



აუჯანყიანობის აუდიტის ანგარიში



სახელმწიფო აუდიტის სამსახური

„პაპტიკიკა“

ინფორმაციული ტექნოლოგიების აუდიტისა
და ადმინისტრირების დეპარტამენტის უფროსი
გიორგი გაჩეჩილაძე

„13“ სექტემბერი 2018 წელი

N 61/36

გვ: N: 2

სოციალურად დაუცველი
ოჯახებისათვის საარსებო შემწეობის
ადმინისტრირების ინფორმაციული
სისტემების ეფექტიანობის აუდიტი

სარჩევი

სარჩევი	2
გამოყენებული ტერმინები	4
შემაჯამებელი მიმოხილვა.....	6
რეკომენდაციები.....	8
1. შესავალი	10
1.1 აუდიტის მოტივაცია	10
1.2 აუდიტის მიზანი და მთავარი კითხვები.....	14
1.3 აუდიტის მასშტაბი	14
1.3.1 აუდიტის მასშტაბის შეზღუდვა	15
1.4 კრიტერიუმები.....	16
1.5 ზოგადი ინფორმაცია.....	17
1.5.1 განმახორციელებელი ერთეულები.....	17
1.5.2 საარსებო შემწეობის გაცემის ბიზნესპროცესი	18
2. აუდიტის მიგნებები.....	26
2.1 ბენეფიციარების შესახებ ინფორმაციის ვალიდაციის პროცესში არსებული ნაკლოვანებები.....	26
2.1.1 უძრავი ქონებისა და სასოფლო-სამეურნეო მიწის შესახებ ინფორმაციის ვალიდაცია	26
2.1.2 ბუნებრივი აირის მოხმარების შესახებ ინფორმაციის ვალიდაცია	27
2.1.3 განათლების დონის მაჩვენებლის გავლენა სარეიტინგო ქულაზე	30
2.2 ასაკის მაჩვენებლის გავლენა სარეიტინგო ქულაზე	32
დასკვნა.....	33
რეკომენდაცია	35
2.3 ინფორმაციულ უსაფრთხოებასთან დაკავშირებული ნაკლოვანებები.....	36
2.3.1 სააგენტოს სისტემაზე ლოგიკური წვდომის კონტროლებთან დაკავშირებული ხარვეზები	37
2.3.1.1 სააგენტოს თანამშრომლებს აქვთ მოვალეობის შესრულებისათვის საჭიროზე მეტი ინფორმაციაზე დაშვება	39
2.3.1.2 ლოგირებასა და მიკვლევადობასთან დაკავშირებული ხარვეზები.....	40
2.3.1.3 აპლიკაციის მომხმარებელთა მართვასთან და პერსონიფიცირებული მომხმარებლის არსებობასთან დაკავშირებული ხარვეზები	42

2.3.1.4 წვდომის კონტროლების სისტემა - სააგენტოში არ არსებობს მოთხოვნები პაროლების სირთულეზე.....	45
2.3.1.5 სისტემის არქიტექტურასთან დაკავშირებული რისკები.....	45
2.3.2 ოპერაციული სისტემებისა და მონაცემთა ბაზების მართვის სისტემის მოწყვლადობის ტესტირება	47
2.3.3 სააგენტოს არ აქვს შემუშავებული ინფორმაციული უსაფრთხოების მართვის სისტემა.....	51
2.3.4 ტერიტორიულ ერთეულებში საბოლოო მომხმარებლის სკანირების შედეგად გამოვლენილი ხარვეზები	53
დასკვნა.....	55
რეკომენდაცია.....	56
2.4 სააგენტოს მიერ შემუშავებული მექანიზმები ვერ უზრუნველყოფს ბენეფიციარებზე თანხის გადარიცხვის ეფექტიან/ადეკვატურ პროცესს.....	57
დასკვნა.....	59
რეკომენდაცია.....	60
დანართი N1 : გამოყენებული მეთოდოლოგია.....	61
ბიბლიოგრაფია	64
კანონები	64
ბრძანებები.....	64
პუბლიკაციები/დოკუმენტები	64

გამოყენებული ტერმინები

ადმინისტრირება – ადმინისტრირება ანგარიშის მიზნებისათვის გულისხმობს საარსებო შემწეობის მართვას: საარსებო შემწეობის მაძიებელი ოჯახებისათვის საარსებო შემწეობის დანიშვნას, გაცემას, შეწყვეტას, გაანგარიშებას, შეჩერებას, აღდგენასა და საარსებო შემწეობის მიღებასთან დაკავშირებული სხვა საკითხების გადაწყვეტას.

აპლიკაცია – კონკრეტული მიზნის განხორციელებისათვის შემუშავებული პროგრამული უზრუნველყოფა, რომელიც გამოიყენება მონაცემთა დამუშავების, ტრანზაქციის შესრულების, ჩანაწერების წარმოებისა და ანგარიშგებისათვის. წინამდებარე ანგარიშის მიზნებისათვის აპლიკაცია წარმოადგენს საარსებო შემწეობის ადმინისტრირების პროცესში გამოყენებულ ინფორმაციულ სისტემებს, კერძოდ, SAESA, SAESA2005 და SSA - დამატება.

ბენეფიციარი – საარსებო შემწეობის მიმღები.

ბიზნესპროცესი – ერთმანეთთან დაკავშირებული საქმიანობების ან ამოცანების სტრუქტურირებული ერთობლიობა, რომლის შედეგად იქმნება გარკვეული პროდუქტი ან მომსახურება მომხმარებლისათვის, ან მომხმარებელთა ჯგუფისათვის.

დეკლარაცია – სპეციალური ფორმის დოკუმენტი, რომელიც შეიცავს მონაცემებს ოჯახის შემადგენლობაში მყოფი წევრების, ოჯახის შემოსავლებისა და გაწეული ხარჯების შესახებ, აგრეთვე მონაცემებს, რომლებიც ასახავს ოჯახის ფაქტობრივ სოციალურ-ეკონომიკურ მდგომარეობას და საჭიროა ოჯახის სარეიტინგო ქულის დასადგენად.

ვალიდაცია - მესამე მხარისაგან მიღებულ ინფორმაციაზე დაყრდნობით იმის დამოწმება, რომ ოჯახის მიერ ოჯახის დეკლარაციაში ასახული მონაცემები რელევანტური და ზუსტია.

ინფორმაციული სისტემა – ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადაწყვეტილების მიღებას. ინფორმაციული სისტემა მოიცავს აპარატურულ და პროგრამულ უზრუნველყოფას, მონაცემებს, ხალხს, პროცესებსა და მათ ურთიერთკავშირს.

მაძიებელი – მონაცემთა ბაზაში რეგისტრაციის მსურველი ოჯახი, რომელიც შეიძლება გახდეს სოციალური დახმარების მიმღები.

მეთოდოლოგია – „სოციალურად დაუცველი ოჯახების (შინამეურნეობების) სოციალურ - ეკონომიკური მდგომარეობის შეფასების მეთოდოლოგიის დამტკიცების შესახებ“ საქართველოს მთავრობის 2014 წლის 31 დეკემბრის N758 დადგენილებით დამტკიცებული მეთოდოლოგია.

სააგენტო – საჯარო სამართლის იურიდიული პირი - სოციალური მომსახურების სააგენტო.

სამინისტრო – საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო.

სარეიტინგო ქულა – პირობითი ერთეული, რომელიც მონაცემთა ბაზაში რეგისტრირებული ოჯახის სოციალურ - ეკონომიკური მდგომარეობის მაჩვენებელია.

სოციალური აგენტი – სპეციალური უფლებამოსილებით აღჭურვილი პირი, რომელიც ახორციელებს მაძიებელი ოჯახის იდენტიფიკაციასა და სოციალურ-ეკონომიკური მდგომარეობის აღწერას.

სოციალურ-ეკონომიკური მდგომარეობა – სააგენტოს უფლებამოსილი პირის მიერ ჩატარებული ვიზუალური დათვალიერებისა და გამოკითხვის (ინტერვიუების) შედეგად დაფიქსირებული მონაცემებისა და ფაქტების ერთობლიობა.

