ინფორმაციული უსაფრთხოების უზრუნველყოფის ძირითადი პრინციპები საბანკო სისტემაში

ოთარ შონია, აკაკი შონია, კორნელი ოდიშარია, ნინო ცომაია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

დეტალურადაა განხილული საბანკო სისტემის ინფორმაციული ინფრასტრუქტურის ყველა დონის საშიშროებათა წყაროები, წარმოდგენილია მათგან დაცვის ძირითადი მოთხოვნები, ჩამოყალიბებულია საბანკო ობიექტების კომპლექსური დაცვის კონცეფცია. მოცემულია საქართველოს საბანკო სისტემაში ინფორმაციული უსაფრთხოების თვალსაზრისით არსებული მდგომარეობის ანალიზი, წარმოდგენილია რეკომენდაციები.

საკვანძო სიტყვები: საბანკო სისტემა. საკრედიტო ორგანიზაცია. საშიშროების წყარო. დაცვის კონცეფცია, ინფორმაციული უსაფრთხოება.

1. შესავალი

პრაქტიკა გვიჩვენებს, რომ საფრთხეებისათვის ეფექტური წინააღმდეგობის გაწევის და ბანკის, საკრედიტო ორგანიზაციის ან ნებისმიერი ფირმის უსაფრთხო და სტაბილური მუშაობის პირობების შექმნისათვის უნდა ჩამოყალიბდეს დაცვის კომპლექსური სისტემა და უზრუნველყოფილ იქნას მისი სწორად ფუნქციონირება.

2. ძირითადი ნაწილი

ბანკები, საკრედიტო ორგანიზაციები ან ფირმები ინდივიდუალურებია, ამიტომ მათი კომპლექსური დაცვის სისტემებიც ინდივიდუალურია. აქ უსაფრთხოების უზრუნველყოფის აუცილებელი მიმართულებები უნდა იყოს:

- პერსონალის და კლიენტების სიცოცხლე, ჯანმრთელობა;
- შენობა, მოწყობილობები, ქონება და ფასეულობები;
- ინფორმაცია მისი ყველა ფორმით.

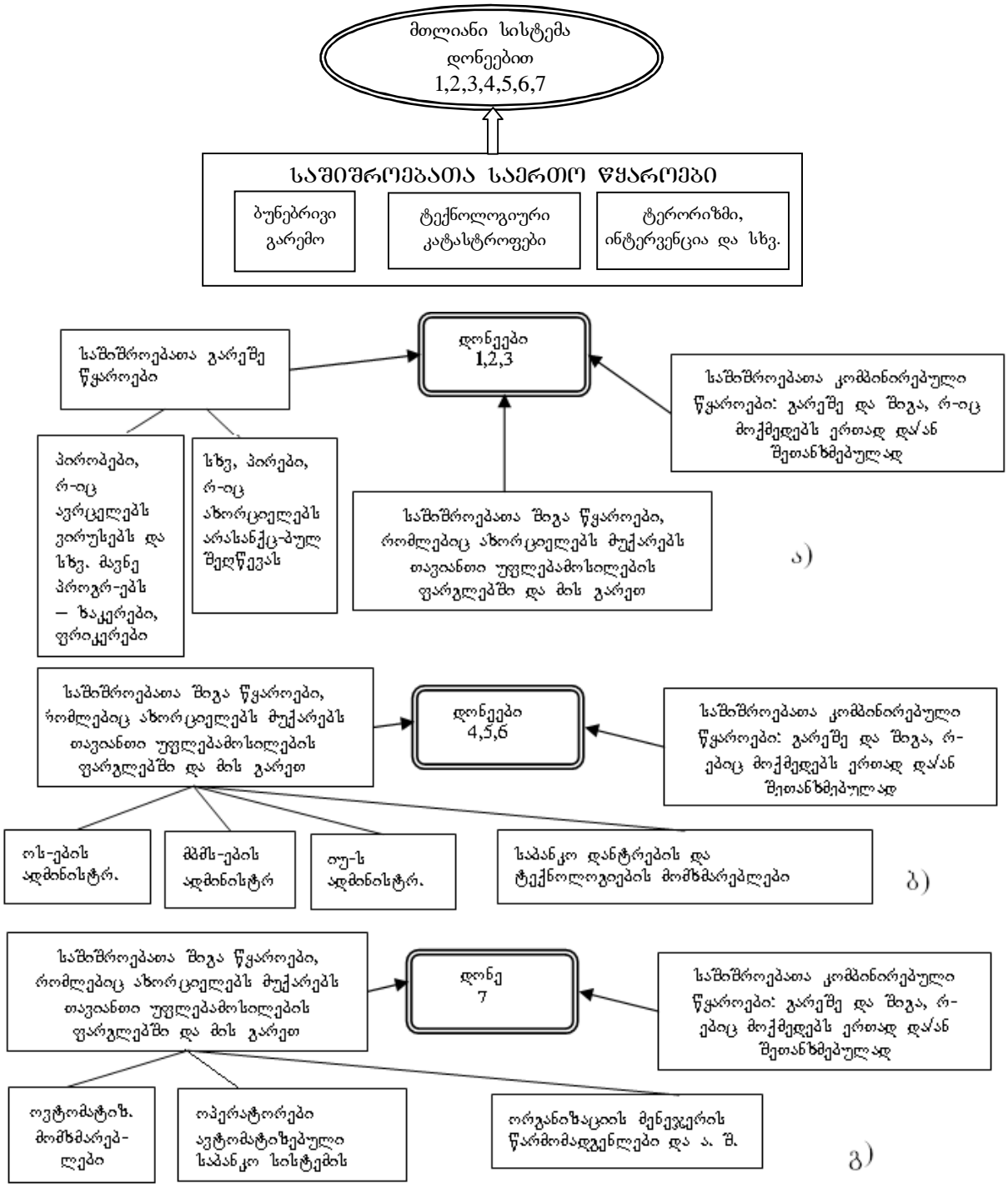
იმისათვის, რომ შეიქმნას ბანკის ან მისი დანაყოფის ეფექტური დაცვა, სწორად განისაზღვროს მრავალფეროვანი ტექნიკური საშუალებების გამოყენების ძირითადი მიმართულებები და მეთოდები, უზრუნველყოფილ იქნას ოპტიმალური თანაფარდობა დაცვის პარამეტრებსა და მის ღირებულებას შორის, აუცილებელია ჩატარდეს საბანკო ობიექტების (ცხადია, ვრცელდება სხვა სახის ობიექტებზეც) ანალიზი შესაძლო მუქარებისაგან მათი მოღვაწეობის დაცვის თვალსაზრისით.

