროფესიული დაავადება: ოსტეოქონდროზი, ხერხემლის გამრუდება, ხელის მტევნების სახსრების დაავადება. ამ უკანასკნელით, როგორც წესი, ავადდებიან პერსონალურ კომპიუტერთან მომუშავე ოპერატორები. შეზღუდული პოზით გამონვეული მავნე ზემოქმედების შესამცირებლად, ოპერატორის სამუშაო ადგილი უნდა აღიჭურვოს სპეციალური ავეჯით (სკამი, მაგიდა);

კომპიუტერთან მუშაობა საჭიროებს ყურადღების დაძაბვას, რაც იწვევს ფსიქიკურ დაძაბულობას, რომლის შედეგადაც ადამიანს ეწყება უძილობა, კოშმარული სიზმრები, მოუსვენარი ძილი და სხვა ფსიქიკური გადახრები. აღნიშნულის თავიდან ასაცი-

ლებლად, პირველ რიგში საჭიროა შევამციროთ კომპიუტერთან მუშაობის ხანგრძლივობა, სამუშაო დროის პერიოდში შევისვენოთ რამდენჯერმე და ჩავატაროთ ვარჯიშები, ნაკლებად ვითამაშოთ მძაფრსიუჟეტიანი თამაშები, მოვუსმინოთ მუსიკას;

გამოსხივება. კომპიუტერთან მომუშავე ადამიანისათვის მავნებელია ელექტრონული ველი, რომელიც წარმოიქმნება მონიტორსა და მასთან მომუშავე ოპერატორს შორის. მონიტორიდან ატყორცნილი დიდი სიჩქარით მოძრავი მტვრის ნაწილაკები ეჯახებიან ადამიანის სახეს. ასეთი ნაწილაკების შესამცირებლად საჭიროა ოთახის ვენტილიზაცია, ჰაერის განმენდა, მუშაობის დამთავრების შემდეგ ხელ-პირის დაბანა. აღნიშნული ველის მავნებლური ზემოქმედება ადამიანზე ჯერ ბოლომდე არ არის შესწავლილი. დადგენილია მხოლოდ, რომ ელექტრონული ველის ზემოქმედება იწვევს თავის ტკივილს. კომპიუტერზე მუშაობისას ჯანმრთელობისათვის უარყოფითი შედეგების თავიდან აცილების მიზნით საჭიროა:

- სამედიცინო ჩვენებების მიხედვით კომპიუტერთან შეზღუდული მუშაობა, რაც ითვალისწინებს კომპიუტერთან ყოველი ორი საათის მუშაობის შემდეგ 15-წუთიან შესვენებას და ამ პერიოდში სხვადასხვა ვარჯიშების შესრულებას, განსაკუთრებით იმ ორგანოების ვარჯიშს, რომლებიც კომპიუტერთან მუშაობისას განიცდიან დაძაბულობას (თვალები, ხელის მტევნები, კისერი, ბეჭედი);
- სამუშაო ადგილის სწორი ორგანიზება (ნორმალური განათება, ხმაურსანინააღმდეგო სისტემის ორგანიზება, კომპიუტერის განლაგება კედლიდან სათანადო მანძილზე, მონიტორსა და მომუშავეს შორის მანძილი არ უნდა იყოს 0,7 მეტრზე ნაკლები).

საზოგადოების საყოველთაო ინფორმატიზაციის პროცესი უნდა წარიმართოს იმ მიმართულებით და საშუალებებით, რომ ინფორმატიზაციას ჰქონდეს ჰუმანური ორიენტაცია, რომლის ცენტრშიც ყოველთვის ადამიანი იქნება. აღმოიფხვრას ინფორმატიზაციის ისეთი უარყოფითი სოციალურ-ეკონომიკური შედეგები, როგორიცაა: კულტურის დაცემა, ადამიანის ფსიქიკის დაქვეითება, დადებითი ეროვნული ტრადიციების მსხვრევა, ეთიკუ-

რი ნორმების დამახინჯება, შრომის დეჰუმანიზაცია, უმუშევრობა, ადამიანის უფლებების დარღვევა.

კომპიუტერისათვის მიუწვდომელი და გაუგებარია ისეთი ადამიანური ცნებები, როგორიცაა: მორალი, პასუხისმგებლობა, სალი აზროვნება, ამიტომ მას ვერ დაეკისრება მორალური პასუხისმგებლობა ჩადენილი დანაშაულისათვის, მას ვერც დამნაშავის სკამზე დასვამ. ყოველგვარი კომპიუტერული დანაშაულის ჩადენისას პასუხი უნდა აგოს ადამიანმა, მას უნდა დაეკისროს პასუხისმგებლობა მომხდარ ფაქტზე.

პროგრამული პროდუქტის მოპარვის საწინააღმდეგოდ მრავალი ღონისძიება ტარდება: კანონი ინტელექტუალური საკუთრებისა და კომპიუტერული დანაშაულის შესახებ, კომპიუტერული სისტემების მფლობელების წახალისება, რაც გამოიხატება იმაში, რომ თუ მან ადრე პროგრამული უზრუნველყოფა შეიძინა ლიცენზირებული გზით, მაშინ, ამ პროგრამული პროდუქტის გაუმჯობესებული, სრულყოფილი ვერსიის ბაზარზე გამოშვების შემთხვევაში, საავტორო უფლებით მოსარგებლე ფირმა ან პიროვნება მას ამ ვარიანტს გაცილებით შეღავათიან ფასებში მიჰყიდის. გარკვეული ინიციატივა პროგრამული პროდუქტების მოპარვის საწინააღმდეგო ღონისძიებების გატარებასთან დაკავშირებით აიღო ჯგუფმა, რომელიც შეიქმნა 1997 წელს. ამ ჯგუფში გაერთიანდნენ ჩრდილოეთ ამერიკის, ევროპის, აზიის, წყნაროკეანეთის რეგიონში პროგრამული პროდუქტების გამავრცელებელი განყოფილებების ხელმძღვანელები. მას ხელმძღვანელობს ფირმა **Adobe Systems Europe**-ის გენერალური მენეჯერი დერეკ გრეი (**Derek Gray**). მან აღნიშნა, რომ **CD-ROM** დისკსა და იმ დოკუმენტაციების კომპლექტში, რომელიც თან ახლავს კომპიუტერებს, მოთავსებული იქნება გაფრთხილება პროგრამის არალეგალურად გავრცელების შემთხვევაში პასუხისმგებლობის შესახებ და მითითებული იქნება, რომ პროგრამის განახლება შესაძლებელია მხოლოდ იმათთვის, ვინც კანონიერადაა რეგისტრირებული.

ქვემოთ განვიხილავთ მონაცემების მთლიანობის, კონფიდენციალობისა და ნამდვილობის დაცვის კრიპტოგრაფიულ მეთოდს.

13.5. კრიპტოგრაფია

ადამიანებს დიდი ხანია ალელვებით ინფორმაციის დაცვის პრობლემა. კრიპტოლოგიის ისტორია ადამიანის ენის ისტორიის ტოლია. ვინაიდან საზოგადოების წევრთა უმრავლესობამ არ იცოდა წერა-კითხვა, ამიტომ დაწერილი სახით გავრცელებული ინფორმაცია მათთვის თავისთავად წარმოადგენდა საიდუმლოს და დაშიფრულს. მაგ., ძველი ინდოეთისა და ეგვიპტის საღმრთო წიგნები. შემდგომში დამწერლობის ფართოდ გავრცელებამ გამოიწვია კრიპტოლოგიის დამოუკიდებელ მეცნიერებად ჩამოყალიბება. პირველი კრიპტოსისტემები გვხვდება ჩვენი წელთაღრიცხვის დასაწყისში. მაგალითად, ცეზარი მიმონერის დროს იყენებდა გარკვეული სახით სისტემატიზებულ შიფრს, რომელსაც შემდგომში მისი სახელი ეწოდა. კრიპტოლოგიურმა სისტემებმა ფართო გავრცელება პოვეს პირველი და მეორე მსოფლიო ომის დროს, განსაკუთრებით, მეორე მსოფლიო ომის შემდეგ, როცა შეიქმნა გამოთვლითი საშუალებები, კომპიუტერული ქსელები, გლობალური ქსელი – ინტერნეტი, რომელთა დახმარებითაც წარმოებს დიდი მოცულობის ინფორმაციის მოძრაობა და რომელიც დაცვას საჭიროებს. ინფორმაციის დაცვისა და გარდაქმნის პრობლემებით დაკავებულია კრიპტოლოგიის (**kriptos** – საიდუმლო, **logos** – მეცნიერება) მეცნიერება. კრიპტოლოგია იყოფა ორ მიმართულებად: კრიპტოგრაფია; კრიპტოანალიზი.

ამ ორი მიმართულების მიზანი ურთიერთსაწინააღმდეგოა. კრიპტოგრაფია იკვლევს ინფორმაციის გარდაქმნის მათემატიკურ მეთოდებს, კრიპტოანალიზი კი – გასაღების გარეშე ინფორმაციის გაშიფვრის შესაძლებლობებს. თანამედროვე კრიპტოგრაფია მოიცავს ოთხ ძირითად განყოფილებას:

- სიმეტრიული კრიპტოსისტემები;
- კრიპტოსისტემები ღია გასაღებით ;
- ელექტრონული ხელმოწერის სისტემები;
- გასაღებების მართვა.