შემაჯამებელი მიმოხილვა

საზოგადოებრივი კეთილდღეობის მისაღწევად სახელმწიფო მნიშვნელოვან როლს ასრულებს საზოგადოებისათვის საბაზისო სოციალური დაცვის სისტემის შექმნისა და შესაბამისი სერვისით უზრუნველყოფის თვალსაზრისით¹. აღნიშნული მიმართულებით 2006 წლიდან მიმდინარეობს საარსებო შემწეობის პროგრამა. პროგრამის მიზანია, მიზნობრივი სოციალური ჯგუფებისთვის საარსებო მინიმუმის გაცემით, ქვეყანაში სიღარიბის უკიდურესი ფორმების აღმოფხვრა და სოციალური რისკების შემცირება.

საარსებო შემწეობის დანიშვნისა და გაცემის პროცესი მნიშვნელოვანწილად ეყრდნობა საარსებო შემწეობის პროგრამის მართვის ინფორმაციულ სისტემებს. შესაბამისად, სახელმწიფო აუდიტის სამსახურმა შეაფასა საარსებო შემწეობის გაცემის ბიზნესპროცესის ეფექტიანობა, მასში გამოყენებული ინფორმაციული სისტემების კონტროლის მექანიზმები და ინფორმაციული უსაფრთხოების საკითხები.

საარსებო შემწეობის პროგრამის ეფექტიანობის აუდიტის შედეგად გამოვლინდა რიგი ნაკლოვანებები, რომელიც გავლენას ახდენს პროგრამის ეფექტიან მართვაზე:

სააგენტოს არ გააჩნია საარსებო შემწეობის მაძიებელთა სარეიტინგო ქულის გამოთვლისათვის საჭირო ზოგიერთი ცვლადის ვალიდაციის ქმედითი მექანიზმი. ასევე არ ხდება დროთა განმავლობაში ზოგიერთი ცვლადის ავტომატური განახლება, კერძოდ:

- › სააგენტო ვერ ახორციელებს ბუნებრივი აირის მოხმარებისა და განათლების დონის მაჩვენებლების ვალიდაციას. აღნიშნული ერთი მხრივ, დაკავშირებულია იმასთან, რომ სააგენტოს არ აქვს გაფორმებული ხელშეკრულებები/მემორანდუმები შესაბამის უწყებებთან და მეორე მხრივ, ქვეყნის დონეზე სრულყოფილი მონაცემების არარსებობასთან. შესაბამისად, აღნიშნული გარემოება გავლენას ახდენს და რისკის ქვეშ აყენებს მაძიებელთათვის შესაბამისი ადეკვატური ქულის გამოთვლის

¹ საქართველოს სოციალურ-ეკონომიკური განვითარების სტრატეგია, საქართველო 2020.

პროცესს და არათანაბარ პირობებში აყენებს საარსებო შემწეობის
მაძიებლებს;

- › სააგენტოს მიერ არ ხორციელდება სარეიტინგო ქულის გამოთვლის
პროცესში გათვალისწინებული ერთ-ერთი მნიშვნელოვანი კომპონენტის,
ბენეფიციარის ასაკის განახლება აპლიკაციაში. კერძოდ, დროთა
განმავლობაში კონკრეტული ბენეფიციარის ასაკის ცვლილებასთან ერთად,
აპლიკაციაში ასახული ასაკი ავტომატურად არ იცვლება. ზემოხსენებულ
გარემოებას გავლენა აქვს ოჯახის სარეიტინგო ქულასა და შესაბამისად,
საარსებო შემწეობის ოდენობის განსაზღვრაზე. აღნიშნული გარემოება
ზრდის საბიუჯეტო რესურსების ადეკვატური ხარჯვის რისკს.

სააგენტო სათანადოდ ვერ უზრუნველყოფს ინფორმაციული უსაფრთხოების
საკანონმდებლო ნორმების შესრულებას. სააგენტო, როგორც კრიტიკული
ინფორმაციული სისტემის სუბიექტი, არსებული საკანონმდებლო ვალდებულების
მიუხედავად, სათანადოდ ვერ უზრუნველყოფს ინფორმაციული უსაფრთხოების
მინიმალური მოთხოვნების შესრულებას და რისკის ქვეშ აყენებს საქართველოს
მოქალაქეთა შესახებ არსებული ინფორმაციის კონფიდენციალურობასა და
მთლიანობას. კერძოდ, არ არის შემუშავებული შესაბამისი პოლიტიკები და
პროცედურები წვდომისა და პრივილეგიების განსაზღვრისათვის, რაც იწვევს
თანამშრომელთა არავტორიზებული დაშვების შესაძლებლობას მოქალაქეთა
კონფიდენციალურ ინფორმაციაზე. აღნიშნული მიგნება საყურადღებოა, ვინაიდან
არ არსებობს სისტემის მომხმარებელთა მიერ განხორციელებული ქმედებების
მონიტორინგის ქმედითი სისტემა. ამასთანავე, სააგენტო ვერ უზრუნველყოფს
რაიონული ცენტრების ადეკვატურ ტექნიკურ მხარდაჭერას (IT support), რაც
ზრდის ინფორმაციული უსაფრთხოების დარღვევის რისკს.

სააგენტოს არ აქვს აუტოსინგის მონიტორინგის ეფექტიანი სისტემა. სააგენტო
2014 წლის შემდეგ არ ახორციელებს კონტრაქტორის, სს „ლიბერთი ბანკის“ მიერ
ხელშეკრულებით ნაკისრი ვალდებულებების შესრულების მონიტორინგს,
მიუხედავად იმისა, რომ აღნიშნული წარმოადგენს საარსებო შემწეობის
მნიშვნელოვან კომპონენტს. შესაბამისად, სააგენტო არ ფლობს ინფორმაციას იმის

შესახებ, თუ რამდენად ეფექტიანად ახორციელებს ბანკი ნაკისრ ვალდებულებებს საბიუჯეტო სახსრების მიზნობრივი ხარჯვის მიმართულებით.

აუდიტის შედეგად გამოვლენილი ნაკლოვანებებისა და არსებული მდგომარეობის გასაუმჯობესებლად, სახელმწიფო აუდიტის სამსახურმა შეიმუშავა რეკომენდაციები.

რეკომენდაციები

- › არსებული გამოწვევების პირობებში, სააგენტომ უზრუნველყოს სარეიტინგო ქულის ოდენობაზე გავლენის მქონე მონაცემების **შესაძლო მაქსიმალური სიზუსტე**. აღნიშნული მოიცავს შემდეგი მიმართულებების განვითარებას:
 - არსებული გამოწვევების პირობებში, ბუნებრივი აირის მოხმარებისა და განათლების დონის მაჩვენებლების შემთხვევაში მნიშვნელოვანია, სააგენტომ განიხილოს პრობლემის გადაჭრის სხვადასხვა გზები და შეიმუშაოს ქმედითი მექანიზმები, ბენეფიციარის მიერ დეკლარირებული ინფორმაციის ვალიდაციისათვის;
 - სააგენტომ, არსებული რესურსების გათვალისწინებით, განიხილოს ქულის დათვლის პროცესში გამოყენებული ასაკის ველის შესაბამისობა არსებულ მდგომარეობასთან. კერძოდ, ქულის მუდმივი სისწორის უზრუნველსაყოფად, აპლიკაციაში შესაბამისი ბრძანების მოდიფიცირება, რომელიც პერიოდულად ან წელიწადში ერთხელ მაინც, განაახლებს ასაკის ველს.
- › სააგენტომ, როგორც კრიტიკული ინფორმაციული სისტემის სუბიექტმა, უზრუნველყოს არსებული საკანონმდებლო ნორმების გათვალისწინებით ინფორმაციული უსაფრთხოების მართვის სისტემის შემუშავება და პრაქტიკაში დანერგვა, მათ შორის, გამოვლენილი ნაკლოვანებების შესაბამისად მნიშვნელოვანია, განხორციელდეს:
 - შემუშავდეს პოლიტიკა და პროცედურები წვდომისა და პრივილეგიების განსაზღვრის მიზნით;
 - დაინერგოს სისტემაში მომხმარებელთა მიერ განხორციელებული ქმედებების მონიტორინგის ქმედითი სისტემა;