ბანკის საკრედიტო ორგანიზაციის მოღვაწეობა წარიმართება მის შემადგენლობაში შემავალი ინფორმაციული ინფრასტრუქტურის მხარდაჭერით, რომელიც უზრუნველყოფს საბანკო საკრედიტო სისტემის ტექნოლოგიის რეალიზაციას და შეიძლება წარმოდგენილი იქნას მისი ძირითადი დონეების იერარქიის სახით:

- I დონე: ფიზიკური – კავშირის ხაზები, აპარატურული საშუალებები და ა. შ.
- II დონე: ქსელური – ქსელური აპარატურული საშუალებები: მარშუტიზატორები, კომუნიკატორები, კონცენტრატორები და ა. შ.
- III დონე: ქსელური დანართები და სერვისები;

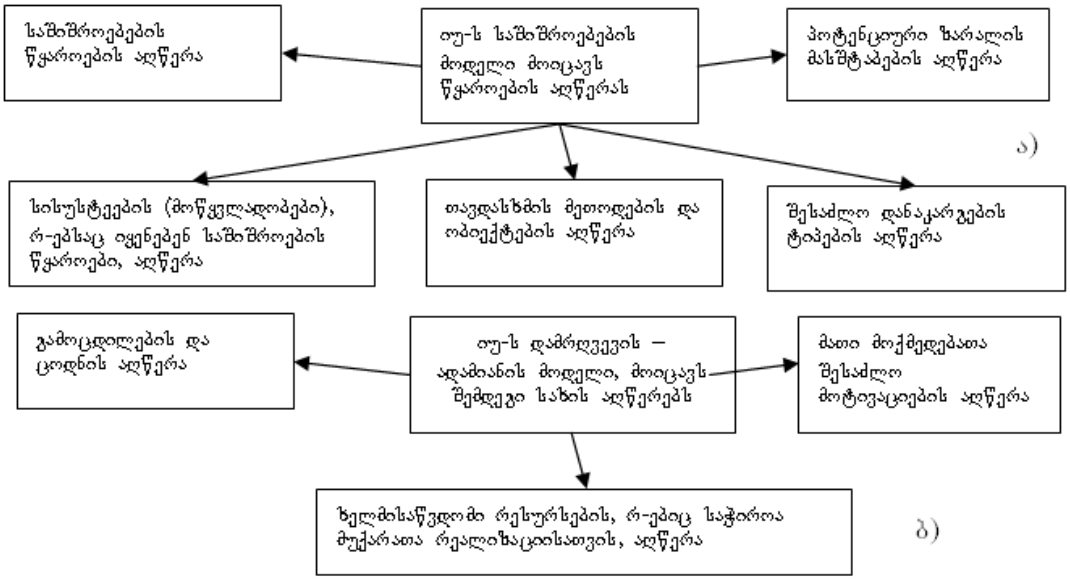
- IV დონე: ოპერაციული სისტემები (ოს);
- V დონე: მონაცემთა ბაზების მართვის სისტემები (მბმს);
- VI დონე: საბანკო ტექნოლოგიური პროცესები და დანართები;
- VII დონე: ორგანიზაციის ბიზნეს-პროცესები.

ცხადია, დაცვის კომპლექსური სისტემის შესაქმნელად პირველ რიგში, უნდა განისაზღვროს თითოეული დონისათვის კონკრეტულად დასაცავი ობიექტები და საშიშროებათა წყაროები. დონეების მიხედვით საშიშროებათა წყაროების შესაძლო კლასიფიკაცია მოცემულია 1-ელ ნახაზზე(ა, ბ, გ):



ნახ. 1

კლასიფიცირებული საშიშროების წყაროები მუქარების რეალიზაციისას იყენებს ობიექტების დაცვის სისტემის სისუსტეებს (მოწყვლადობებს), ამიტომ ინფორმაციული უსაფრთხოების (იუ) პროგნოზი უნდა ემყარებოდეს საშიშროებათა და დამრღვევათა მოდელებს, რომლებიც უნდა წარმოადგენდეს ძირითად ინსტრუმენტებს ორგანიზაციის მენეჯმენტისა და მისი იუ-ს უზრუნველყოფის სისტემის გაშლის, მხარდაჭერისა და სრულყოფისას. ასეთი საჭირო მოდელების კლასიფიკაცია მოცემულია მე-2 ა, ბ ნახაზზე.



ნახ. 2.