კრიპტოგრაფიული მეთოდების ძირითად მიმართულებას წარმოადგენს კავშირის არხებში ინფორმაციის გადაცემისას

კონფიდენციალობის დაცვა, გადაცემული შეტყობინების ნამდვილობის დადგენა. კრიპტოგრაფია საშუალებას იძლევა, რომ დაშიფრული ინფორმაციის წაკითხვა შესაძლებელი გახდეს მხოლოდ გასაღების მეშვეობით. დაშიფვრასა და გაშიფვრას ექვემდებარება ტექსტი, რომელიც აგებულია რაღაც ალფაბეტის საფუძველზე, რომელშიც მოიაზრება კოდირებას დაქვემდებარებული ინფორმაციული ნიშნების სასრული სიმრავლე. ტექსტი ეს არის ალფაბეტიდან აღებული მონესრიგებულ ელემენტთა კრებული. მაგ., ქართული ალფაბეტი შედგება 33 ელემენტისაგან (ასოსაგან), სტანდარტული კოდი **ASCII** და **KOU-8 – 256** სიმბოლოსაგან, ბინარული ალფაბეტი კი – ორი (0, 1) სიმბოლოსაგან და ა. შ.

დაშიფვრა მონაცემების გარდაქმნის ისეთი პროცესია, როდესაც საწყისი ტექსტი გარდაიქმნება დაშიფრულ ტექსტად. გაშიფვრა, დაშიფვრის შებრუნებული პროცესია, როდესაც გასაღების საფუძველზე დაშიფრული ტექსტი გარდაიქმნება საწყის ტექსტად. **გასაღები** – ეს არის ინფორმაცია, რომელიც აუცილებელია ტექსტის დასაშიფრად და გასაშიფრად. კრიპტოსისტემები იყოფა სიმეტრიულ და ღია გასაღების სისტემებად. სიმეტრიულ კრიპტოსისტემებში ინფორმაციის დასაშიფრად და გასაშიფრად გამოიყენება ერთი და იგივე გასაღები, ხოლო ღია გასაღების სისტემებში – ორი გასაღები, ღია და დახურული (საიდუმლო), რომლებიც მათემატიკურად ერთმანეთთანაა დაკავშირებული. ინფორმაციის დაშიფვრა წარმოებს ღია გასაღებით, გაშიფვრა კი – დახურული გასაღებით. ღია გასაღები ცნობილია ფართო საზოგადოებისათვის, დახურული კი მხოლოდ შეტყობინების მიმღებისათვის. ტერმინი გასაღების მართვა გულისხმობს გასაღების შედგენასა და მის გავრცელებას მომხმარებლებს შორის.

ინფორმაციის უსაფრთხოება მჭიდროდაა დაკავშირებული ელექტრონულ-ციფრულ ხელმოწერასთან. ელექტრონულ-ციფრულ ხელმოწერაში იგულისხმება ტექსტთან მისი გარდამქმნელის მიერთება, რაც საშუალებას იძლევა, ტექსტის მიღებისას სხვა მომხმარებელმა შეამოწმოს შეტყობინების ნამდვილობა და ავტორობა.

კრიპტოსისტემების დახასიათება წარმოებს ისეთი მაჩვენებლებით როგორიცაა კრიპტომდგრადობა, რომელშიც იგულისხმება შიფრის მახასიათებლები, რომლებიც განსაზღვრავენ გასაღების გარეშე მის მდგრადობას გაშიფვრასთან მიმართებაში. კრიპტომდგრადობის მაჩვენებლებია გასაღების ყველა შესაძლო რაოდენობა და კრიპტოანალიზისათვის საჭირო აუცილებელი საშუალო დრო.

თანამედროვე კრიპტოსისტემებს წაეყენება შემდეგი მოთხოვნები:

- დაშიფრული შეტყობინების წაკითხვა შესაძლებელია, მხოლოდ გასაღების საშუალებით;

- დაშიფრული ტექსტის გასაშიფრად საჭირო ოპერაციების რაოდენობა არ უნდა იყოს ნაკლები გასაღებების შესაძლო რაოდენობაზე;

- დაშიფვრის ალგორითმის სტრუქტურული ელემენტები უნდა იყოს უცვლელი;

- დაშიფრული ტექსტის სიგრძე ტოლი უნდა იყოს სანყის ტექსტის;

- ყველა შესაძლო გასაღებიდან აღებულმა გასაღებმა უნდა უზრუნველყოს ინფორმაციის დაცვა. დაშიფრულ ტექსტში შეტანილი დამატებითი ბიტები საიმედოდ უნდა იყოს დამალული.

კრიპტოგრაფია ქსელში ინფორმაციის მოძრაობისას წყვეტს მრავალ პრობლემას. კერძოდ: აუთენტიფიკაციის, კონფიდენციალობის, მონაცემების მთლიანობის და ინფორმაციის გაცვლისას მონაწილეთა კონტროლის.

ტერმინი **დაშიფვრა** ნიშნავს მონაცემების ისეთი სახით გარდაქმნას, რომ მისი წაკითხვა ადამიანს, ტექნიკურ ან პროგრამულ საშუალებებს არ შეუძლიათ დაშიფვრა-გაშიფვრის გასაღების გარეშე.

ინფორმაციის კრიპტოგრაფიული დაცვის მეთოდის მთავარ კომპონენტს წარმოადგენს **გასაღები**, რომელიც უზრუნველყოფს მონაცემების დაშიფვრას და გაშიფვრას. **გასაღები** – ეს არის სიმბოლოთა გარკვეული თანმიმდევრობა, რომელსაც ააგებს ინფორმაციის კრიპტოგრაფიული დაცვის დაშიფვრისა

და გაშიფვრის ალგორითმი. თითოეული ასეთი გარდაქმნა ცალსახად განისაზღვრება გასაღებით, რომელსაც განსაზღვრავს კრიპტოლოგიური ალგორითმი.

ციფრული ხელმოწერა. ელექტრონული ციფრული ხელმოწერა – არის ელექტრონული დოკუმენტის რეკვიზიტი, რომლის დანიშნულებაც, ინფორმაციის კრიპტოგრაფიული გარდაქმნის შედეგად მიღებული ელექტრონული დოკუმენტი დაიცვას გაყალბებისაგან, დაადგინოს, რომ ელექტრონულ დოკუმენტში ადგილი არ აქვს ინფორმაციის დამახინჯებას და უზრუნველყოს ხელმოწერის გასაღების სერტიფიკატის მფლობელის იდენტიფიცირება.

ელექტრონული ციფრული ხელმოწერა ელექტრონულ დოკუმენტში სამართლებრივად თანაბარმნიშვნელოვანია ქალაქის დოკუმენტზე შესრულებული ჩვეულებრივი ხელმოწერისა, იმ შემთხვევაში, თუ შესრულებულია შემდეგი მოთხოვნები:

- ხელმოწერის გასაღების სერტიფიკატს, რომელიც ეკუთვნის ამ ელექტრონულ-ციფრულ ხელმოწერას, ელექტრონული ციფრული ხელმოწერის განხორციელების მომენტისათვის არ დაუკარგავს მოქმედების ვადა;

- ელექტრონულ დოკუმენტზე შესრულებული ელექტრონული ციფრული ხელმოწერა დადასტურებულია;

- ელექტრონული ციფრული ხელმოწერა შესრულებულია ხელმოწერის გასაღების სერტიფიკატში მითითებული წესებისა და მოთხოვნების სრული დაცვით.

ახლო მომავალში ძირითადად, გარიგებების გაფორმება მოხდება ელექტრონული ციფრული ხელმოწერის გამოყენებით. ელექტრონული ციფრული ხელმოწერისათვის საჭირო დახურული გასაღების სერტიფიკატის გაცემა ხდება სერტიფიკაციების გამცემი ცენტრის მიერ. ელექტრონული ციფრული ხელმოწერის არსი მდგომარეობს შემდეგში: კრიპტოგრაფიული ხელ-ფუნქციის დახმარებით გამოითვლება ფიქსირებული სიგრძის სიმბოლოთა მოკლე სტრიქონი (ხეში). შემდეგ ეს ხეში იშიფრება მფლობელის დახურული გასაღებით და მიიღება დოკუმენტის ხელმოწერა. ხელმოწერა დაედება დოკუმენტს. ამ გზით მიიღება ხელმოწერილი დოკუმენტი. იმ პირს, ვისაც სურს დაადგინოს დოკუმენ-

ტის ნამდვილობა, შეუძლია ელექტრონული ციფრული ხელმოწერის გაშიფვრა მფლობელის ღია გასაღებით და დოკუმენტის ხეშის გამოთვლა. დოკუმენტი ჩაითვლება ნამდვილად, თუ გამოთვლილი ხეში დაემთხვევა ხელმოწერილიდან გაშიფრულს.

ციფრული ხელმოწერით ინფორმაციის დაცვა ქსელებში მოიცავს ხელმოწერის გამოსათვლელ და ხელმოწერის შემოწმებულ ორ ალგორითმს: პირველი ალგორითმის შესრულება წარმოებს მხოლოდ ავტორის მიერ, ხოლო მეორე ხელმისაწვდომია ნებისმიერი პიროვნებისათვის, რათა შესაძლებელი გახდეს ხელმოწერის სისწორის შემოწმება. კრიპტოგრაფიული დაცვა და ინფორმაციის უსაფრთხოება მუშაობს განსაზღვრული ალგორითმით და შედეგადად ერთი ან რამდენიმე არითმეტიკული ფორმულის მიხედვით დაშიფვრის ალგორითმისაგან.