- უზრუნველყოფილ იქნეს ბიზნესპროცესში გამოყენებული ინფორმაციული სისტემების დაცულობის მუდმივი ტექნიკური მხარდაჭერა.
- › საბიუჯეტო რესურსების მიზნობრივი ხარჯვისა და პროგრამით გათვალისწინებული შედეგების ეფექტიანად მიღწევისათვის, *სოციალური მომსახურების სააგენტომ* უზრუნველყოს სს „ლიბერთი ბანკთან“ გაფორმებული ხელშეკრულებით გათვალისწინებული პირობების ქმედითი მონიტორინგის მექანიზმების შემუშავება და დანერგვა. სხვა დანარჩენთან ერთად, აღნიშნულის ფარგლებში, უნდა განისაზღვროს მონიტორინგის შედეგების ანგარიშების პერიოდულობა, ფორმატი და შესაბამისი პასუხისმგებელი პირები/სტრუქტურული ერთეული.

1. შესავალი

1.1 აუდიტის მოტივაცია

ქვეყანაში სიღარიბის ზღვარს მიღმა მყოფი მოსახლეობის მდგომარეობა ერთ-ერთი ყველაზე მწვავე სოციალურ-ეკონომიკური პრობლემაა. შესაბამისად, მოსახლეობის სოციალური დაცვა და სიღარიბით გამოწვეული რისკების შემცირება სახელმწიფოსათვის მნიშვნელოვან გამოწვევასა და პრიორიტეტს წარმოადგენს. აღნიშნული პრიორიტეტი ითვალისწინებს შესაბამისი ბენეფიციარების უზრუნველყოფას სოციალური ინტეგრაციისათვის საჭირო რესურსებითა და შესაძლებლობებით. სოციალური პოლიტიკის სისტემა, თავის მხრივ, უნდა უზრუნველყოფდეს საზოგადოების წინსვლას და გავლენა ჰქონდეს ქვეყნის სოციალურ სტაბილურობაზე.

საქართველოს მთავრობამ ქვეყნის სწრაფი განვითარების განხორციელებისათვის შეიმუშავა მთავრობის 4-პუნქტიანი გეგმა. აღნიშნული გეგმის ერთ-ერთ მიმართულებას სოციალური დაცვის პოლიტიკის გაუმჯობესება წარმოადგენს, რომლის ძირითად პრინციპებად განსაზღვრულია:

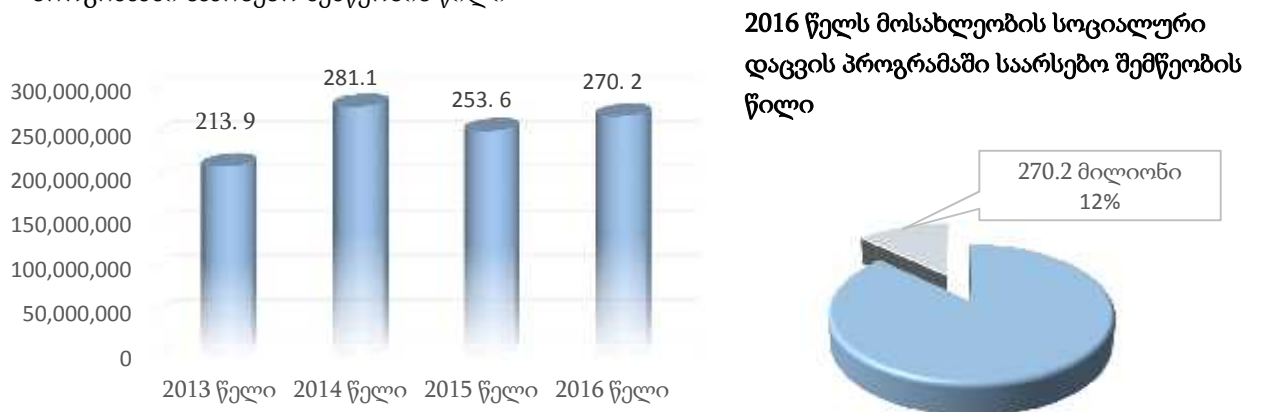
- › სიღატაკის დაძლევა და სიღარიბის შემცირება;
- › სოციალური დახმარების სისტემის ეფექტიანობა;
- › სამართლიანობა და გამჭვირვალობა;
- › დასაქმების მოტივაციის გაზრდა და ხელშეწყობა.

სოციალური დახმარების სისტემის ფუნქციონირებას არეგულირებს და კოორდინაციას უწევს *საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო* (შემდგომში - სამინისტრო).

სოციალური პოლიტიკის მიმართულებით მნიშვნელოვანია სააგენტოს მიერ ადმინისტრირებული მოსახლეობის მიზნობრივი ჯგუფების სოციალური დახმარების ქვეპროგრამა, რომლის მატერიალურად არსებითი კომპონენტია საარსებო შემწეობა.

პროგრამისათვის გამოყოფილმა თანხამ 2016 წელს 270.2 მლნ ლარი შეადგინა. წლების მანძილზე საარსებო შემწეობის პროგრამის ფარგლებში გაცემული თანხების შესახებ დეტალური ინფორმაცია და 2016 წელს საარსებო შემწეობის წილი მოსახლეობის სოციალური დაცვის პროგრამაში წარმოდგენილია გრაფიკზე №1.1.

გრაფიკი №1.1: წლების მიხედვით სააგენტოს მიერ გაცემული საარსებო შემწეობის მოცულობა მილიონ ლარებში² და 2016 წელს მოსახლეობის სოციალური დაცვის პროგრამაში საარსებო შემწეობის წილი



საარსებო შემწეობის გაცემის პროგრამის განხორციელების პროცესში კრიტიკული მნიშვნელობა აქვს ინფორმაციულ სისტემებს, რადგან მათი გამოყენებით ხორციელდება: შემწეობის მაძიებელი პირების რეგისტრაცია, ქულის მინიჭება, სტატუსისა და საარსებო შემწეობის თანხის მოცულობის განსაზღვრა და ა.შ. შესაბამისად, მნიშვნელოვანია აღნიშნული ინფორმაციული სისტემის სანდო და ზუსტი ფუნქციონირება.

დამატებით უნდა აღინიშნოს, რომ საქართველოს მთავრობის დადგენილების შესაბამისად, სააგენტო განსაზღვრულია როგორც კრიტიკული ინფორმაციული სისტემის სუბიექტი³ და ვალდებულია უზრუნველყოს ბიზნესპროცესში გამოყენებული ინფორმაციული სისტემების უწყვეტი ფუნქციონირება და

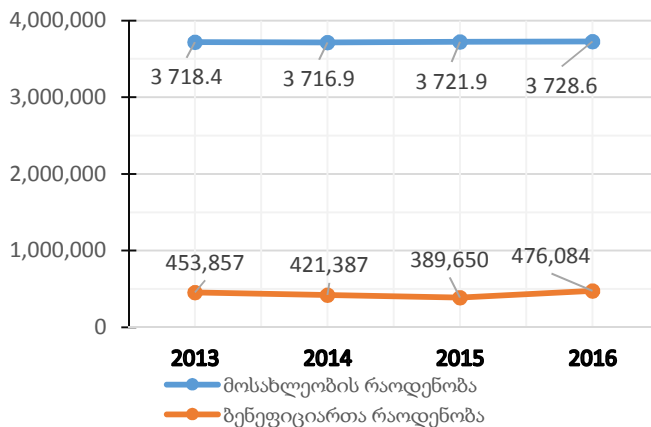
² საარსებო შემწეობის ოდენობა მოცემულია სოციალური მომსახურების სააგენტოს ვებგვერდზე წარმოდგენილ სტატისტიკურ მონაცემებზე დაყრდნობით.