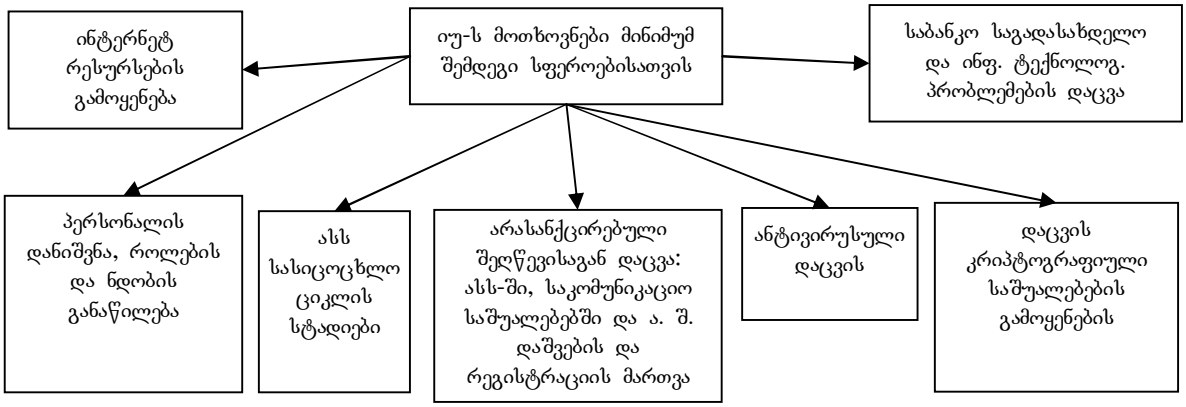
იუ-ს საშიშროების ანალიზისას ამოსავალ წერტილს უნდა წარმოადგენდეს იმის გათვალისწინება, რომ ეს საშიშროებანი უშუალო გავლენას ახდენს ორგანიზაციის მოღვაწეობის ოპერაციულ რისკებზე. ოპერაციული რისკები კი გავლენას ახდენს ორგანიზაციის ბიზნესპროცესებზე [1]. თავის მხრივ ოპერაციულ რისკებზე მოქმედებს შემდეგი საექსპლუატაციო ფაქტორები: ტექნიკური უწესივრობები, ორგანიზაციის პერსონალის, კლიენტების მცდარი და/ან წინასწარგანზრახული ბოროტი მოქმედებები, მათი უშუალო დაშვებისას ავტომატიზებულ საბანკო სისტემასთან (ასს) და სხვა.

საბანკო სისტემის ინფორმაციული უსაფრთხოების ქვეშ ვგულისხმობთ მის დაცულობას ინფორმაციულ სფეროში სხვადასხვა მუქარების პირობებში. დაცულობა კი, პირველ რიგში მიიღწევა ინფორმაციული უსაფრთხოების თვისებათა ერთობლიობის – კონფიდენციალობა, ურღვევობა, ინფორმაციული აქტივების და ინფრასტრუქტურების ხელმისაწვდომობა – უზრუნველყოფით. საამისოდ კი ორგანიზაციას უნდა გააჩნდეს ინფორმაციული უსაფრთხოების პოლიტიკა, რისთვისაც:

- ორგანიზაციის მესაკუთრემ (და/ან მენეჯმენტმა) უნდა უზრუნველყოს სო-ს იუ-ს პოლიტიკის დამუშავება, მიღება და დანერგვა, ამ პოლიტიკის რეალიზაციისათვის საჭირო რესურსების გამოყოფის ჩათვლით;
- პოლიტიკამ უნდა აღწეროს იუ-ს მენეჯმენტის სისტემის მიზნები და ამოცანები და განსაზღვროს წესების ერთობლიობა, მოთხოვნები და სახელმძღვანელო პრინციპები ინფორმაციული უსაფრთხოების სფეროში, რომლებითაც უნდა იხელმძღვანელოს ორგანიზაციამ თავის მოღვაწეობაში;

- უნდა დაინიშნოს პიროვნებები, რომლებიც პასუხს აგებენ იუ-ს პოლიტიკის რეალიზაციაზე და მის აქტიურად მდგომარეობაში შენარჩუნებაზე.

სო-ს იუ-ს პოლიტიკაში განსაზღვრული უნდა იყოს ყველა სფერო, რომლებსაც წაეყენება უსაფრთხოების უზრუნველყოფის საერთო მოთხოვნები (ნახ.3). ეს მოთხოვნები აუცილებლად უნდა იყოს ურთიერთშეთანხმებული და უწყვეტი ამოცანების კომპლექსის, ქვესისტემის, დონეების და სასიცოცხლო ციკლის სტადიების მიხედვით. იუ-ს მოთხოვნები უნდა განსაზღვრავდეს სო-ს მოღვაწეობის შინაარსსა და მიზნების უსაფრთხოების მართვის პროცესის ჩარჩოებში.