კრიპტოსისტემით ინფორმაციის დაცვის პროგრამული სისტემა მოიცავს გასაღებს, მონაცემების დაშიფვრის ალგორითმებს, დასაშიფრ ტექსტს და დაშიფრულ ტექსტს. თავდაპირველად დაშიფრავი ალგორითმი გამოიყენება დასაშიფრავ ტექსტისათვის, შემდეგ კი, გაშიფვრის მიზნით, მიმართავენ მის გენერირებას. ამის შემდეგ დაშიფრული ტექსტი გადაეცემა ადრესატს, სადაც ამ ალგორითმით წარმოებს მიღებული დაშიფრული ტექსტის გაშიფვრა. გარდა აღნიშნულისა, კრიპტოგრაფიით ინფორმაციის დაცვის სისტემა მოიცავს გასაღებების გენერაციის პროცედურებს და მათ გავრცელებას. სიმეტრიული გასაღებით ინფორმაციის დაშიფვრა-გაშიფვრისათვის გამოიყენება ერთი და იგივე გასაღები. თუ გასაღები არ იყო კომპრომეტირებული გაშიფვრის პროცესში ავტომატურად მოხდება შეტყობინების ავტორის აუთენტიფიკაცია, რადგანაც მხოლოდ მას გააჩნია შეტყობინების გაშიფვრის გასაღები.

კრიპტოგრაფიული ინფორმაციის დაცვა გულისხმობს, რომ მხოლოდ შეტყობინების გადამცემმა და მიმღებმა იციან გასაღები და, ინფორმაციის გადაცემის კომპრომეტაციის შემთხვევაში, საინფორმაციო სისტემის ორივე მომხმარებელს თანაბრად ეკისრება პასუხისმგებლობა. ამ შემთხვევაში ინფორმაციის დაცვის ორგანიზაციულ პრობლემას წარმოადგენს მომხმარებლებს შორის გასაღების გავრცელების უსაფრთხოება ინტერნეტით, მისი

გადაცემისას, ანუ – ინფორმაციის დაცვა უნდა იყოს მაღალ დონეზე. ინფორმაციის დაცვის პროგრამულ-აპარატურული კრიბტოსისტემის დაშიფვრის სიმეტრიული ალგორითმი იყენებს მოკლე გასაღებებს, რაც საშუალებას იძლევა, მიუხედავად საბანკო ინფორმაციის დიდი მოცულობისა, მოკლე დროში განხორციელდეს დაშიფვრა.

სიმეტრიული გასაღების გამოყენება ინფორმაციის დასაშიფრავად წარმოებს შემდეგი თანმიმდევრობით: ორგანიზაციის ინფორმაციის დაცვის სისტემა შეიმუშავებს, ავრცელებს და ინახავს სიმეტრიულ გასაღებს. შემდეგ ინფორმაციის დაცვის სპეციალისტი ან კომპიუტერულ ქსელებში ინფორმაციის დაცვის სისტემის გამგზავნი ტექსტის ხეშფუნქციის საშუალებით ქმნის ელექტრონულ ხელმოწერას და ათავსებს მას ტექსტის სტრიქონებს შორის.

შეტყობინების გადამცემი სარგებლობს დაშიფვრის სწრაფი ალგორითმით და, ელექტრონულ ხელმოწერასთან ერთად, ასიმეტრიული გასაღებით, რომლის დახმარებითაც წარმოებს ინფორმაციის დამშიფრავი სისტემის მომხმარებლის აუთენტიფიკაცია. შეტყობინების მიმღები შეტყობინების გასაშიფრად სარგებლობს იმავე სიმეტრიული ალგორითმით და სიმეტრიული გასაღებით, რომლის საშუალებითაც მოხდა გადასაცემი ტექსტის დაშიფვრა. ამ შემთხვევაში გაშიფვრის შედეგად მიიღება საწყისი ტექსტი და ელექტრონული ხელმოწერა. შეტყობინების მიმღები ელექტრონულ ხელმოწერას გამოყოფს ტექსტიდან და უდარებს ადრე გადაცემულ ელექტრონულ ხელმოწერას, რაც საშუალებას იძლევა შემოწმდეს მონაცემების მთლიანობა და ნამდვილობა.

ახლა განვიხილოთ მონაცემების დაშიფვრის ღია ასიმეტრიული მეთოდი. ამ მეთოდის მიხედვით დაშიფვრისა და გაშიფვრის გასაღებები სხვადასხვაა, მიუხედავად იმისა, რომ მათი შექმნა ერთდროულად წარმოებს. ინფორმაციის დაცვის ამ სისტემის შემთხვევაში ერთი გასაღების გავრცელება ხდება საჯაროდ, მეორე კი გადაეცემა ფარულად. ერთი გასაღებით დაშიფრული ტექსტის გაშიფვრა წარმოებს მეორე გასაღებით. ასიმეტრიული გასაღების გატეხვას ჰაკერები ცდილობენ გასაღების პირდაპირი გადარჩევის მეთოდით. ამიტომ ასიმეტრიული გასაღების სიგრძე

დიდია. რაც უფრო გრძელია ეს გასაღები, მით მეტი დროა საჭირო მის გასატყუად. ასიმეტრიული გასაღების გამოყენება წარმოებს შემდეგი თანმიმდევრობით: საიდუმლო ასიმეტრიული გასაღები ეგზავნება მის მფლობელს, ღია ასიმეტრიული გასაღები კი ინახება მონაცემთა ბაზაში და მისი ადმინისტრირება წარმოებს ინფორმაციის დაცვის სამუშაოების სერტიფიკაციის ცენტრში. მის კონტროლს ახორციელებს ინფორმაციის დაცვის სპეციალისტი. იქმნება ტექსტის ელექტრონული ხელმოწერა და მიღებული შემდეგი იშიფრება ასიმეტრიული ალგორითმით. საიდუმლო გასაღები იგზავნება და ინახება სიმბოლოთა სტრიქონში, ემატება ტექსტს. ასეთი სახით დაშიფრული ტექსტი ეგზავნება ინფორმაციის მიმღებს. ინფორმაციის გამგზავნმა გასაღების გაცემის სერტიფიკაციის ცენტრიდან უნდა მიიღოს ღია გასაღები.

ამრიგად, ინფორმაციის დაცვის ალგორითმები საშუალებას იძლევა, ინფორმაცია 100%-ით იყოს დაცული იმ მომხმარებლისგან, რომლისთვისაც გასაღები არ არის ცნობილი.

13.6. ინფორმაციის დაცვის ბიომეტრიული სისტემები

მომავალში ინფორმაციის დაცვის სფეროში ახალი ტექნოლოგიების გამოყენება საშუალებას მისცემს კომპიუტერების მომხმარებლებს, ინფორმაციის დაცვის პაროლის სისტემა შეცვალონ უფრო საიმედო და ეფექტური საშუალებებით, რომლებიც დაფუძნებული იქნება ბიომეტრიულ სისტემებზე. ბიომეტრიკა არის მეცნიერება, რომელიც სწავლობს ადამიანის სხეულის სხვადასხვა თვისებებს (მაგ., თითის ანაბეჭდი, თვალის გუგა, ადამიანის ხმა და სხვ.) აღნიშნულიდან ერთ-ერთი შეიძლება გამოვიყენოთ პიროვნების იდენტიფიკაციისთვის. ადამიანის ფიზიოლოგიური პარამეტრები თითოეული ადამიანისთვის არის უნიკალური და უცვლელი მისი სიცოცხლის განმავლობაში. პიროვნების იდენტიფიკაციის ბიომეტრიული სისტემები ბოლო პერიოდში ფართოდ ინერგება სხვადასხვა ქვეყანაში, რომელთა რაოდენობა სამ ათეულზე მეტია. ბიომეტრიული პასპორტები, როგორც პიროვნების დამადასტურებელი დოკუმენტი ფართოდ გამოიყენება საქართველოშიც.

ბიომეტრული იდენტიფიკაცია საშუალებას იძლევა, წარმატებით გადავწყვიტოთ მთელი რიგი პრობლემები:

- თავიდან ავიცილოთ ბოროტმზრახველების შეღწევა დაცულ ნაგებობებსა და ტერიტორიაზე გაყალბებული ან მოპარული დოკუმენტებით, ან კიდევ სხვისი პაროლის გამოყენებით;

- შევზღუდოთ ინფორმაციასთან შეღწევა ინფორმაციის დაცვის მიმართულებით;

- გავზარდოთ პიროვნების პასუხისმგებლობა.

- გამოვრიცხოთ ის უხერხულობები, რომელსაც ადგილი აქვს პაროლის დავიწყების, გასაღებისა და ბარათების დაკარგვის გამო;

- საპასუხისმგებლო ობიექტებთან შეღწევა უნდა განხორციელდეს მხოლოდ სერტიფიცირებული სპეციალისტების მიერ.

შელწვევის ბიომეტრული კონტროლი არის ავტომატიზებული მეთოდი, რომლის დახმარებითაც პიროვნების იდენტიფიკაცია ხორციელდება ადამიანის ფიზიოლოგიური უნიკალური თვისებების ან მისი ქცევის მახასიათებლებით. მიუხედავად იმისა, რომ დროთა განმავლობაში ადამიანის ქცევა (ხელმოწერა, ხმა, და სხვ.) შეიძლება შეიცვალოს, პიროვნების იდენტიფიკაციისას უპირატესობა მაინც ფიზიოლოგიური თვისებების გამოყენებას ენიჭება.