³ საქართველოს მთავრობის 2014 წლის 29 აპრილის N312 დადგენილება „კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ“.

მონაცემთა კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის პრინციპების დაცვა⁴.

სააგენტოს სტატისტიკისა და ანალიზის სამმართველოს მონაცემების მიხედვით, სოციალურად დაუცველ მოქალაქეთა რაოდენობა წლების განმავლობაში მეტ - ნაკლებად სტატიკური ტენდენციით ხასიათდება. გრაფიკზე №1.2 წარმოდგენილია წლების მიხედვით საარსებო შემწეობის მიმღებთა წილი ქვეყნის მთლიან მოსახლეობასთან მიმართებაში, რომელმაც 2016 წელს 12.77% შეადგინა. აღსანიშნავია, რომ 2015 წელს ბენეფიციართა დიდი რაოდენობა ამოვარდა საარსებო შემწეობის მიმღებთა სიიდან, რაც აიხსნება მეთოდოლოგიის ცვლილების შედეგად გამოწვეული ხარვეზით⁵.

გრაფიკი №1.2: 2013 - 2016 წლებში საარსებო შემწეობის მიმღები მოსახლეობის რაოდენობა და წილი მთლიან მოსახლეობაში⁶



წელი	მოსახლეობის რაოდენობა (მილიონი)	ბენეფიციართა რაოდენობა	ბენეფიციართა წილი მთელ მოსახლეობაში
2013	3 718.4	453,857	12.21%
2014	3 716.9	421,387	11.34%
2015	3 721.9	389,650	10.47%
2016	3 728.6	476,084	12.77%

ასევე აღსანიშნავია, რომ პროგრამის ადმინისტრირებაში არსებული ხარვეზების გამო, 2015 და 2016 წლებში საჭირო გახდა საქართველოს კანონში „სოციალური

⁴ საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“.

⁵ 2015 წლის მაისი-ივლისის პერიოდში დიდი რაოდენობის ბენეფიციარებისათვის „სოციალურად დაუცველის“ სტატუსის შეწყვეტა, რაც სამინისტრომ მიიჩნია მეთოდოლოგიის ნაკლოვანებად და გახდა მეთოდოლოგიაში დამატებითი ცვლილებების განხორციელების საფუძველი, შესაბამისად, შეიცვალა მარტოხელა პენსიონერთა კოეფიციენტი.

⁶ მოსახლეობის რაოდენობა განისაზღვრა საქართველოს სტატისტიკის ეროვნული სამსახურის მონაცემებზე (2017 წელს გადაანგარიშებული მონაცემები) დაყრდნობით, ხოლო საარსებო შემწეობის მიმღებ ბენეფიციართა რაოდენობა – სააგენტოს მონაცემებზე დაყრდნობით.

დახმარების შესახებ“ ცვლილების შეტანა და საარსებო შემწეობის სახით ზედმეტად გადარიცხული თანხების ლეგალიზება, კერძოდ:

- › 2015 წლის პირველ აპრილამდე ბენეფიციარებზე ზედმეტად გადარიცხული საარსებო შემწეობის თანხების (ზედმეტად დარიცხული საარსებო შემწეობის თანხა დაახლოებით შეადგენს 767,526 ლარს) ლეგალიზება;
- › 2015 წლის პირველი აპრილიდან 2016 წლის 1 ივლისამდე ზედმეტად გადარიცხული თანხების (ზედმეტად დარიცხული საარსებო შემწეობის თანხა დაახლოებით შეადგენს 900,500 ლარს) ლეგალიზება.

ასევე აღსანიშნავია, რომ საარსებო შემწეობის პროგრამის ფარგლებში სააგენტოს კონტროლის დეპარტამენტმა დააფიქსირა ბენეფიციარებზე საბიუჯეტო სახსრების ზედმეტად გადარიცხვის ფაქტები. აღნიშნული განპირობებული იყო სხვადასხვა ხარვეზის გამო, როგორებიცაა დეკლარაციაში ასახულისაგან განსხვავებული სოციალურ-ეკონომიკური მდგომარეობა, დეკლარაციის მარეგულირებელი ნორმების შეუსაბამოდ კორექტირება და სხვა საკანონმდებლო მოთხოვნების დარღვევა.

2016 წელს სამინისტროში სახელმწიფო აუდიტის სამსახურის მიერ ჩატარებული ეფექტიანობის აუდიტის⁷ ფარგლებში გამოვლინდა პროგრამის ადმინისტრირებასთან დაკავშირებული ისეთი ნაკლოვანებები, როგორიცაა ბენეფიციართა დაბალი ინფორმირებულობისა და საარსებო შემწეობის დანიშვნის დროში გახანგრძლივებული პროცედურები.

საარსებო შემწეობის პროგრამის ქვეყნის მოსახლეობაზე არსებითი სოციალურ-ეკონომიკური გავლენიდან და ადმინისტრირების პროცესში ინფორმაციული სისტემის როლიდან გამომდინარე, სახელმწიფო აუდიტის სამსახურმა მიზანშეწონილად მიიჩნია შეესწავლა საარსებო შემწეობის გაცემის პროცესი და

⁷ საარსებო შემწეობის მიმღები შრომისუნარიანი ბენეფიციარების სოციალურ დახმარებებზე დამოკიდებულების შემცირება, რეგისტრაციის №59/36, <http://sao.ge/files/auditi/auditis-angarishebi/2016/tb-socialuri-daxmarebebi.pdf>

აღნიშნულ პროცესში გამოყენებული ინფორმაციული სისტემის მართვის
არსებული პრაქტიკა.

1.2 აუდიტის მიზანი და მთავარი კითხვები

აუდიტის მიზანია შეფასდეს, რამდენად ეფექტიანად ახდენს სააგენტო საარსებო
შემწეობის პროგრამის ადმინისტრირებას და რამდენად უზრუნველყოფილია
მოქალაქეთა შესახებ არსებული ინფორმაციის უსაფრთხოება.

აუდიტის მიზნის შესაფასებლად მთავარ კითხვად განისაზღვრა:

რამდენად უზრუნველყოფს არსებული პროცედურები და ინფორმაციული
სისტემები საარსებო შემწეობის ეფექტიან ადმინისტრირებას და მოქალაქეთა
შესახებ სააგენტოში არსებული ინფორმაციის დაცულობას?

აუდიტის ქვეკითხვებად განისაზღვრა შემდეგი:

1. რამდენად ეფექტიანი პროცედურებია დანერგილი ოჯახის სოციალურ-
ეკონომიკური მდგომარეობის შეფასებისათვის და რამდენად
ადეკვატურად უზრუნველყოფს არსებული ინფორმაციული სისტემა
ბიზნესპროცესით გათვალისწინებული მიზნების მიღწევას?
2. რამდენად უზრუნველყოფილია ინფორმაციული უსაფრთხოება და
მესამე მხარეებისაგან მოქალაქეთა შესახებ მიღებული მონაცემების
კონფიდენციალურობისა და მთლიანობის დაცვა, ინფორმაციის
მიმოცვლისა და ტერიტორიულ ერთეულებთან კომუნიკაციის
პროცესში?
3. რამდენად ეფექტიანად/ადეკვატურად უზრუნველყოფს სააგენტო
ბენეფიციარებზე თანხის გადარიცხვის პროცესს?

1.3 აუდიტის მასშტაბი

აუდიტის მიზნებიდან გამომდინარე, სახელმწიფო აუდიტის სამსახურმა
შეისწავლა სააგენტოს მიერ 2015-2016 წლებში სოციალურად დაუცველი ოჯახების
პროგრამის ფარგლებში განხორციელებული საქმიანობა. აუდიტის ობიექტია
სამინისტრო, როგორც პროგრამის პოლიტიკაზე პასუხისმგებელი ორგანო და ასევე

სამინისტროს დაქვემდებარებული სააგენტო, როგორც პროგრამის უშუალო
ადმინისტრირებაზე პასუხისმგებელი უწყება.