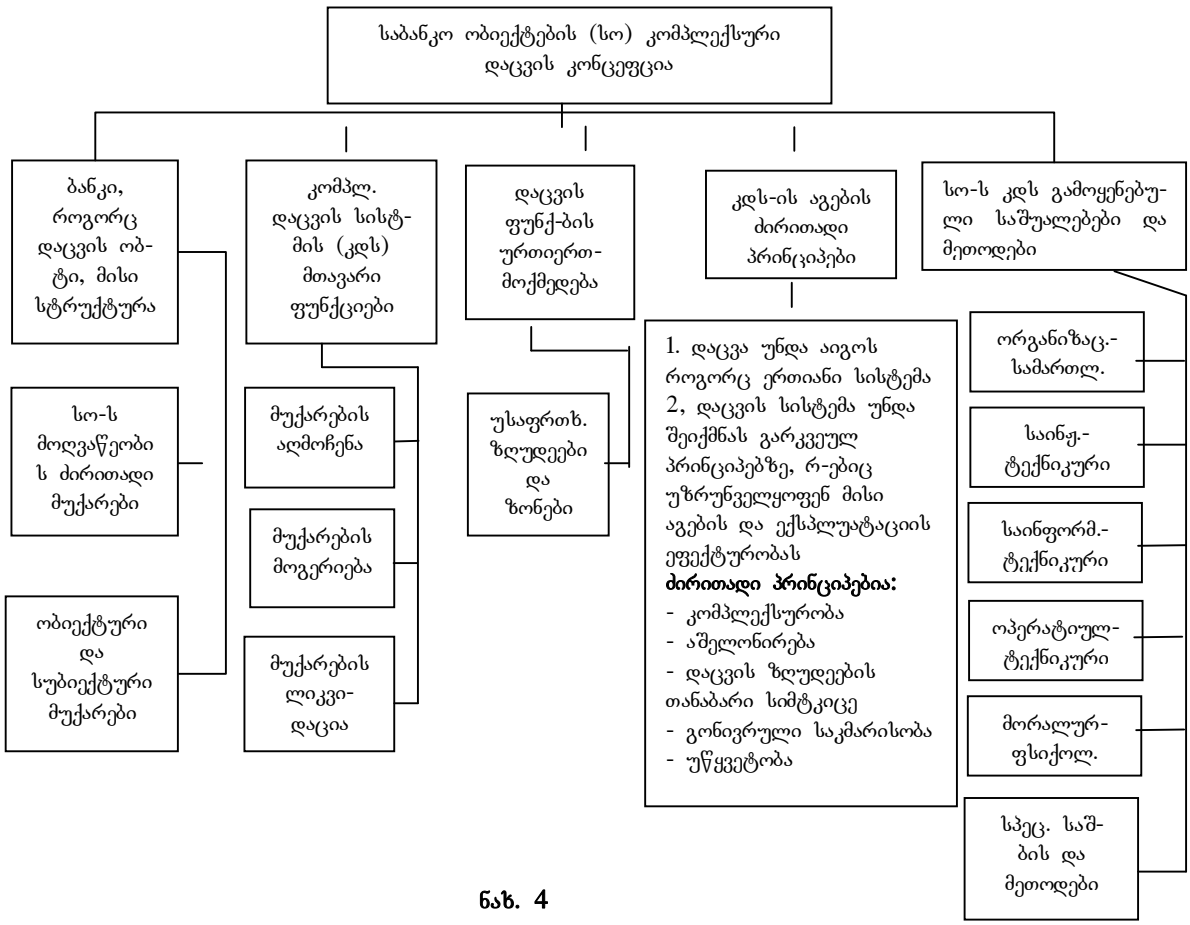
ნახ. 3

მთელ მსოფლიოში ნებისმიერი კომპანიისათვის ინფორმაციული უსაფრთხოება განსაკუთრებით ფასეული და პრიორიტეტული მიმართულებაა, თუმცა ხშირ შემთხვევაში უმაღლეს დონეზე დაცვა უამრავ სიძნელეებთანაა დაკავშირებული. ინფორმაციული უსაფრთხოების დაბალი დონის მიზეზად, პირველ რიგში, შეიძლება დავასახელოთ შემდეგი ფაქტორები [2]: კვალიფიციური სპეციალისტების ნაკლებობა, ამ სფეროს არასაკმარისი დაფინანსება და თავად ორგანიზაციის მიერ იმ რისკების არასათანადოდ გაცნობიერება, რომლებიც ინფორმაციულ უსაფრთხოებასთანაა დაკავშირებული. არსებობს საკმაოდ საინტერესო მონაცემები: იმ დანაკარგების 80%, რომელიც დაკავშირებულია იუ-ს დარღვევასთან, გამოწვეულია თავად კომპანიის თანამშრომელთა მოქმედებით, რომელთა 50% მონაცემთა გადინებას შეგნებულად ახორციელებს. 2006 წელს რუსეთის თითქმის მილიონამდე მოქალაქე დაზარალდა პრივატული ინფორმაციის გადინების შედეგად, ინტელექტუალური საკუთრების საერთაშორისო ალიანსის ცნობით კი ამერიკულ კომპანიებს 2005 წელს ჩინელმა ჰაკერებმა 2,3 მილიარდი აშშ დოლარის ოდენობის ზიანი მიაყენეს. აქვე უნდა აღინიშნოს კომპანიების მხრიდან ინფორმაციული უსაფრთხოების მოთხოვნების და წესების, დაცვის მექანიზმების მიმართ არასათანადო ყურადრების ფაქტები. მაგალითად, შვედურმა ბანკმა „ნორდეამ“ ნახევარ მილიონ ევროზე მეტი დაკარგა იმის გამო, რომ მისმა 250 თანამშრომელმა „ტროიანული“ ვირუსით დასნებოვნებული პროგრამა გადმოტვირთა, ხოლო Society Generale-მა კი თაღლითური ოპერაციების შედეგად 5 მილიარდი ევრო დაკარგა.

იმ შემთხვევაში, როდესაც ორგანიზაციები არ აფასებს იუ-ს დარღვევებთან დაკავშირებულ დანახარჯებს, მათ ასევე არ შეუძლია დაიანგარიშონ, ანაზღაურდება თუ არა ადრე გატარებული დაცვის ზომები. გარდა ამისა არსებობს ორგანიზაციის ირიბი დანახარჯები, რომლებიც

დაკავშირებულია პერსონალის მოცდენასთან და მწარმოებლურობის შემცირებასთან, აგრეთვე კონკრეტული დარღვევების შემდეგ იუ-ს სისტემის სრულყოფასთან (რაც შეიძლება უფრო ძვირი აღმოჩნდეს, ვიდრე იუ-ს სისტემის თავდაპირველი შექმნა). თუ ამას დავუმატებთ რეპუტაციის შელახვას, რაც შეიძლება ორგანიზაციას მიაყენოს იუ-ს სისტემის გარღვევამ, მაშინ ზარალის საერთო მოცულობა შეიძლება იყოს საკმაოდ დიდი.