13.7. ინფორმაცია როგორც სამართლებრივი რეგულირების სფერო

საზღვარგარეთ დიდი ხანია აღმოცენდა სამართლის ისეთი მიმართულება, როგორიცაა კომპიუტერული სამართალი, რომელმაც განვითარებისა და სრულყოფის შედეგად მიიღო საინფორმაციო სამართლის სახელწოდება. ინფორმაციულად განვითარებულ მრავალ ქვეყანაში მოქმედებს სახელმწიფო პროგრამები, რომელთა დანიშნულებაა ნაციონალური ინფორმაციული რესურსების სამართლებრივი დაცვა და სრულყოფა. საინფორმაციო სამართალში განსაზღვრულია ინფორმაციის ძირითადი სამართლებრივი ტერმინები, საინფორმაციო სისტემების სამარ-

თლებრივი ასპექტები, მონაცემთა სტრუქტურები, სისტემური და გამოყენებითი პროგრამული უზრუნველყოფა. განსაზღვრულია ინფორმაციული პროდუქტებისა და ნაკეთობების სამართლებრივი მახასიათებლები. ისევე როგორც სამეურნეო საქმიანობისა და ბიზნესის ობიექტებს, გამოთვლით ტექნიკასა და ინფორმაციული ტექნოლოგიების ობიექტებს სამართლებრივი კუთხით გააჩნია სპეციფიკურობა.

რადგან მანქანური ინფორმაციის წარმოებას აქვს მასობრივი და ინდუსტრიული ხასიათი, ამიტომ აუცილებელია ამ დარგის სამართლებრივი უზრუნველყოფა. მასთან დაკავშირებულ ყველა სუბიექტს უნდა ჰქონდეს მკაფიოდ განსაზღვრული უფლება-მოვალეობები, როგორც ინფორმაციის, ასევე სხვა სუბიექტებთან მიმართებაში.

ინფორმაციულ-გამოთვლითი მომსახურების ბაზრის განვითარებამ გამოიწვია ის, რომ ინფორმაცია გახდა ყველაზე ყიდვადი და გაყიდვადი საქონელი. აღმოცენდა ინფორმაციული ბიზნესი, რომელიც საჭიროებს ეფექტიან ინფორმაციულ მენეჯმენტს და შესაბამის სამართლებრივ ნორმებს. შექმნილია და ვითარდება ინტერნაციონალური, მულტინაციონალური და ტრანსნაციონალური საინფორმაციო სისტემები (გლობალური, და ლოკალური გამოთვლითი ქსელები). მიმდინარეობს ინფორმაციული საზოგადოების მშენებლობის პროცესი, რაც სამართლებრივ უზრუნველყოფას საჭიროებს.

ინფორმატიზაციის საშუალებების ბაზარზე მოქმედებს საერთო ხასიათის სამართლებრივი აქტები. მათი საშუალებით ხდება ბიზნესის სამართლებრივი დაცვა. ამ შემთხვევაში ძირითადად გამოიყენება ის სამართლებრივი აქტები, რომელთა მიხედვითაც რეგულირდება, მაგ., სასურსათო, ნავთობპროდუქტების და ავტომანქანების ბაზარი. ინფორმატიზაციის საშუალებების ბაზარზე წარმოქმნილი კონფლიქტური სიტუაციების რეგულირება ხდება სამართლის საერთო ნორმების საფუძველზე, მაგრამ ინფორმაციული ბიზნესის სფეროში წარმოქმნილი სიტუაციები, გამომდინარე ამ დარგის სპეციფიკიდან, საჭიროებს სპეციალური სამართლებრივი აქტებით რეგულირებას. მაგ., როცა საქმე ეხება სუპერელექტრონული გამომთვლელი მანქანებით

ვაჭრობას, ამ სფეროში ბაზრის კონტროლი წარმოებს მწარმოებელი სახელმწიფოს და მყიდველი ქვეყნის ინტერესებიდან გამომდინარე. მაგ., მსოფლიოში სუპერკომპიუტერები განიხილება, როგორც ქვეყნის სტრატეგიული რესურსი, ამიტომ ნებისმიერი ყიდვა-გაყიდვის ოპერაცია ამ სახის კომპიუტერებზე რეგულირდება მკაცრი კანონმდებლობით, გამომდინარე სახელმწიფოს ინტერესებიდან და, როგორც შედეგი, ბიზნესი უნდა დაემორჩილოს კანონით დადგენილ შეზღუდვებს. ეს პროცესი განსაკუთრებით კონტროლდება აშშ-ში, ქვეყნის კანონმდებლობით. არის შემთხვევები, როცა კანონმდებლობის დარღვევით სუპერკომპიუტერებით ვაჭრობისას დამრღვევი კომპანიის მიმართ გამოიყენეს მკაცრი სანქციები. მაგ., 1996 წელს კომპანია IBM კოლუმბიის ფედერაციული ოლქის სასამართლოს მიერ დაჯარიმდა 8,5 მლნ. დოლარით რუსეთისთვის 17 სუპერკომპიუტერის მიყიდვის გამო.

13.8. საბანკო საინფორმაციო სისტემების უსაფრთხოება

ინფორმაციული ტექნოლოგიების განვითარებამ და საბანკო საინფორმაციო სისტემების შექმნამ დღის წესრიგში დააყენა ინფორმაციული უსაფრთხოების პრობლემა. ინფორმაციული უსაფრთხოება ნიშნავს საბანკო ინფორმაციაზე არასანქცირებულ წვდომას, რომლის დროსაც ადგილი აქვს ინფორმაციის მთლიანობის დარღვევას, ინფორმაციის გაყალბებას, მოპარვას, კონფიდენციალურ ინფორმაციასთან არაკანონიერ წვდომას.

საბანკო სისტემის უსაფრთხოების მეთოდებისა და საშუალებების შემუშავებამდე საჭიროა დადგინდეს, უსაფრთხოების რა მოვლენებთან შეიძლება გვექონდეს საქმე, კერძოდ, გარე უსაფრთხოებასთან, სისტემის შიგნით უსაფრთხოებასთან, განზრახ ან შემთხვევით უსაფრთხოებასთან. პირველ რიგში, აუცილებელია, შევაფასოთ დასაცავი ინფორმაციის ღირებულება, შემდეგ უნდა განისაზღვროს იმ მეთოდებისა და საშუალებების ღირებულება რომელთა გამოყენებასაც ვფიქრობთ. ამ ორი ვარიანტის შედარების შემდეგ გაცხადდება დაცვის რა მეთოდები

და ხერხები უნდა იქნეს გამოყენებული ინფორმაციის დასაცავად. ბანკში ინფორმაციის დაცვა უნდა განხორციელდეს კომპლექსურად, ანუ უნდა გამოიყენონ დაცვის ადმინისტრაციული, ტექნიკური, პროგრამული და სამართლებრივი მეთოდები. მოკლედ, თითოეული საბანკო საინფორმაციო სისტემის ადმინისტრაციულ დაცვაში იგულისხმება სათანადო კადრების შერჩევა, იმ შენობა-ნაგებობების დაცვა, სადაც განლაგებულია საინფორმაციო სისტემა. საინფორმაციო სისტემის შიგნით დაცვა გულისხმობს იმას, რომ თითოეული თანამშრომლისათვის გამოყოფილია სამუშაო ადგილი და მისი გადაადგილების არეალი, რომლის დარღვევაც არასასურველია. კადრები უნდა შეირჩეს როგორც პროფესიონალიზმის, ისე სანდოობის გათვალისწინებით. აგრეთვე მხედველობაში უნდა იქნეს მიღებული ის დაუნერგელი კანონები, რომელთა დარღვევამ ბანკს შეიძლება მიაყენოს მატერიალური ან მორალური ზარალი (ბანკის საიდუმლო ინფორმაციის გაცემა, ბანკის რესურსების არადანიშნულებით გამოყენება და ა. შ.). ობიექტის გარე დაცვა გულისხმობს ისეთი ტექნიკური საშუალებების გამოყენებას, რომლებიც დაბრკოლებას შეუქმნის გარეშე პირს, შეაღწიოს შენობაში (სიგნალიზაცია, ელექტრონული გასაღებები, დაცვის მუშაკები და სხვ.). როდესაც საუბარია ბანკის საინფორმაციო სისტემის ტექნიკურ დაცვაზე, ამ შემთხვევაში, აქცენტი კეთდება ინფორმაციის შეგროვების, დამუშავების და შენახვის ტექნიკური საშუალებების საიმედოობაზე. დაცვის ტექნიკური საშუალებები შევიძინოთ მაღალი იმიჯის მქონე ფირმებიდან ტენდერების ჩატარების საფუძველზე. საჭიროა შევიძინოთ სარეზერვო ტექნიკა, რაც საშუალებას მოგვცემს, ტექნიკის მწყობრიდან გამოსვლის შემთხვევაში, შეუფერხებლად დავამუშაოთ ინფორმაცია. საჭიროა გაგვაჩნდეს უწყვეტი დენის წყაროები. თუ შესაძლებელია, ბანკს უნდა ჰქონდეს ელექტროკვების დამატებითი ხაზი.

ბანკში არსებული ინფორმაციის დაცვა ითვალისწინებს ოპერაციული სისტემების, გამოყენებითი პროგრამული პაკეტების და მონაცემთა ბაზების დაცვას. დაცვის მიზნით იყენებენ ანტივირუსულ პროგრამებს. საბანკო საინფორმაციო სისტემების შეძენის ან საკუთარი ძალებით შემუშავების დროს განსაკუთრებუ-

ლი ყურადღება უნდა მიექცეს საინფორმაციო სისტემის უსაფრთხოების უზრუნველყოფას, წინააღმდეგ შემთხვევაში, შეიძლება საჭირო გახდეს ორჯერ მეტი დანახარჯების გაღება სისტემის შეძენის ღირებულებასთან შედარებით. პროგრამული დაცვა მოიცავს აგრეთვე ინფორმაციასთან შეღწევის სხვადასხვა პრიორიტეტების დადგენას, რაც შესაძლებელია განხორციელდეს პაროლების გამოყენების საფუძველზე. ინფორმაციის დაცვა უნდა განხორციელდეს ქვეყანაში არსებული კომპიუტერული (საინფორმაციო) სამართლის სრული დაცვის საფუძველზე.