აუდიტი ჩატარდა შემდეგი სტანდარტებისა და სახელმძღვანელოების
გამოყენებით:

- › უმაღლესი აუდიტორული ორგანიზაციების აუდიტის საერთაშორისო
სტანდარტები (ISSAIs):
 - ეფექტიანობის აუდიტის სტანდარტი ISSAI 3000 და ISSAI
3100;
 - ინფორმაციული ტექნოლოგიების აუდიტის
სახელმძღვანელო ISSAI 5300.
- › ინფორმაციული ტექნოლოგიების აუდიტის სახელმძღვანელო
უმაღლესი აუდიტორული ორგანიზაციებისთვის⁸;
- › აშშ-ს უმაღლესი აუდიტორული ორგანოს მიერ შემუშავებული
ფედერალური ინფორმაციული სისტემების აუდიტის
სახელმძღვანელო (FISCAM);
- › ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის
(Information Systems Audit and Control Association - ISACA) მიერ
შემუშავებული ინფორმაციული ტექნოლოგიების რწმუნების ჩარჩო
(ITAF).

1.3.1 აუდიტის მასშტაბის შეზღუდვა

აუდიტის მიმდინარეობისას, აუდიტის ობიექტის მხრიდან დაფიქსირდა
აუდიტის მასშტაბის შეზღუდვა, რამაც საბოლოოდ გამოიწვია დაგეგმილი
პროცედურის გაუქმება. კერძოდ, მიმდინარე აუდიტის ფარგლებში, ბენეფიციართა
მონაცემთა ბაზების დაცულობის შეფასების მიზნით, აუდიტის ჯგუფმა დაგეგმა
მოწყვლადობის ტესტირების პროცედურები, რომლის ფარგლებში უნდა
შეფასებულიყო აუდიტის პერიოდში (2015-2016 წლებში) მონაცემების დაცულობა.
პროცედურის ჩატარებამდე რამდენიმე დღით ადრე, აუდიტის ჯგუფისათვის
უცნობი მიზეზებით, განახლდა შესასწავლი სერვერის ოპერაციული სისტემა,

⁸ WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.

მონაცემთა ბაზის მართვის სისტემა და უსაფრთხოების პროგრამები. შესაბამისად, სრულად შეიცვალა გარემო, რომელშიც მუშავდებოდა მონაცემები და რომელიც არ იყო განახლებული ბოლო ათწლეულის მანძილზე. ზემოაღნიშნულიდან გამომდინარე, აუდიტის ჯგუფმა ვედარ შეაფასა აუდიტის პერიოდში გამოყენებული სერვერების ოპერაციული სისტემების უსაფრთხოება/დაცულობა. დეტალური ინფორმაცია განხილულია №2.3.2 ქვეთავში.

დამატებით აღსანიშნავია, რომ აუდიტის ჯგუფმა სააგენტოსგან ვერ მიიღო სს „ლიბერთი ბანკთან“ აუდიტის მასშტაბით გათვალისწინებული საკითხების განხილვისათვის ადეკვატური ინფორმაცია. კერძოდ, ვერ გახდა შესაძლებელი შემდეგი ინფორმაციის მიღება და დადასტურება:

- › არსებობდა თუ არა 2014 წლის შემდეგ სს „ლიბერთი ბანკთან“ გაფორმებული ხელშეკრულების მონიტორინგზე პასუხისმგებელი პირი ან ერთეული;
- › არსებობდა თუ არა ბენეფიციარებზე საარსებო შემწეობის თანხის გადარიცხვისათვის ალტერნატიული გზები;
- › უზრუნველყოფილი იყო თუ არა ბანკის მიერ უკან დასაბრუნებელი თანხების დაბრუნებისა და ჯარიმების გადახდების პროცესების განხორციელება.

1.4 კრიტერიუმები

საარსებო შემწეობის პროგრამის მართვისა და ფუნქციონირების შეფასების მიზნით, აუდიტის პროცედურების ჩატარებისას გამოყენებულ იქნა შემდეგი კრიტერიუმები:

მარეგულირებელი ნორმატიული აქტები:

- › საქართველოს კანონი „სოციალური დახმარების შესახებ“;
- › საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“;
- › საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“;
- › საქართველოს მთავრობის 2014 წლის 31 დეკემბრის №758 დადგენილება „სოციალურად დაუცველი ოჯახების

(შინამეურნეობების) სოციალურ-ეკონომიკური მდგომარეობის შეფასების მეთოდოლოგიის დამტკიცების შესახებ“;

- › საქართველოს მთავრობის 2006 წლის 28 ივლისის №145 დადგენილება „სოციალური დახმარების შესახებ“;
- › საქართველოს მთავრობის 2010 წლის 24 აპრილის №126 დადგენილება „ქვეყანაში სიღატაკის დონის შემცირებისა და მოსახლეობის სოციალური დაცვის სრულყოფის ღონისძიებათა შესახებ“;
- › საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის მინისტრის 2010 წლის 20 მაისის №141/5 ბრძანება „სოციალურად დაუცველი ოჯახების სოციალურ-ეკონომიკური მდგომარეობის შეფასების წესის დამტკიცების თაობაზე“;
- › საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის მინისტრის 2006 წლის 22 აგვისტოს №225/5 ბრძანება „მიზნობრივი სოციალური დახმარების დანიშვნისა და გაცემის წესის დამტკიცების შესახებ“;
- › მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის №2 ბრძანება „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“.

საერთაშორისო სტანდარტები და საუკეთესო პრაქტიკის სახელმძღვანელოები:

- › NIST (National Institute of Standards and Technology) სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტის მიერ შემუშავებული სტანდარტები;
- › ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ შემუშავებული ჩარჩო (framework) COBIT 5.

1.5 ზოგადი ინფორმაცია

1.5.1 განმახორციელებელი ერთეულები

„სოციალური დახმარების შესახებ“ საქართველოს კანონის საფუძველზე სააგენტო დადგენილი წესით უზრუნველყოფს ფულადი სოციალური დახმარებების

ადმინისტრირებას⁹. საარსებო შემწეობის გაცემის პროცესის ადმინისტრირებას ინფორმაციული ტექნოლოგიების დეპარტამენტთან კოორდინაციით ახორციელებს სააგენტოს სოციალური დახმარების ადმინისტრირების დეპარტამენტი. აღნიშნულ პროცესში ასევე მნიშვნელოვანია სამინისტროს სოციალური დაცვის დეპარტამენტი, რომელიც პასუხისმგებელია საარსებო შემწეობის პროგრამის მიმართულებით სახელმწიფო პოლიტიკის განხორციელების სტრატეგიული გეგმისა და მექანიზმების შემუშავებასა და მონიტორინგზე¹⁰. გრაფიკზე №1.3 წარმოდგენილია საარსებო შემწეობის გაცემის პროცესში სააგენტოსა და სამინისტროს შესაბამისი ერთეულების ზოგადი ფუნქციები.

გრაფიკი №1.3: განმახორციელებელი დეპარტამენტების ფუნქცია-მოვალეობები



უნდა აღინიშნოს, რომ სამინისტროს საკუთრებაშია სასერვერო ინფრასტრუქტურა და შესაბამისად, ფიზიკურ მოვლასა და ტექნიკურ უზრუნველყოფაზე პასუხისმგებელია სამინისტროს ინფორმაციული ტექნოლოგიების დეპარტამენტი, ხოლო სააგენტოს ადმინისტრირებაში მყოფ პროგრამებში გამოყენებული ინფორმაციული სისტემების პროგრამულ უზრუნველყოფაზე - სააგენტოს ინფორმაციული ტექნოლოგიების დეპარტამენტი.