ამრიგად, სო-ს უზარალოდ ფუნქციონირებისათვის აუცილებლად უნდა გააჩნდეს საბანკო ობიექტების (ფაქტობრივად დაცვას ექვემდებარება ორგანიზაციის ყველა სახის აქტივები) კომპლექსური დაცვის ერთიანი კონცეფცია და ამ კონცეფციაზე აგებული სო-ს დაცვის კომპლექსური სისტემა. აღნიშნული კონცეფციის არსი კარგად ჩანს მე-4 ნახაზზე.



ნახ. 4

იმის გათვალისწინებით, რომ საბანკო სისტემა ნებისმიერი სახელმწიფოსათვის წარმოადგენს განსაკუთრებით მნიშვნელოვან ობიექტს, მიზანშეწონილად მიგვაჩნია განვიხილოთ საქართველოს საბანკო სისტემის უსაფრთხოების უზრუნველყოფის სფეროში არსებული მდგომარეობა. საამისოდ კი შესაძლებელია გამოყენებულ იქნას:

- ორგანიზაციული, სამართლებრივი დოკუმენტები;
- სახელმწიფოში არსებული შესაბამისი სტანდარტები;
- აუდიტების შენიშვნები;
- რამდენადაა გამოყენებული მსოფლიო პრაქტიკის სტანდარტები (მაგალითად: BS 7799/ISO 17799)
- ინციდენტების რაოდენობა უსაფრთხოების სფეროში;
- ინციდენტების შედეგად განცდილი ფინანსური დანახარჯები;
- ინფორმაციულ უსაფრთხოებაზე გაწეული დანახარჯები.

ფაქტია, რომ დღეისათვის საქართველოს საბანკო სისტემაში იუ-ს ინციდენტების შესახებ რაიმე სერიოზული, საზოგადოებისათვის ხელმისაწვდომი ინფორმაცია არ არსებობს. ვფიქრობთ, რომ საქართველოში მსგავსი ინციდენტები ჯერჯერობით ან არ მომხდარა, ან არ გახმაურებულა. თუმცა იმის გათვალისწინებით, რომ საქართველოში ინფორმაციული ტექნოლოგიების (იტ) დანერგვა–განვითარებას არ მიუღია ისეთი მასშტაბები, როგორც ესაა თუნდაც საშუალო განვითარების სახელმწიფოებში, რაზეც მეტყველებს ის ფაქტი, რომ Economist Intelligence Unit-ის მიერ გამოქვეყნებულ მსოფლიოს ქვეყნების ,,ელექტრონული მზადყოფნის" რეიტინგში საქართველო მსოფლიოს 70-ქვეყნებშიც კი ვერ მოხვდა შესაბამისად ამ სფეროში დანაშაულებრივ, კანონსაწინააღმდეგო ქმედებებს არ მიუღია აღნიშნულ ქვეყნებში არსებული მასშტაბები. მაგრამ ეს სრულებით არ იძლევა დამშვიდების საბაბს, რაც ნათლად გამოჩნდა 2008 წლის აგვისტოს თვეში რუსეთის სამხედრო- და კიბერაგრესიისას. მართალია, ეროვნული ბანკის განკარგულებით ქვეყნის საბანკო სისტემამ უარი თქვა კლიენტების დისტანციურ მომსახურებაზე და ინტერნეტ რესურსების გამოყენებაზე და ამით თავიდან იქნა აცილებული შესაძლო ფართო მასშტაბის ზარალი, მაგრამ საქართველო, ისევე როგორც ნებისმიერი სახელმწიფო, ვერ იქნება ჩაკეტილი ქვეყანა, ევროსახელმწიფოებისაკენ სწრაფვის, ეკონომიკური აღამავლობის და ქვეყნის მთლიანობის აღდგენის პირობებში, უნდა ველოდოთ ინფორმაციული ტექნოლოგიების კიდევ უფრო მეტი ინტენსივობით დანერგვას საზოგადოებრივი ცხოვრების ნებისმიერ სფეროში, რომ არაფერი ვთქვათ ისეთ სწრაფად პროგრესირებად ორგანიზაციებზე, როგორებიცაა ბანკები, საკრედიტო ორგანიზაციები. პოსტსაბჭოთა სივრცის სახელმწიფოების გამოცდილება გვიჩვენებს, რომ მაგალითად, ქვეყანაში პლასტიკური ბარათების დანერგვის მომენტიდან ორი წლის განმავლობაში ამ სფეროში დანაშაულობათა დონე ფაქტობრივად რჩება ნულის ტოლი, ხოლო შემდეგ სწრაფად იზრდება 0,7-0,8 %-მდე (ესაა თაღლითობით საგადასახადო სისტემის დანაკარგების შეფარდება ბარათების ბრუნვით მიღებულ შემოსავალთან) და გარკვეული დროის განმავლობაში რჩება ამ დონეზე [3]. ასეთი მკვეთრი ზრდა განპირობებულია, პირველ რიგში, თანამედროვე იტ-ს ფართოდ დანერგვით და ბაზრის განვითარებით.

ამრიგად, ინფორმაციული უსაფრთხოების უზრუნველყოფის სფეროში გაჩერება ძალზე საშიშია, ამიტომ თანამედროვე იტ-ს დანერგვასთან ერთად უნდა იხვეწებოდეს დაცვის ტექნოლოგიებიც. ეს გარემოება, მოყვანილი კრიტერიუმების მიხედვით, საქართველოს საბანკო სისტემის ორგანიზაციული სამართლებრივ დოკუმენტებში აუცილებლად უნდა იყოს ასახული. ყოველი საბანკო ინსტრუქცია ან ნორმატიულ-სამართლებრივი დოკუმენტი პირდაპირ თუ ირიბად უნდა ითვალისწინებდეს უსაფრთხოების საკითხებს და გავლენას ახდენდეს ბანკის კომპლექსური დაცვის სისტემის მუშაობისუნარიანობასა და ეფექტურობაზე.