არ არის გასაკვირი, რომ უსაფრთხოების საკითხები განსაკუთრებულ ყურადღებას იქცევს როგორც ბანკის კლიენტების, ასევე ბანკის თანამშრომლების მხრიდან. მოქალაქე თავის პერსონალურ მონაცემებს, მათ შორის კონფიდენციალურს, ანდობს საფინანსო-საკრედიტო დაწესებულებებს.

საბანკო საინფორმაციო სისტემაში შენახული ინფორმაცია, რომელიც ასახავს ანგარიშებზე მოთავსებულ რეალურ ფულს, ეხება მრავალი ადამიანისა და ორგანიზაციის ინტერესებს. ამ ინფორმაციის საფუძველზე შესაძლებელია ანგარიშსწორება, პროცენტების დარიცხვა, კრედიტის გაცემა. ამ ინფორმაციის არასანქცირებულმა მოდიფიკაციამ შეიძლება გამოიწვიოს სერიოზული ზარალი. უსაფრთხოების პრობლემების ზრდა დაკავშირებულია კომპიუტერული ქსელების განვითარებასა და გავრცელებასთან. განაწილებულმა სისტემებმა და დაშორებულ სისტემებთან წვდომამ წინა პლანზე წამოსწია დასამუშავებელი და გადასაცემი ინფორმაციის უსაფრთხოების პრობლემა. თანამედროვე საბანკო სისტემების თავისებურებები უარყოფითად მოქმედებს ინფორმაციის უსაფრთხოებაზე.

საბანკო სისტემა წარმოადგენს ღია სისტემას, რომელშიც ავტომატიზებულ სამუშაო ადგილებსა და ქვესისტემებს შორის დამყარებულია კავშირები.

მიუხედავად ინფორმაციის კრიპტოლოგიური დაცვისა, არაეფექტურია პაროლებით ინფორმაციის დაცვა. საბანკო საინფორმაციო სისტემები მუშაობენ ოპერაციული სისტემების გარემოში და სისტემის უსაფრთხოება დამოკიდებულია გამოყენებული ოპერაციული სისტემის დაცვის ხარისხზე. უსაფრთხოების

ნებისმიერი ღონისძიების მიზანს წარმოადგენს ბანკის მფლობელისა, და კანონიერი კლიენტის დაცვა სისტემაზე შემთხვევით ან განზრახ ზემოქმედების შედეგად მოსალოდნელი მატერიალური და მორალური ზიანის მიყენებისაგან.

მანამ, სანამ განვიხილავთ ბანკში ინფორმაციის დაცვის მეთოდებს და საშუალებებს, და ვინაიდან დაცული უნდა იყოს ბანკის საიდუმლო და კომერციული ინფორმაცია, საჭიროა დავადგინოთ, რომელი ინფორმაცია საჭიროებს დაცვას და რა არის საბანკო საიდუმლოება.

კომერციული ინფორმაციის ცნებაში იგულისხმება ნებისმიერი კონფიდენციალური და მმართველობითი, სამეცნიერო-ტექნიკური, საქმიანი და სხვა სახის ინფორმაცია, რომელიც ფასეულია ბანკისთვის კონკურენტებთან უპირატესობების მისაღწევად და მოგების მისაღებად.

ტერმინი „საბანკო საიდუმლო“ შეიძლება ორნაირად გავიგოთ:

პირველი – საბანკო საიდუმლოებაში ესმით კომერციული საიდუმლოების ერთ-ერთი სახე, ბანკის კუთვნილობაში არსებული კონფიდენციალური ინფორმაცია.

მეორე – ბანკის საიდუმლოებაში, ვიწრო გაგებით, ესმით:

- საკრედიტო დანესებულების ვალდებულება, შეინახოს საიდუმლოდ კლიენტის მიერ შესრულებული ოპერაციები, ანაბრები და სხვ;

- კლიენტის ანგარიშზე საშუალებების მოძრაობა და ნაშთი;

- მიღებული დეპოზიტების და გაცემული კრედიტების რაოდენობა და სტრუქტურა;

- მონაცემები ბანკის კლიენტების, აქციონერების და თანამშრომლების შესახებ;

- ფასიან ქაღალდებში ინვესტიციების რაოდენობა;

- დანვრილებითი ბალანსი და საბუღალტრო ანგარიშგებები;

- ხელფასი და სოციალური გადახდები;

- კონკრეტული დოკუმენტები, ინფორმაციის სხვა სახის მატარებლები, ზეპირი ინფორმაციის კონკრეტული მოცულობა.

საბანკო საინფორმაციო სისტემის უსაფრთხოებაში იგულისხმება ბანკის ნორმალური ფუნქციონირების პროცესში შემთხვევით ან განზრახ ჩარევის შემთხვევაში მისი დაცულობის მდგომარეობა. განასხვავებენ საბანკო საინფორმაციო სისტემის გარე და შიდა უსაფრთხოებას. გარე უსაფრთხოების სისტემა უზრუნველყოფს როგორც შიგა შემთხვევითი ზემოქმედების ან, ასევე, ინფორმაციასთან ნებისმიერი არასანქცირებული შელწევისაგან დაცვას. შიგა უსაფრთხოების სისტემა დაკავშირებულია მომხმარებლისა და მომსახურე პერსონალის საქმიანობის რეგლამენტირებასთან, ორგანიზაციის რესურსებსა და ინფორმაციასთან შელწევასთან.

ინფორმაციის ძირითად საფრთხეებს მიეკუთვნება:

- კონფიდენციალური ინფორმაციის გახსნა, რომელიც ხორციელდება ინფორმაციასთან არასანქცირებული წვდომით, არხების მოსმენით და სხვ.;
- ინფორმაციის არასანქცირებული გამოყენება, – ინფორმაციის გახსნისა და მოდიფიკაციის საშუალება, რამაც მომხმარებელს შეიძლება მიაყენოს ფინანსური ზარალი;
- ინფორმაციის შეცვლა, ანუ მონაცემთა ბაზაში არასანქცირებული ცვლილებების განხორციელება, რის გამოც მომხმარებელი იძულებულია, უარი თქვას ასეთი ინფორმაციის გამოყენებაზე, რამდენადაც დამატებითი ძალისხმევაა საჭირო მის აღსადგენად;
- ინფორმაციის შეცდომით გამოყენება იმ შეცდომის შედეგია, რომელსაც ადგილი აქვს ბანკის საინფორმაციო სისტემის პროგრამულ უზრუნველყოფაში;
- მომსახურებაზე უარი – ინფორმაციის მიწოდების დაყოვნება, რამაც შეიძლება გამოიწვიოს მომხმარებლის მცდარი მოქმედება;
- მიღებულ ინფორმაციაზე უარი – როცა ინფორმაციის გადამცემი ან მიმღები არ აღიარებს ინფორმაციის მიღების ან გა-

დაცემის ფაქტს, რომელმაც მნიშვნელოვნად შეიძლება დააზარალოს ერთ-ერთი მხარე.

ინფორმაციის უსაფრთხოებას დამატებით სიძნელეებს უქმნის ლოკალური და გლობალური ქსელების გამოყენება, რაც დაკავშირებულია კავშირის არსებით ინფორმაციის გადაცემისას მის იდენტიფიკაციასთან.

ინფორმაციის დაცვის ღონისძიებების გატარებამ შეიძლება გამოიწვიოს:

- დაცულ ინფორმაციასთან მუშაობის გართულება;
- დაცული ინფორმაციის ღირებულების გაზრდა;
- სისტემის რესურსების დამატებითი დატვირთვა;
- სისტემის დაცვის მიზნით დამატებითი პერსონალის გამოყენება.

ობიექტის დაცვამ ხელი არ უნდა შეუშალოს მის სასარგებლოდ გამოყენებას. მხედველობაშია მისაღები, რომ ბანკი წარმოადგენს ღია სისტემას, რაც გამოიხატება კლიენტებთან, ბანკ-კორესპონდენტებთან და ბირჟებთან კავშირის დამყარებაში.

ამრიგად, დაცვის სისტემის დაპროექტებისას გასათვალისწინებელია სისტემის დაცვის მდგომარეობის შეთანხმებულობა ბანკის საინფორმაციო სისტემის ინფორმაციის გახსნილობასთან.

დღეისათვის აღიარებული და მიღებულია ინფორმაციული ტექნოლოგიების დაცვის შეფასების შემდეგი კრიტერიუმები: **კონფიდენციალობა** – ინფორმაციის დაცვა არასანქცირებული მიღებისაგან; **მთლიანობა** – ინფორმაციასთან არასანქცირებული წვდომისაგან დაცვა.