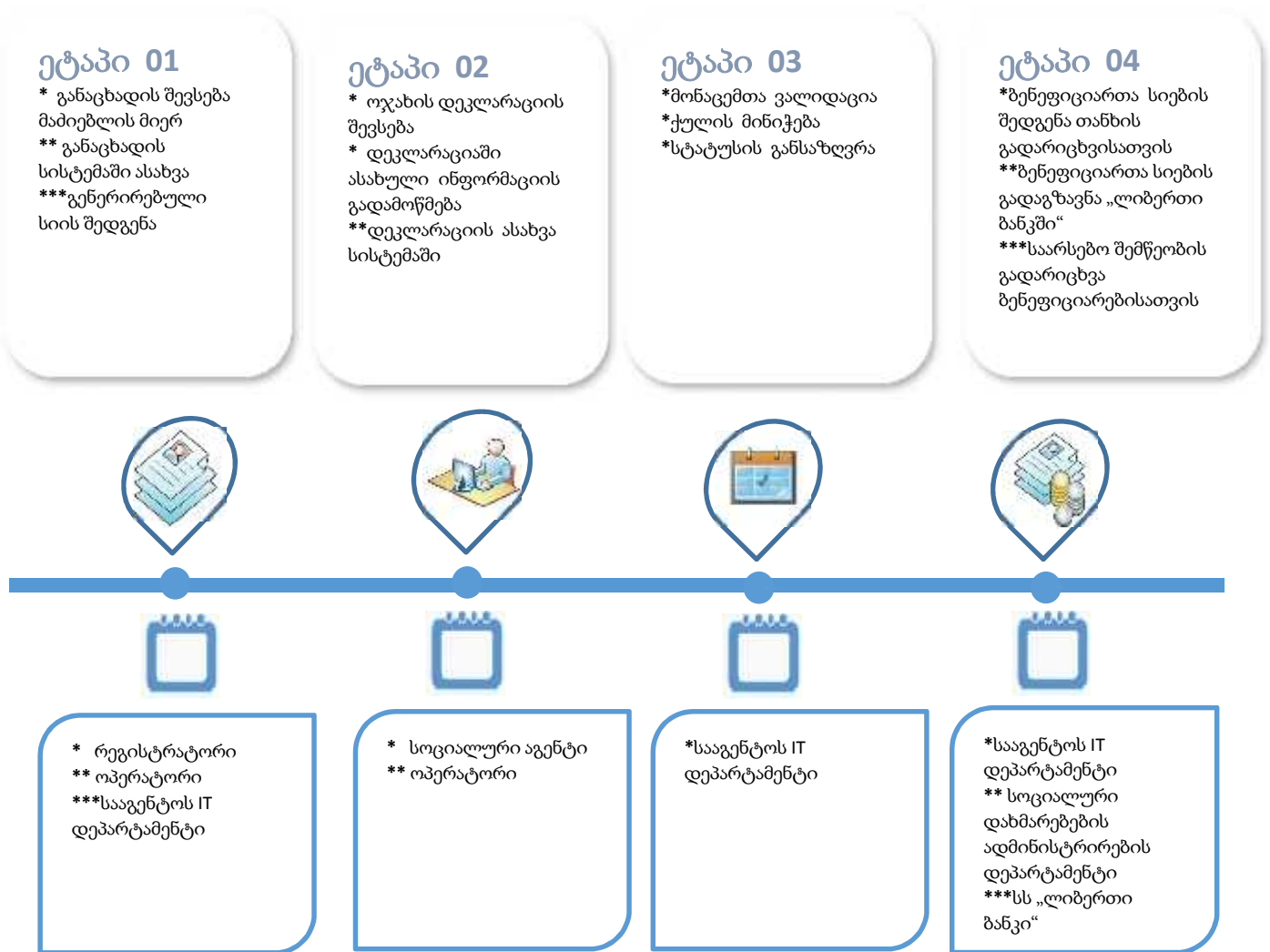
1.5.2 საარსებო შემწეობის გაცემის ბიზნესპროცესი

დიაგრამა №1.1 წარმოდგენილია მაძიებლის სოციალურად დაუცველი ოჯახების სიაში რეგისტრირების პროცესი და შესაბამის პროცესზე პასუხისმგებელი ერთეულები:

⁹ საქართველოს კანონი „სოციალური დახმარების შესახებ“, მუხლი 17, პუნქტი „ე“.

¹⁰ საქართველოს შრომის, ჯანმრთელობისა და სოციალური სამინისტროს დებულება.

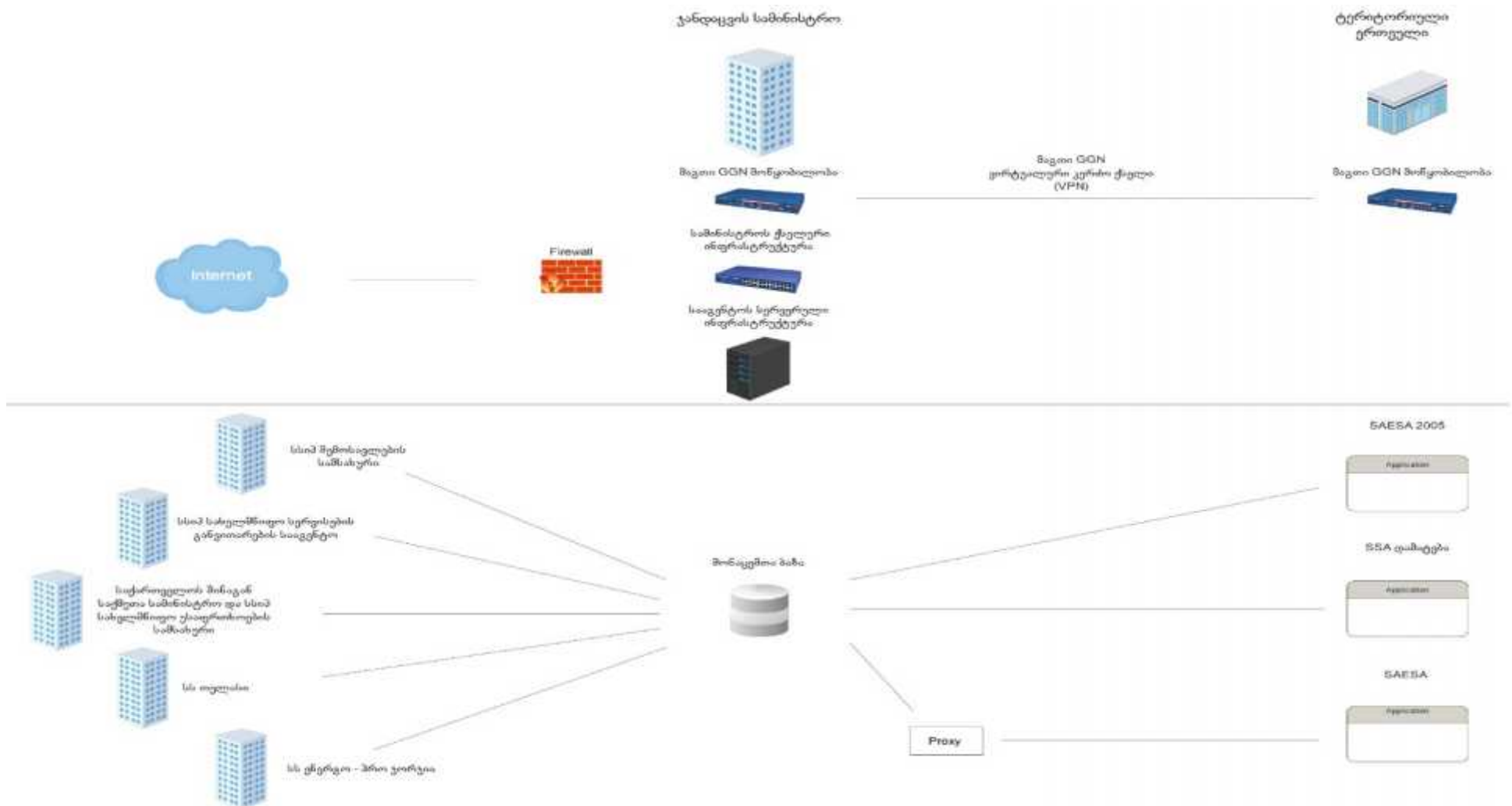
დიაგრამა №1.1: ოჯახების მონაცემთა ერთიან ბაზაში რეგისტრირების პროცესი



ზემოთ მოცემულ დიაგრამაზე ასახულ პირველ ეტაპზე, რეგისტრატორი თითოეულ ახალ განაცხადს ანიჭებს ოჯახის თორმეტნიშნა უნიკალურ საიდენტიფიკაციო ნომერს (FID) და ხელით შეაქვს რეესტრის ჟურნალში, სადაც თითოეულ განაცხადს რიგითობის მიხედვით მინიჭებული აქვს უნიკალური ნომერი. თუ ბენეფიციარი პირველად მიმართავს სააგენტოს, მისი განაცხადი პირდაპირ ხვდება ოპერატორთან, ხოლო განმეორებითი მიმართვის შემთხვევაში, განაცხადი კანცელარიის გავლით ეგზავნება ოპერატორს სისტემაში ასახვისათვის.