ჩვენ შევეცდებით ამ კუთხით გავაანალიზოთ ხელმისაწვდომი სამართლებრივი დოკუმენტები მაინც.

საქართველოს ორგანულ კანონში „საქართველოს ეროვნული ბანკის შესახებ“ ფაქტობრივად არაფერია ნათქვამი ნებისმიერი ტიპის საბანკო საქმიანობის, ოპერაციების უსაფრთხოების უზრუნველყოფის შესახებ, თუ არ ჩაითვლება „მუხლი-18: საიდუმლოება და ინტერესთა შეუთავსებლობა“ და "მუხლი-67: მარეგლამენტირებელი დებულებები“, რომლებშიც მითითებულია, რომ ეროვნული ბანკის, სააგენტოსა და სამსახურის არც ერთ ნებისმიერი რანგის თანამშრომელს ან აუდიტორს არა აქვს არაუფლებამოსილი პირის კონფიდენციალურ ინფორმაციასთან დაშვების უფლება, უფლება – გათქვას ან გაავრცელოს ასეთი უფლება. მაგრამ არაფერია თქმული საბანკო აქტივების უსაფრთხოების უზრუნველყოფის მეთოდებსა და საშუალებებზე. ასევე არაფერია თქმული ელექტრონულ ანგარიშსწორებისას იუ-ს უზრუნველყოფაზე, მხოლოდ გაკვრითაა მინიშნული, რომ კომერციულ ბანკსა და არასაბანკო სადეპოზიტო დაწესებულებებს გადაეცემათ იუ-ს საკითხებში ფორმატები და სტანდარტები, მაგრამ არაა მითითებული თუ რა სტანდარტებზე და ფორმატებზეა საუბარი, ან რა მოთხოვნებს უნდა აკმაყოფილებდეს იუ-ს სფეროში როგორც ეროვნული ბანკი, ასევე მის კონტროლს ქვეშ მყოფი კომერციული ბანკები და არასაკრედიტო სადეპოზიტო დაწესებულებები.

რაც შეეხება საქართველოს კანონს „კომერციული ბანკების საქმიანობის შესახებ“, მასში ერთ-ერთი უმთავრესი საკითხია საბანკო საქმიანობის ლიცენზიის გაცემის პირობები (მუხლები 3, 5, 6), რომლებშიც საერთოდ არაა დაფიქსირებული თუ რა პირობებს უნდა აკმაყოფილებდეს საბანკო საქმიანობის მთხოვნელი უსაფრთხოების უზრუნველყოფის მიმართულებით. ამ კანონშიც მხოლოდ ერთი „მუხლი-17“ ეხება საბანკო საიდუმლოების დაცვის საკითხს და არაფერია თქმული თუ როგორ, რა მეთოდებით და საშუალებებით, რა სტანდარტების და ნორმატიული დოკუმენტების მიხედვით უნდა იყოს დარეგულირებული საბანკო საქმიანობის უსაფრთხოება. ასევე საბანკო დაწესებულების კლიენტების ბანკთან ურთიერთობების უსაფრთხოება. არაა განსაზღვრული თუ რა პირობებს უნდა აკმაყოფილებდეს კომერციული ბანკის ფილიალები აქტივების უსაფრთხოების უზრუნველყოფის თვალსაზრისით.

უნდა აღვნიშნოთ, რომ ერთ-ერთი უმთავრესი ამოცანა, რომელსაც წყვეტს აუდიტორი იტ-ს სფეროში, ესაა კლიენტების ინფორმაციული რესურსების დაცულობის დონის შეფასება. ამ მიმართულებით სამუშაოებმა განსაკუთრებული აქტუალობა შეიძინა აშშ-ს 2001 წლის 11 სექტემბერს მომხდარი ტრაგიკული მოვლენების შემდეგ.

უნდა დავეთანხმოთ იმ ექსპერტების მოსაზრებას, რომლებიც თვლიან, რომ მთელს მსოფლიოში ინფორმაციული უსაფრთხოების განვითარება მიმდინარეობს ძალიან მსგავსი გზით, თანაც ტენდენციები, რომლებიც უკვე გამოჩნდნენ მსოფლიოს წამყვან ქვეყნებში, აუცილებლად, ხვად დიდი ალბათობით თავს იჩენს სხვა ნებისმიერ ქვეყანაში. ამდენად, განვითარებადმა ქვეყნებმა, რომელთა რიცხვს საქართველოც მიეკუთვნება, უნდა მოახერხონ ისწავლონ სხვის შეცდომებზე [2]. მაგრამ სამწუხაროდ ჩვენს მიერ გაანალიზებული საქართველოში მოქმედი ნორმატიული

დოკუმენტები, რომლებიც ეხებიან საბანკო სისტემის საქმიანობას, ამ სურვილის დასტურად ვერ გამოდგებიან.