ინფორმაციის დაცვა შეიძლება შემდეგი ფუნქციების განხორციელების საფუძველზე: იდენტიფიკაცია და აუთენტიფიკაცია მომხმარებლის ნამდვილობის შემოწმება; ახალი მომხმარებლის რეგისტრაცია და ძველის ამოღება; შეღწევის მართვა – მონაცემთა ბაზებთან წვდომის შეზღუდვა და მომხმარებლის ბაზებთან შეღწევის უფლებამოსილების განსაზღვრა; აუდიტი – მომხმარებლის მიერ შესრულებული მოქმედებების კორექტუ-

ლობის შემოწმება, სისტემაში მომხმარებლის მიერ შესრულებული ოპერაციების დაფიქსირება; ობიექტის ხელმეორედ გამოყენება – მომხმარებლის მოქმედებამ არ უნდა მიიყვანოს სისტემა იქამდე, რომ შეუძლებელი გახდეს მონაცემთა ბაზების გამოყენება; ინფორმაციის სიზუსტე – იგულისხმება სისტემის ცალკეულ ნაწილებს შორის ცალსახა შესაბამისობა, რომელიც უზრუნველყოფს კავშირების სიზუსტეს და მონაცემების შეუცვლელობას ინფორმაციის გაცვლისას; მომსახურების საიმედოობა – იმის გარანტია, რომ მომხმარებელი დროულად მიიღებს მოთხოვნილ ინფორმაციას, რომ რესურსებთან წვდომის დრო არ გადაჭარბებს მოცემული პროცედურის შესრულებისთვის დასაშვებ დროს; ინფორმაციის გაცვლა – საკომუნიკაციო არხების მეშვეობით უზრუნველყოფს გარე სამყაროსთან ინფორმაციის უსაფრთხო გაცვლას და წაუყენებს მოთხოვნებს შემდეგი ფუნქციების უსაფრთხო განხორციელებას: აუთენტიფიკაცია, წვდომების მართვა, კონფიდენციალობა, მთლიანობა, შესასრულებელი მოქმედებების შეუძლებლობა.

არასანქცირებული შეღწევისაგან დაცვის მთავარ საშუალებას წარმოადგენს შეღწევების გამიჯვნა. ეს უკანასკნელი უზრუნველყოფს: მონაცემებთან შეღწევის გამიჯვნას, საბეჭდო მონაცემებთან შეღწევის გამიჯვნას, პროცესების იზოლირებას, ე.ი. მომხმარებელს შეუძლია მხოლოდ თავის რესურსებთან შეღწევა.

გარე მატარებლებზე მონაცემების არასანქცირებული ჩაწერის ან ინფორმაციასთან არასანქცირებული შეღწევის თავიდან აცილების მიზნით უნდა განხორციელდეს ისეთი ღონისძიებები, როგორიცაა:

- მომხმარებლის იდენტიფიკაცია და აუთენტიფიკაცია, მომხმარებლის მიმაგრება მის მიერ შესრულებულ პროცესებთან;
- მომხმარებლის მიერ განხორციელებული მოქმედებების რეგისტრაცია;
- მომხმარებლის რეგისტრაციისა და ამოგდების შესაძლებლობა, ქვესისტემების ჩამონათვლის შეცვლა და მომხმარებლის უფლებების შეცვლა.

**არასანქცირებული შეღწევის მცდელობისას რეაქციის სახე-
ები:**

- სიგნალის გამოცემა, დაბლოკვა, არასანქცირებული შეღწე-
ვის აღდგენა, ტესტირება;
- ოპერატიული მეხსიერებისა და დაცულ მონაცემებთან მუშა-
ობის შემდეგ ინფორმაციის მატარებლების სამუშაო არის
განმენდა;
- ანგარიშგებების, გამომავალი ფორმებისა და ასლების აღრი-
ცხვა;
- პროგრამული და ინფორმაციული ნაწილის მთლიანობის კონ-
ტროლი.

მონაცემების დაცვა შეიძლება განხორციელდეს ფრაგმენ-
ტულად ან კომპლექსურად.

ინფორმაციის ფრაგმენტულად დაცვა გულისხმობს გარკვე-
ულ პირობებში მკაცრად განსაზღვრული საფრთხისაგან დაცვას.
ასეთი მიდგომის ღირსებას წარმოადგენს კონკრეტული საფრ-
თხისაგან დაცვის მრავალი საშუალების ამორჩევის შესაძლე-
ბლობა. აქედან გამომდინარე, ამ მეთოდის უარყოფითი მხარეა
მისი ლოკალური მოქმედება. ამრიგად, ფრაგმენტული დაცვის
მეთოდი უზრუნველყოფს საბანკო საინფორმაციო სისტემის
კონკრეტული ელემენტის დაცვას კონკრეტული საფრთხისაგან.

კომპლექსური დაცვის დროს ადგილი აქვს საფრთხეების წი-
ნააღმდეგ რამდენიმე დაცვის მეთოდის (სამართლებრივი, პროგ-
რამულ-ტექნიკური, ორგანიზაციული) გამოყენებას. დაცვის
სისტემების აგება უნდა მოხდეს შემდეგი თანმიმდევრობით:

- მოქმედი ნორმატიული ბაზის შესწავლა;
- საბანკო საინფორმაციო სისტემის ანალიზი და დასაცავი ობ-
იექტების გამოყოფა;
- დაცვის სისტემისთვის წაყენებული მოთხოვნების ფორმირე-
ბა;
- დაცვის სისტემის რეალიზება.

ინფორმაციის დაცვის სისტემის შექმნა გადის რამდენიმე ეტაპს:

პირველ ეტაპზე წარმოებს სააღმსრულებლო ორგანოების სტრუქტურის დადგენა. ბანკის ყველა დაწესებულებაში უნდა ჩამოყალიბდეს საშემსრულებლო ორგანოები, რომლებიც პრაქტიკულად განახორციელებენ ინფორმაციის დაცვის სამუშაოებს. ეს შეიძლება იყოს დაწესებულების ინფორმაციული უსაფრთხოების ადმინისტრირების ჯგუფი.

ბანკის შიგა კონტროლის სამსახურის ძირითადი ფუნქციები:

- ინფორმაციული ნაკადების სქემების შედგენა, წარმოება და ანალიზი, რათა გამოვლინდეს ინფორმაციის დაცვაში არსებული ნაკლოვანებები და შემუშავდეს მათი აღმოფხვრის ღონისძიებები;
- თანამშრომლების მიერ ტექნოლოგიური ოპერაციების ორგანიზება და შესრულება;
- თანამშრომლებისათვის აპარატურულ, პროგრამულ და ინფორმაციულ რესურსებთან შეღწევის უფლებამოსილების განსაზღვრა;
- ინფორმაციის კოლექტიური და ინდივიდუალური გამოყენებისას უსაფრთხოების დაცვის საშუალებების ექსპლუატაციაში და ორგანიზებაში მონაწილეობის მიღება;
- ბანკის თანამშრომლებისათვის და კლიენტებისათვის ინფორმაციულ უსაფრთხოებაზე ინსტრუქტაჟის ჩატარება და უსაფრთხოების საშუალებების გამოყენების სწავლება;
- ბანკის თანამშრომლების მხრიდან უსაფრთხოების მოთხოვნების დაცვის კონტროლი და იმ შემთხვევების გამოკვლევა, რომელსაც ადგილი ჰქონდა ინფორმაციის დაცვის სფეროში.

მეორე ეტაპზე უნდა განისაზღვროს დაცვის ობიექტები. ამ ეტაპზე, გამომდინარე ინფორმაციის მატარებლებიდან, გავრცელების არხებიდან, შენახვისა და დამუშავების საშუალებებიდან, განისაზღვრება დასაცავი ინფორმაციის სახეები. შემდეგ უნდა დადგინდეს ამა თუ იმ ინფორმაციის კონფიდენციალობის ხარისხი და გამომდინარე მათი დაცვის ხარისხიდან, მოხდეს ინფორმა-

ციის დაყოფა კატეგორიებად. აქვე უნდა დადგინდეს თითოეული კატეგორიის ინფორმაციის მიხედვით პოტენციური საფრთხეები.

მესამე ეტაპზე უნდა განხორციელდეს ინფორმაციის აღმოცენების, გავრცელების, შენახვისა და დამუშავების ანალიზი. ამ დროს დგება ინფორმაციის ტექნოლოგიური სქემები, მიიღება რა მხედველობაში ბანკის თითოეული დანესებულების მიერ შესრულებული ფუნქციები და მათ მიერ გამოყენებული არხები და საშუალებები. ამ ეტაპზე ყურადღება უნდა გამახვილდეს გამოყენებულ საგადამხდელო სისტემაზე, ელექტრონული დოკუმენტბრუნვის სისტემაზე, პლასტიკური ბარათების გამოყენებით ინფორმაციულ უზრუნველყოფაზე, ბანკის საინფორმაციო სისტემაზე და სხვ.

მეოთხე ეტაპზე ხორციელდება შესაძლო საფრთხეების ანალიზი და მათგან დაცვის პრიორიტეტული მიმართულებები. ინფორმაციის დაცვა უნდა განხორციელდეს:

- არასანქცირებული წვდომისა და კოპირებისაგან;
- არასანქცირებული ცვლილებებისა და ბლოკირებისაგან;
- ინფორმაციის არასანქცირებული გადაცემისა და მიღებისაგან.

პოტენციური საფრთხეების სახეები დამოკიდებულია მრავალ ფაქტორზე:

- ბანკის ფილიალების ქსელის არსებობაზე;
- ბანკის განყოფილებებთან კავშირის არსებზე;
- ბანკში გამოყენებული ქსელების სტრუქტურაზე;
- ბანკის მიერ განხორციელებულ მომსახურების სახეებსა და ბანკში ინფორმაციის დამუშავების ჩამოყალიბებულ ტექნოლოგიაზე;
- ბანკის პერსონალის სტრუქტურაზე.

მეხუთე ეტაპზე წარმოებს ძირითადი მარეგლამენტირებელი დოკუმენტების შემუშავება.