ბიზნესპროცესში გამოყენებული სისტემები

დიაგრამა №1.2: ლოგიკური ტოპოლოგიის მოდელი



სააგენტოს ტერიტორიული ერთეულები აღნიშნული პროცესის განხორციელებისათვის იყენებენ 3 განსხვავებულ სამომხმარებლო ინტერფეისს: SAESA 2005, SAESA, SSA - დამატება, რომლებიც ინფორმაციას იღებენ საერთო მონაცემთა ბაზიდან. შესაბამისად, საბოლოო მომხმარებლებს სამი სხვადასხვა დესკტოპ აპლიკაციის საშუალებით გააჩნიათ წვდომა MS SQL ბაზასთან, რომელშიც განთავსებულია ბენეფიციართა შესახებ მონაცემები. ტერიტორიულ ერთეულებში აღნიშნულ აპლიკაციებზე დაშვება აქვს ბიზნესპროცესში ჩართულ ყველა თანამშრომელს, როგორც არის, რეგისტრატორი, ოპერატორი, მთავარი და უფროსი სპეციალისტები, უფროსი სოციალური აგენტი და სოციალური აგენტი. ტერიტორიულ ერთეულებს სამინისტროსთან კავშირი აქვს კერძო ვირტუალური ქსელით (VPN), რომლის გამართვისა და ტექნიკური უზრუნველყოფისათვის სააგენტოს გაფორმებული აქვს ხელშეკრულება შპს „მაგთიკომთან“. შესაბამისად, ინფორმაციის მიმოცვლა სააგენტოსა და ტერიტორიულ ერთეულებს შორის ხდება დაცული არხის საშუალებით. დიაგრამა №1.2 - ზე წარმოდგენილია ლოგიკური ტოპოლოგიის მოდელი.

მესამე მხარეები

სააგენტოს ინფორმაციული ტექნოლოგიების დეპარტამენტი, ოჯახის დეკლარაციაში წარმოდგენილი ინფორმაციის ვალიდაციის, გენერაციის შედგენისა და ქულის გამოთვლის მიზნით, იყენებს სხვადასხვა უწყებიდან მიღებულ ინფორმაციას. კერძოდ, ინფორმაციის ვალიდაცია ხდება სსიპ - შემოსავლების სამსახურიდან, სსიპ - სერვისების განვითარების სააგენტოდან, შინაგან საქმეთა სამინისტროდან, სსიპ - სახელმწიფო უსაფრთხოების სამსახურიდან, სს „თელასიდან“, სს „ენერგო - პრო ჯორჯიადან“ მიღებულ ინფორმაციაზე დაყრდნობით. აღნიშნულ სტრუქტურებთან გაფორმებული ხელშეკრულების ფარგლებში მისაღები ინფორმაცია წარმოდგენილია ცხრილში №1.1.

ცხრილი №1.1: ხელშეკრულებით გათვალისწინებული მოსაწოდებელი ინფორმაცია

უწყებები	მოწოდებული ინფორმაციის ტიპი	ინფორმაციის მოწოდების პერიოდულობა
სსიპ - შემოსავლების სამსახური	ინფორმაცია რეგისტრაციის მაძიებლის ან/და რეგისტრირებული ოჯახების წარმომადგენლების <u>შემოსავლების</u> შესახებ	ყოველთვიურად
სსიპ - სახელმწიფო სერვისების განვითარების სააგენტო	<u>პირადი ინფორმაცია</u> საქართველოს მოქალაქეების შესახებ	თვეში 3-ჯერ/მონაცემთა სამინისტროს სერვერზე განთავსებით
საქართველოს შინაგან საქმეთა სამინისტრო და სსიპ - სახელმწიფო უსაფრთხოების სამსახური	რეგისტრაციის მაძიებელი ან/და რეგისტრირებული ოჯახების საზღვრის გადაკვეთისა და მექანიკური სატრანსპორტო საშუალებების შესახებ ინფორმაცია	სააგენტოს მოთხოვნის საფუძველზე/ელექტრონულ ბაზაზე რეალურ დროში დაშვების გზით
სს „თელასი“ სს „ენერგო - პრო ჯორჯია“	რეგისტრაციის მაძიებელი და/ან რეგისტრირებული ოჯახების მიერ გაწეული კომუნალური ხარჯების შესახებ ინფორმაცია. (აბონენტის ნომერი; მისამართი; მოხმარებული ელექტროენერგიის ოდენობა; დარიცხული თანხა - თვე და წელი; გადახდილი თანხა და სუბსიდირება)	ყოველთვიურად, ბაზაზე რეალურ დროში დაშვების გზით

ცხრილში წარმოდგენილი ინფორმაციის გაცვლა ხდება ვირტუალური კერძო ქსელით (VPN) და განთავსდება სამინისტროს მფლობელობაში არსებულ სერვერებზე. შინაგან საქმეთა სამინისტროს, სსიპ - სახელმწიფო უსაფრთხოების სამსახურის, სს „თელასისა“ და სს „ენერგო - პრო ჯორჯიას“ შემთხვევაში, მონაცემების მიღება ხდება ვებსერვისის საშუალებით, სსიპ - შემოსავლების სამსახურისაგან ინფორმაციის მიღება ხდება მონაცემთა ბაზების განთავსებით სამინისტროს სერვერზე. რაც შეეხება სსიპ - სახელმწიფო სერვისების განვითარების სააგენტოს, ინფორმაციის მიღება ხდება როგორც მონაცემთა ბაზებზე სააგენტოს რეალურ დროში დაშვებით, ასევე აღნიშნული მონაცემთა ბაზების სამინისტროს სერვერზე განთავსებით. აღსანიშნავია, რომ სააგენტოს წარმომადგენლების განცხადებით, ზოგიერთ შემთხვევაში გარე უწყებებიდან მიღებული ინფორმაციის სიზუსტე და სისრულე არ არის უზრუნველყოფილი. კერძოდ, არსებობს შემთხვევები, როდესაც შემოსავლების სამსახურის მიერ სააგენტოსათვის წარმოდგენილი პიროვნების საიდენტიფიკაციო ნომერი არასწორია, სერვისების განვითარების სააგენტო დროულად ვერ აღრიცხავს გარდაცვალებას, საზღვრის კვეთის შესახებ მონაცემები არაზუსტია. აღნიშნული პრობლემა ხელს უშლის ქულის სწორად დათვლას.

ოჯახის შესახებ არსებული ინფორმაციის ვალიდაცია

სააგენტოს ინფორმაციული ტექნოლოგიების დეპარტამენტის გარდა, ინფორმაციის ვალიდაციის პროცედურას ახორციელებენ სოციალური აგენტებიც. სოციალური აგენტი აკეთებს ინფორმაციის პირველად ვალიდაციას, რომელიც მოიცავს ოჯახის შესახებ შევსებულ დეკლარაციაში წარმოდგენილი ინფორმაციის გადამოწმებას ზემოთ აღნიშნული მონაცემთა ბაზების გამოყენებით. აღნიშნული პროცესისათვის საჭირო რიგი ინფორმაციის ჩამონათვალი განსაზღვრულია საქართველოს მთავრობის დადგენილებით¹¹.