„საქართველოში უნაღდო ანგარიშსწორების წესები“ მუხლი 4.1. ა) პუნქტის თანახმად „ბანკში საგადახდო დავალების ელექტრონული შეტყობილნებების სახით წარდგენა (ან მისი გამოსახულების გადაცემა) ხდება საგადახდო საბუთების ელექტრონული გაცვლის შესახებ ელექტრონული სისტემების, პროგრამულ-კრიპტოგრაფიული დაცვების და ელექტრონულ-ციფრული ხელმოწერების თაობაზე ბანკსა და კლიენტს შორის გაფორმებული ხელშეკრულების საფუძველზე“, შეუძლებელია დღეს საქართველოში კლიენტების უმეტესობას აღნიშნულ ამონაწერში ნახსენებ დაცვის საშუალებაზე მიახლოებითი წარმოდგენა მაინც ჰქონდეთ, რომ არაფერი ვთქვათ მათ გააზრებულ ცოდნაზე. თუ ამასაც დავუმატებთ, რომ საქართველოში კანონიც კი არ არსებობს ელექტრონული ხელმოწერის შესახებ, და თანაც უცნობია უნაღდო ანგარიშსწორებისას საგადხო დავალების ელექტრონული წარდგენის პროცესის დაცვის საქართველოში რეალურად მომქმედი ეროვნული ან საერთაშორისო სტანდარტები, ადვილი წარმოსადგენია თუ რა შანსი აქვთ საქართველოში მომქმედ საკრედიტო ორგანიზაციებს მასობრივად მოიზიდონ კლიენტები ელექტრონული კომერციის ამ და სხვა სფეროებში.

ამ წესში ასევე არაა განსაზღვრული რა დაცვის მექანიზმები უნდა არსებობდეს მონაცემთა ერთიანი ბაზების უსაფრთხოების უზრუნველსაყოფად ელექტრონულ საგადასახადო საბუთებზე წვდომისას. გაუგებარია წვდომისას თუ რა მოქმედებები შეიძლება განხორციელდეს ელექტრონულ საგადასახადო საბუთზე, დამუშავება კი სრულებით არ ნიშნავს მის შესრულებას, აქ ეს ორი ტერმინი გაიგივებულია და გაუგებრობას იწვევს. შეიძლება კლიენტი ვერც მიხვდეს, რომ ფაქტიურად მითითება კეთდება საგადახდო საბუთის შაბლონზე, რომელითაც პერსონალს მომავალში შეუძლია შექმნას სხვადასხვა საბუთი და უწყისი.

წარმოდგენილ წესში მინიშნებაც კი არა გაკეტებული, თუ როგორ, რა მეთოდებით და საშუალებებით, რა წესით, ან რა კონკრეტულ ნორმატიულ დოკუმენტზე დაყრდნობით უნდა ხდებოდეს ელექატრონული საგადახდო საბუთების დაცვა გაყალბებისაგან ან სხვა არასანქცირებული ზემოქმედებებისაგან [4].

დებულებაში „საბანკო პლასტიკური ბარათების შესახებ“ [5], არაფერია თქმული გაყალბებული ბარათების გამოყენების შესაძლებლობაზე, არაა განსაზღვრული, თუ ვის რა პასუხისმგებლობა ეკისრება თუ აღმოჩნდება, რომ გაყალბებული ბარათის გამო ზარალი განიცადა ნამდვილი ბარათის მფლობელმა – კლიენტმა.

ინფორმაციული უსაფრთხოების თვალსაზრისით ვერც დებულება „საქართველოს საბანკო სისტემაში ელექტრონული საქმიანობის შესახებ“ გამოირჩევა დამაჯერებლობით, კონკრეტულობით [6]. მაგალითად, „მუხლი 4: სტანდარტიზაცია“ საერთოდ არ ჩანს თუ რა სტანდარტებზე ხდება მითითება, გაუგებარია რას ნიშნავს ამავე მუხლის მე-4 პუნქტში მოყვანილი დებულება, რომ

ელექტრონული ინფორმაციის გაცვლისას გამოყენებული შეტყობინებები უნდა შეიცავდეს ისეთ ელემენტებს (რეკვიზიტებს), რომლებიც მას ანიჭებს სამართლებრივ სტატუსს.

სრულიად არაფრის მთქმელია „მუხლი 6. ინფორმაციის დაცვის უზრუნველყოფა“-ში გაკეთებული მითითება – ინფორმაციის დაცვის პოლიტიკას განსაზღვრავს სისტემის ორგანიზატორი. ხოლო „მუხლი 7. ელექტრონული ინფორმაციის შენახვა და განადგურება“-ში არაა მითითებული, რა პერიოდულობით და რაზე დამოკიდებულებით უნდა ხდებოდეს ელექტრონული ინფორმაციის ასლის გადაღება, რამდენად დაშორებულ საცავებში უნდა ინახებოდეს ასლები, რა პირობებში უნდა ინახებოდეს ისინი, ვინ აგებს პასუხს მათ დაცვაზე და ა. შ.

ვფიქრობთ, რომ არაა სწორი, როდესაც ამ დებულების მე-8 მუხლით („შეთანხმება სისტემის ორგანიზატორსა და მომხმარებელს შორის ელექტრონული მომსახურების (საქმიანობის) შესახებ") დაფიქსირებულ ხელშეკრულების შემადგენლობაში ფაქტიურად არ ფიგურირებს ელექტრონული საქმის წარმოების უსაფრთხოების უზრუნველყოფის საკითხი, თუ არ ჩავთვლით იმავე მუხლის 4 პუნქტში მოხსენიებულ მომხმარებლისა და მესაკუთრის იდენტიფიკაციის საშუალებებს.