ბანკის უსაფრთხოების კონცეფციისა და ინფორმაციული უსაფრთხოების სამსახურის მუშაობის ძირითადი მიმართულებებისა და სხვა დოკუმენტების შემუშავებისას გაითვალისწინება შემდეგი ფაქტორები:

- თითოეული სახის ინფორმაციისთვის უსაფრთხოების ხარისხი;
- ბოროტმზრახველების შესაძლო ტიპები;
- ბოროტმზრახველების შესაძლო მოლაპარაკება ბანკის თანამშრომლებთან;
- სხვა ფაქტორები.

მარეგლამენტირებელი დოკუმენტები უნდა ეყრდნობოდეს, ერთი მხრივ, ინფორმაციასთან მინიმალური წვდომის პრინციპებს და, მეორე მხრივ, დაცვის საკმარისობის პრინციპებს. ბანკის უსაფრთხოების უზრუნველყოფის მეთოდები და ინსტრუქციები უნდა შედგეს:

- ბანკის დაწესებულებების ინფორმაციული უსაფრთხოების მოთხოვნათა გათვალისწინებით;
- ბანკის ანტივირუსული მუშაობის რეგლამენტის საფუძველზე;
- ინფორმაციულ რესურსებთან მომხმარებლის წვდომის რეგლამენტის საფუძველზე;
- კადრების გადაადგილების შემთხვევაში, შეიძლება შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დარღვევების ფაქტების გამოძიების მეთოდის საფუძველზე ინფორმაციასთან წვდომის უფლებების შეცვლა.
- ბანკის საინფორმაციო სისტემების ავტომატიზებული სამუშაო ადგილების უსაფრთხოების უზრუნველყოფის ინსტრუქციების და მეთოდების საფუძველზე.

მეექვსე ეტაპზე წარმოებს ინფორმაციული უსაფრთხოების სამსახურის ფორმირება. ეს სამსახური შედგება შემდეგი სახის სპეციალისტებისაგან:

- ფიზიკურ არხებში ინფორმაციის დაცვის;
- ლოკალური გამოთვლითი ქსელების დაცვის;
- საბანკო საინფორმაციო სისტემის დაცვის;
- პლასტიკური ბარათების საფუძველზე აგებული საგადამხდელო სისტემების დაცვის. აგრეთვე სასურველია, შტატში ირიცხებოდეს სპეციალისტკრიპტოლოგი.

აღნიშნული ეტაპების გავლის შემდეგ შესაძლებელია დაცვის საშუალებების ამორჩევა. საშუალებების შერჩევისას გარდა

შერჩეული საშუალებების ხარისხისა, ყურადღება უნდა გამახვილდეს ფირმამწარმოებლის მდგომარეობაზე. ფირმას უნდა გააჩნდეს სახელმწიფოს მიერ გაცემული ლიცენზია არასანქცირებული შელწევებისაგან დაცვისა და კრიპტოგრაფიის სფეროში საქმიანობის შესახებ.

დაცვის საშუალებების ამორჩევის შემდეგ დგება საკითხი ამ საშუალებების დანერგვისა და თანხლების შესახებ, რაც საჭიროებს საკმარისად დიდ დროს. ამ ეტაპზე ძირითად განსახილველ პრობლემას წარმოადგენს:

- ბანკის საგადამხდლო სისტემის დაცვა;
- ელექტრონული დოკუმენტბრუნვის სისტემა;
- საბანკო საინფორმაციო სისტემა;
- პლასტიკურ ბარათებზე აგებული საგადამხდლო სისტემა;
- ინფორმაციის გადაცემის ფიზიკური არხები.

მუდმივად უნდა წარმოებდეს ინფორმაციის უსაფრთხოების სფეროში დარღვევების შესახებ ინფორმაციის დაფიქსირება და ბანკისადმი მიყენებული ზარალის განსაზღვრა. უნდა გატარდეს ღონისძიებები მსგავსი შემთხვევების განმეორების თავიდან ასაცილებლად.

უსაფრთხოების უზრუნველყოფის საქმეში დიდი მნიშვნელობა აქვს ბანკის პერსონალთან მუშაობას, ვინაიდან ინფორმაციული უსაფრთხოება ხშირ შემთხვევაში ირღვევა მათი მხრიდან. ბანკის თანამშრომელი გასცემს კონფიდენციალურ ინფორმაციას იმ პირზე, რომელსაც არ გააჩნია აღნიშნული ინფორმაციით სარგებლობის უფლება.

ინფორმაციული უსაფრთხოების დაცვის საშუალებების გამოყენება ამა თუ იმ ზომით ძირითადად საჭიროებს ადამიანის მონაწილეობას. ინფორმაციული უსაფრთხოების უზრუნველყოფა აგრეთვე, ევალება საინფორმაციო სისტემების უშუალო მომხმარებელსაც. ამიტომ ბანკის პერსონალს წარმოდგენა უნდა ჰქონდეს დაცვის მეთოდებზე, საშუალებებზე, რაც საბოლოოდ უზრუნველყოფს ისეთი პრობლემების გადაჭრას, როგორიცაა: ინფორმაციის დაცვის საშუალებების შენახვა;

- ინფორმაციის დაცვა კოპირებისაგან;

- დაცვის საჯარო საშუალებების გამოყენება;
- ანტივირუსული უსაფრთხოება;

კომპიუტერული და ინფორმაციული უსაფრთხოების ცოდნის შემოწმების მიზნით, პერიოდულად უნდა განხორციელდეს ბანკის თანამშრომლების ატესტაცია.

ინფორმაციული უსაფრთხოების თითოეული საშუალებებისა და მეთოდების საჭიროა შესაბამისი რისკების გაანგარიშება.

კითხვები თვითშემოწმებისთვის

1. რა უარყოფითი სოციალურ-ეკონომიკური შედეგები შეიძლება გამოიწვიოს კომპიუტერის უკონტროლო და კანონდარღვევით გამოყენებამ?
2. მოიყვანეთ ინფორმაციზაციის სფეროში სამართალდარღვევების მაგალითები.
3. რომელი კომპიუტერული დანაშაული მიეკუთვნება ფიზიკურ კომპიუტერულ დანაშაულს?
4. რომელი კომპიუტერული დანაშაული მიეკუთვნება ტექნიკურ კომპიუტერულ დანაშაულს?
5. რომელი კომპიუტერული დანაშაული მიეკუთვნება ინტელექტუალურ კომპიუტერულ დანაშაულს?
6. რა სახის ვირუსული პროგრამებია თქვენთვის ცნობილი?
7. დაახასიათეთ კომპიუტერული სისტემების უსაფრთხოებისა და შესაბამისად, კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლის ღონისძიებები.
8. ანტივირუსული პროგრამების გამომწვევი ფირმებიდან რომელია თქვენთვის ცნობილი?
9. რა დაავადებების გამომწვევა შეუძლია პერსონალურ კომპიუტერთან ხანგრძლივ და უკონტროლო მუშაობას?
10. რა განსხვავებაა კრიპტოგრაფიასა და კრიპტოანალიზს შორის?
11. რა ნაწილებისაგან შედგება კრიპტოგრაფია?
12. რისთვის გამოიყენება ციფრული ხელმოწერა?
13. დაახასიათეთ ინფორმაციის ძირითადი საფრთხეები.

14. რა თანმიმდევრობით უნდა განხორციელდეს ბანკში დაცვის სისტემის შემუშავება?
15. რა ღონისძიებებია განსახორციელებელი შეღწევის გამიჯვნის მხარდაჭერისთვის?
16. რა სახის სპეციალისტები უნდა გაერთიანდნენ დაცვის ჯგუფში?
17. დაცვის რა მეთოდები არსებობს საბანკო საინფორმაციო სისტემების დასაცავად?

დასკვნა

დამხმარე სახელმძღვანელო „საბანკო საინფორმაციო სისტემები“ შედგენილია ინფორმაციული ტექნოლოგიების მენეჯმენტის მაგისტრატურის მოდულის სტუდენტებისათვის. წიგნში განხილული საკითხები დალაგებულია სილაბუსის სტრუქტურის შესაბამისად. მასში განხილული საკითხები სრულად ასახავს დისციპლინაში „საბანკო საინფორმაციო სისტემები“ მოქმედ სილაბუსში განხილულ თემებს და საკითხებს. დამხმარე სახელმძღვანელო სტუდენტებს დაეხმარება შეისწავლონ კომერციულ ბანკებში თანამედროვე ინფორმაციული ტექნოლოგიების გამოყენების არსებული მდგომარეობა და პერსპექტივები. წიგნში გაშუქებული მასალის ათვისებისა და ცოდნის დამაგრების მიზნით, თითოეული თემის ბოლოს მასალის ათვისების თვითშემოწმებისთვის მოცემულია კითხვები. გარდა ინფორმაციული ტექნოლოგიების მენეჯმენტის მოდულის სტუდენტებისა, წიგნი დაეხმარება ფინანსებისა და საბანკო საქმიანობის მოდულის სტუდენტებს სპეციალობის ღრმად დაუფლებაში. ვფიქრობთ, წიგნში განხილული საკითხები სასარგებლო იქნება ბანკის თანამშრომლებისთვისაც.

ქართულ-ინგლისური აბრევიატურა

აბ – ავტომატიზებული ბანკი

ასა – ავტომატიზებული სამუშაო ადგილი

ეგმ – ელექტრონული გამომთვლელი მანქანა

სგასა – საკრედიტო განყოფილების

ავტომატიზებული სამუშაო ადგილი

სს – საინფორმაციო სისტემა

სსს – საბანკო საინფორმაციო სისტემა

APC – American Pover Conversion

ATM – automated teller mashine

BACS – bankers Automated Clearing Services

EAF – Elektronishe Abrechnung Frankfur

EAF – Euro Access Furt

CHIPS – Clearing Hous Interbank Payment System

SIC – Swiss Interbank Clearing

S.W.I.F.T. – Sosietyfor World-wide Interbank Financial Teleco-
mmunication

TARGET – Trans Europen Real-time Cross Settle-ment Expres
Transfere System

TCD – Teller Cash Dispenser

TCO – Total cost of Ownership

TTS – Transaction Tracing system

გამოყენებული ლიტერატურა

1. ი. კოვზანაძე, გ. კონტრიძე. თანამედროვე საბანკო საქმე თეორია და პრაქტიკა. თბილისი, 2014. გვ. 15.
2. მალრაძე მ. საბანკო საინფორმაციო სისტემები, გვ. 21-22, გამომცემლობა თბილისის სახელმწიფო უნივერსიტეტი, 2016.
3. Николаева И. Как вести бухгалтерский учет кредитов и займов, 2024. <https://surli.cc/rwnfvb>.
4. Банковское оборудование: основные виды, 2020. <https://surli.cc/kybroc>.
5. Какие основные функции выполняют банкоматы в современном мире? 2024. <https://surl.lu/btvbsl>.
6. რომელ ბანკებს აქვთ საქართველოში ყველაზე ფართო მომსახურების ქსელი? 2020. <https://surl.li/jefomu>.
8. Автоматизированное рабочее место банковского работника, 2020. <https://surl.lu/qmmgdc>.
9. Пластиковые карты и их виды, 2024. <https://surl.li/wtmdzc>.
10. Банковские карты в Грузии: какие работают в мае – июне 2025 года. <https://surl.li/ykbpzo>.
11. მობილბანკში გაზაფხულის კამპანია დაიწყო, 2025. <https://surli.cc/rgzcgf>.
12. სიჭინავა დ., მალრაძე მ. ელექტრონულ ფულზე გადასვლის წანამდღერები და პრობლემები. ჟურნალი „გლობალიზაცია და ბიზნესი“, 6, 2018.
13. Букия Г. Б., Сичинава Д. Ш. и др. Общегосударств. автоматизированные системы безналичного расчета. Сообщение АН ГССР, 1976, том 83, №3, ст. 117-123.
14. მალრაძე მ., ელექტრონული ფული მსოფლიო ფული, ეკონომიკის აქტუალური პრობლემები. (სამეცნიერო ნაშრომთა კრებული). თსუ გამომცემლობა. 1998, ტ. 7, გვ. 87-90.
15. Сколько существует криптовалют? Растущая индустрия <https://www.binance.com/ru/square/post/15938243955041>.
16. График общей рыночной капитализации криптовалют. <https://coinstats.app/ru/market-cap-charts>.
17. სიჭინავა დ., მალრაძე მ. კრიპტოვალუტის მაინინგი: არსებული მდგომარეობა და პერპექტივები. გლობალიზაციის გამოწვევები ეკონომიკასა და ბიზნესში. მე-3 საერთაშორისო კონფერენციის შრომების კრებული, 2018. <https://surl.li/yznkn>.

18. Краны криптовалют – что это, как работают, в чём их смысл? (2024). <https://surl.li/xkrdoq>.
19. Чем известен Дэвид Чаум в мире криптовалют (2022). <https://surl.li/nqldnf>.
20. История блокчейна: как технология блокчейн меняет мир? (2022). <https://surl.li/lttulb>.
21. Sichinava D. Cryptocurrency – A Future Medium of Exchange. Economics and Business, Journal (2019). <http://www.eb.tsu.ge>.
20. Стейблкоины: что это такое и как они работают? (2024). <https://surl.lu/dqlfsl>.
22. PayPal запустил свой стейблкоин (2023). <https://habr.com/ru/news/753374/>.
23. Цифровая валюта: Будущее ваших денег (2023). <https://surl.li/unrmma>.
24. cifruli lari – ras mogvitans erovnuli bankis kriptovaluta (2021). <https://eb.tsu.ge/doc/4.pdf>.
25. Нестеров И. О. цифровые валюты центральных банков: инновационный инструмент для более эффективных внутренних и международных расчетов (2023). <https://economicsjournal.spbu.ru/article/view/13885>.
26. Названы страны, запустившие цифровые валюты ЦБ (2023). <https://surl.li/vwdhgi>.
27. ЦБ Швеции завершил первый этап тестирования национальной цифровой валюты, 2021.
28. Глава НБГ рассказал о переходе к цифровому лари на форуме euromoney (2022). <https://spress.ge/50313/>.
29. Цифровая валюта Sand Dollar борется за свою значимость после падения FTX (2023). <https://surl.li/ykixzy>.
30. В ЕЦБ оценили последствия введения цифрового евро, 2022. <https://surl.li/kcuqyt>.
31. Цифровая иена. <https://surl.li/jooxxw>.
32. Банк Кореи начинает пилотное тестирование цифровой валюты (2025). <https://surl.li/niyfoo>.
33. erovnuli banki cifruli laris proeqtis Semdeg etapze gadadis (2023). <https://businessformula.ge/News/12394>.
34. Техпартнером НБГ в проекте CBDC стала компания ripple, 2023). <https://spress.ge/56707/>.
35. AML и KYC: О сложных понятиях простыми словами (2022). <https://surl.lu/xxhbbw>.

36. Из чего складывается цена биткоина, и какие факторы на неё влияют? (2020). <https://surl.li/owprhx>.
37. Путь к господству биткоина: 13 событий, определивших будущее денег (2020). <https://surl.lt/rsxnvf>.
38. Эксперты рассказали, сколько стоит добыть биткоин, (2019). <https://surl.li/npwkjd>.
39. Сколько всего Ripple есть сегодня – сколько будет завтра? <https://surl.lu/cffinen>.
40. Количество Биткоинов ограничено или нет?, (2024) <https://surl.li/rkrenk>.
41. Как будет формироваться курс libra и gram, (2019). <https://surl.lu/jeijqk>.
42. От чего зависит курс Bitcoin? 2020. <https://surli.cc/ppcuky>.
43. Джеймс Альтушер: к 2020 году биткоин будет стоить \$1 млн., 2020. <https://surli.cc/ithhie>.
44. vin arian e.w **Bitcoin** veSapebi, 2024. <https://dev.ge/news/bitk-1709627659>.
45. Bitcoinis Rirebulebam rekordul niS-nuls miaRwia. <https://surl.li/mjctp>.
46. Научно-Технический Энциклопедический Сло-варь. <https://surl.lu/ypamwv>.
47. Сколько всего биткоинов в обращении и когда будет добыт последний, 2024. <https://dzengi.com/ru/skolko-vsego-bitkoinov> .
48. Лучшие криптобиржи в 2025: ТОП рейтинг криптовалютных бирж, 2025. <https://surl.lu/rtxpyt>.
49. Количество криптобанкоматов в мире уже превышает 39 тыс, 2022. <https://surl.li/pzvg tq>.
50. 2024 Year Review & 2025 Year Ahead, 2024. <https://crypto.com/en/-research/2024-review-2025-ahead>.
51. Balancing Innovation and Protection: Under-standing the Landscape for DeFi Regulation, 2022. <https://surl.li/veksms>.
52. Cryptocurrencies: Regulatory Perspectives and Implications for Investors, 2021. <https://surl.lu/nkveme>.
53. Oksana A. Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions, 2024. <https://surl.li/xektss>.
54. Cryptocurrency regulations are changing across the globe. Here's what you need to know, 2024. <https://surl.lt/ioopis>.
55. The State of Cryptocurrency Regulations in China, 2024. Cryptocurrency.Law. <https://surl.lu/revnmj>.
56. Cryptocurrency regulations are changing across the globe. Here's what you need to know, 2024. <https://surl.lu/jkonmz>.
57. Global Regulatory Outlook for Cryptocurrencies, 2024. <https://surl.li/xocvhw>.

58. SEC признала 37 криптовалют ценными бумагами: что теперь будет, 2023. <https://surl.li/zkmyrq>.
59. ra aris MiCA (kripto aqotivebis bazrebis regulacia)? 2023. <https://surl.li/eawrjw>.
60. В каких странах мира запрещены криптовалюты? 2024. <https://surl.li/swnsdf>.
61. Золотая лихорадка: почему в Грузии выгодно "до-бывать" криптовалюту, 2018. <https://surl.li/imdhsy>.
62. Factors Influencing Cryptocurrency Adoption in Georgia, 2022. <https://surl.li/smdygz>.
63. Cryptocurrency in Georgia & Tbilisi: A Comprehensive Guide, 2023. <https://surl.cc/yhlqxz>.
64. Криптовалюта в Грузии | Правовые и налоговые рамки. <https://surl.li/jrlzjl>.
65. Система SWIFT: что это такое, зачем нужна и как работает в России, 2022. <https://surl.cc/tpshsm>.
66. maRraZe. m. informaciuli menejmenti, (2017). damxmare saxelmZRvanelo. gamomcemloba „universali“, 2017.
67. Тендер, 2023. <https://surl.li/blgjf>.
68. Глобальное состояние интернета в феврале 2025 года. <https://surl.li/xsdagy>.
69. Потери от киберпреступности, 2025. <https://surl.li/zzyqsa>.
70. Что такое вредоносное ПО? 2025. <https://surl.li/nwxmiu>.