ძალზე ზოგადია, ელექტრონული საქმისწარმოების უსაფრთხოების თვალსაზრისით, სისტემის ორგანიზატორის პასუხისმგებლობის საფუძვლები – ვალდებულებების შეუსრულებლობის მიზეზები, გარდა ტექნიკური საშუალებებისა შეიძლება იყოს პერსონალის მხრიდან უსაფრთხოების წესების არ ცოდნა, რეალური მუქარების და სისტემის დაცულობის შეუფასებლობა და ა. შ. კონკრეტულობა და დამაჯერებლობა აკლია მე-11 მუხლში მოცემულ მოთხოვნებსაც. არ ჩანს, თუ რა ვალდებულებები აკისრია სისტემის მომხმარებელს მისი უსაფრთხოების უზრუნველყოფის მხრივ, ვინაიდან, როგორც ვნახერთ, ეს საკითხი არც მე-8 მუხლის მე-4 პუნქტშია დასმული. იგივე შეიძლება ითქვას მე-13 მუხლზეც. აქ ალბათ სწორი იქნებოდა დაფიქსირებული ყოფილიყო ელექტრონული ინფორმაციის გარანტირებული გაცვლის მექანიზმები, ხოლო რაც შეეხება მე-14 მუხლს, არც აქაა დაფიქსირებული მექანიზმი, რომელიც საშუალებას მისცემდა გადამხდელს შეტყობინების უკან გამოთხოვისა. კერძოდ, თუ შეტყობინება გამოთხოვადია, მასში დათქმული უნდა იყოს შეტყობინების შესრულებამდე რაღაც მინიმალური დრო, რომლის განმავლობაშიც, გადამხდელს ეცოდინება, რომ შეძლებს მის გამოთხოვას.

ჩატარებული ანალიზი მიგვანიშნებს იმაზე, რომ აუცილებელია დაუყოვნებლივ მოხდეს საქართველოს საბანკო სისტემის (და არა მარტო) უსაფრთხოების უზრუნველყოფის სფეროში არსებული მდგომარების დეტალური შესწავლა და შეიქმნას, მსოფლიოს წამყვანი ქვეყნების გამოცდილების გათვალისწინებით და შესაბამისი სპეციალისტების გამოყენებით, საბანკო სისტემის უსაფრთხოების ზოგადი კონცეფცია. ელექტრონულ ინფორმაციასთან დაკავშირებით, აუცილებელია ასევე მიღებული იქნას კანონი (ან კანონები) კრიპტოგრაფიული სისტემების შესახებ, ბიომეტრიული მახასიათებლების გამოყენების შესახებ, ელექტრონული არქივების შესახებ, ინფორმაციულ უსაფრთხოებასთან დაკავშირებული მარეგულირებელი ნორმატიული აქტები.

ყველაფერი ამის განსასაზღვრავად, სტრატეგიის დასამუშავებლად და მის განსახორციელებლად უნდა არსებობდეს (საიმისოდ შეგვიძლია ვისარგებლოთ სხვა ქვეყნების მდიდარი გამოცდილებით) რაიმე კომისია ან კომიტეტი, რომელსაც სახელმწიფოს დონეზე ექნება დავალებული აღნიშნული პრობლემების ორგანიზება და კოორდინაცია.

3. დასკვნა

საბანკო სისტემის უსაფრთხოების უზრუნველყოფის პროცესში არ არსებობს მეორეხარისხოვანი საკითხები, ნებისმიერი ფაქტორი, რომელსაც შეუძლია რაიმე გავლენა იქონიოს ორგანიზაციის უსაფრთხოდ ფუნქციონირებაზე, გათვალისწინებული უნდა იყოს უსაფრთხოების საერთო პოლიტიკის განსაზღვრისას და დაცვის კომპლექსური სისტემის აგების დროს. საბანკო სისტემის უსაფრთხოების ძირითად პრინციპებზე დაყრდნობით გაანალიზებულ იქნა საქართველოს საბანკო სისტემის შესახებ სხვადასხვა ნორმატიული დოკუმენტები და გამომუშავებულ იქნას რეკომენდაციები, რომელთა რეალიზაციამ, საქართველოში ინფორმაციული ტექნოლოგიების სულ უფრო ფართო მასშტაბით დანერგვის პირობებში, შეიძლება ხელი შეუწყოს საქართველოს საბანკო სისტემის უსაფრთხოების უზრუნველყოფის გაუმჯობესებას.

ლიტერატურა

1. Банковские риски: учебное пособие. Под ред. О. И. Лаврушина и Н. И. Валенцевой – 2-е изд., стер. – М.: КНОРУС, 2008
2. Аудит информационной безопасности: глобальное исследование КПРМГ. – http://goap.ru.
3. Безопасность, криминалистика, промышленный шпионаж, разное – http://www.phreaking.ru/razdeldisplay.php?razdelid=239
4. საქართველოში უნაღდო ანგარიშსწორების წესები. საქ.ეროვნ.ბანკი. ბრძ.-№166 26.06.2007
5. დებულება „საბანკო პლასტიკური ბარათების შესახებ“ – დამტკიცებულია საქართველოს ეროვნული ბანკის პრეზიდენტი 2007 წ. 26. 06. №166 ბრძანებით
6. დებულება „საქართველოს საბანკო სისტემაში ელექტრონული საქმიანობის შესახებ“ – დამტკიცებულია საქართველოს ეროვნული ბანკის პრეზიდენტი 2003 წ. 12. 07. №135 ბრძანებით.

MAIN PRINCIPLES OF SECURITY INFORMATIONAL SAFETY OF BANK SYSTEM

Shonia Otar, Shonia Akaki, Odisharia Korneli, Tsomaia Nino
Georgian Technical University

Summary

The article concerns to all levels of danger sources of bank system information structures, basic needs of protection against them and formulated conception of complex safety for the bank objects as well. Here is done the analysis of an existing situation of the information safety in the Georgian bank system nowadays.

ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ СИСТЕМЫ

Шония О., Шония А., Одишария К., Цомая Н.
Грузинский Технический Университет

Резюме

Детально рассмотрены источники опасности всех уровней информационной инфраструктуры банковской системы, представлены основные требования защиты от них, сформулирована концепция комплексной защиты банковских объектов. Представлен анализ существующей ситуации с точки зрения информационной безопасности в банковской системе Грузии.