¹¹ „ქვეყანაში სიღატაკის დონის შემცირებისა და მოსახლეობის სოციალური დაცვის სრულყოფის ღონისძიებათა შესახებ“ საქართველოს მთავრობის 2010 წლის 24 აპრილის №126 დადგენილება, მუხლი 1, პუნქტი 2, ქვეპუნქტი „ა“.

ცხრილში №1.1 წამოდგენილი მესამე მხარეებისაგან მიღებულ მონაცემთა ბაზებზე დაყრდნობით, სოციალური აგენტი ბენეფიციართა შესახებ ინფორმაციის გადამოწმებას ახდენს SAESA აპლიკაციების გამოყენებით და სააგენტოში არსებული სხვა ბაზების მეშვეობით, რომლებთან დაკავშირება შესაძლებელია/ხორციელდება ვებგვერდის მეშვეობით, რომელიც განკუთვნილია მხოლოდ შიდა მოხმარებისათვის.

საარსებო შემწეობის ოდენობა და თანხის გაცემა

2014 წლის ბოლოს სამინისტრომ გაეროს ბავშვთა ფონდთან (UNICEF) თანამშრომლობით შეიმუშავა საარსებო შემწეობის მაძიებელთა შეფასების ახალი მეთოდოლოგია¹², რომელიც ძალაში შევიდა 2015 წლის მაისიდან. აღნიშნული მეთოდოლოგიის ფარგლებში მოხდა სარეიტინგო ქულის ოდენობაზე მოქმედი ინდიკატორებისა და კოეფიციენტების ცვლილება და შეიცვალა საარსებო შემწეობის თანხის მოცულობა. ახალი მეთოდოლოგია ასევე ითვალისწინებს სოციალურად დაუცველი ოჯახების დიფერენცირებას სხვადასხვა ქულის კატეგორიებში, რაც წარმოდგენილია ცხრილში №1.2.

ცხრილი №1.2: ოჯახების დიფერენცირება

ზღვრული ქულა	შემწეობის ოდენობა ოჯახის თითოეულ წევრზე
<30,001	60 ლარი
30,001 - 57,001	50 ლარი
57,001 - 60,001	40 ლარი
60,001 - 65,001	30 ლარი
<100,001	10 ლარი – 16 წლამდე ბავშვებზე

ქულის ვალიდაციისა და საარსებო შემწეობის შესაბამისი ოდენობის განსაზღვრის შემდგომ, სააგენტოს ინფორმაციული ტექნოლოგიებისა და სოციალური დახმარებების ადმინისტრირების დეპარტამენტის მიერ მომზადებული

¹² საქართველოს მთავრობის 2014 წლის 31 დეკემბრის №758 დადგენილება „სოციალურად დაუცველი ოჯახების (შინამეურნეობების) სოციალურ-ეკონომიკური მდგომარეობის შეფასების მეთოდოლოგიის დამტკიცების შესახებ“.

ბენეფიციართა სიების გადაგზავნა ხდება სს „ლიბერთი ბანკში“. სააგენტოსთან გაფორმებული ფულადი გასაცემლების გაცემის/დარიგების უსასყიდლო საბანკო მომსახურების თაობაზე ხელშეკრულების ფარგლებში, ბანკი ვალდებულია უზრუნველყოს ბენეფიციართათვის შესაბამისი საარსებო შემწეობის თანხის გადარიცხვა და შეასრულოს სხვა საბანკო ოპერაციები უსასყიდლოდ.

2. აუდიტის მიგნებები

2.1 ბენეფიციარების შესახებ ინფორმაციის ვალიდაციის პროცესში არსებული ნაკლოვანებები

ოჯახის სარეიტინგო ქულის დათვლის პროცესი კომპლექსურია და აერთიანებს, როგორც ოჯახის საცხოვრებელი პირობების დათვალიერებასა და შეფასებას, ასევე ოჯახის შესახებ სხვადასხვა სახის ინფორმაციის მოგროვებასა და ვალიდაციას. კერძოდ, საცხოვრებელი პირობების შეფასებას აკეთებს სოციალური აგენტი, ხოლო ოჯახის შესახებ ინფორმაციის ვალიდაცია ხდება სხვადასხვა სამთავრობო ან კერძო უწყებებიდან მიღებულ ინფორმაციაზე დაყრდნობით. (იხ. ცხრილი №1.1).

აუდიტის შედეგად გამოიკვეთა მამიებელი და ბენეფიციარი ოჯახების სარეიტინგო ქულის დათვლაში მონაწილე ზოგიერთი ფაქტორის ვალიდაციასთან დაკავშირებული ნაკლოვანებები, რომელიც რიგ შემთხვევაში გამოწვეულია სახელმწიფოს დონეზე ცენტრალიზებული ინფორმაციის არარსებობით. ზემოთ აღნიშნული ფაქტორებია:

- › ინფორმაცია ოჯახის კუთვნილი სასოფლო-სამეურნეო მიწის ნაკვეთისა და უძრავი ქონების შესახებ;
- › ინფორმაცია ოჯახის მიერ ბუნებრივი აირის მოხმარების ფულადი მაჩვენებელი;
- › ინფორმაცია ოჯახის წევრების განათლების შესახებ.

საყურადღებოა, რომ აუდიტის მიმდინარეობისას, სააგენტომ შეძლო ჩამოთვლილი ნაკლოვანებების ნაწილობრივ გამოსწორება.

2.1.1 უძრავი ქონებისა და სასოფლო-სამეურნეო მიწის შესახებ ინფორმაციის ვალიდაცია

აუდიტის მიმდინარეობისას სააგენტოს არ ჰქონდა სათანადო მექანიზმები სასოფლო-სამეურნეო მიწებთან და უძრავ ქონებასთან დაკავშირებული ინფორმაციის ვალიდაციისათვის. კერძოდ, საარსებო შემწეობის მამიებელი ოჯახი

თავად აწვდიდა კუთვნილი სასოფლო-სამეურნეო მიწის შესახებ ინფორმაციას სააგენტოს სოციალურ აგენტს, რისი ვალიდაცია/გადამოწმება ვერ ხერხდებოდა და ითვლებოდა უტყუარ ინფორმაციად. ამასთანავე, ოჯახის მიერ უძრავი ქონების შესახებ ინფორმაციის გადამოწმება ხორციელდებოდა ხელით, კერძოდ, სოციალური აგენტები საჯარო რეესტრის ეროვნული სააგენტოს ვებგვერდზე ამოწმებდნენ თითოეული ბენეფიციარის მიერ მიწოდებულ ინფორმაციას, თუმცა, აუდიტის მიმდინარეობისას, სააგენტოსა და საჯარო რეესტრის ეროვნულ სააგენტოს შორის 2017 წლის 27 ივლისს გაფორმდა ხელშეკრულება ზემოაღნიშნული ინფორმაციის ავტომატურ რეჟიმში მიღების თაობაზე. შესაბამისად, სიღარიბის ზღვარს მიღმა მყოფი ოჯახების მონაცემთა ერთიან ბაზაში განთავსებული ინფორმაციის ვალიდაციის პროცესი გახდება ავტომატიზებული, რაც ხელს შეუწყობს სააგენტოს ადამიანური და დროითი რესურსების პროდუქტიულ გამოყენებას.

2.1.2 ბუნებრივი აირის მოხმარების შესახებ ინფორმაციის ვალიდაცია

არსებული მდგომარეობით, სააგენტოს არ გააჩნია მამიებელი ან/და ბენეფიციარი ოჯახის მიერ ბუნებრივი აირის მოხმარების მაჩვენებლის ვალიდაციის მექანიზმი. აღნიშნული მაჩვენებელი გამოიყენება სარეიტინგო ქულის გამოთვლაში და შესაბამისად, გავლენას ახდენს სააგენტოს გადაწყვეტილებაზე - დანიშნოს, შეაჩეროს, შეწყვიტოს ან განსაზღვროს საარსებო შემწეობის მოცულობა.

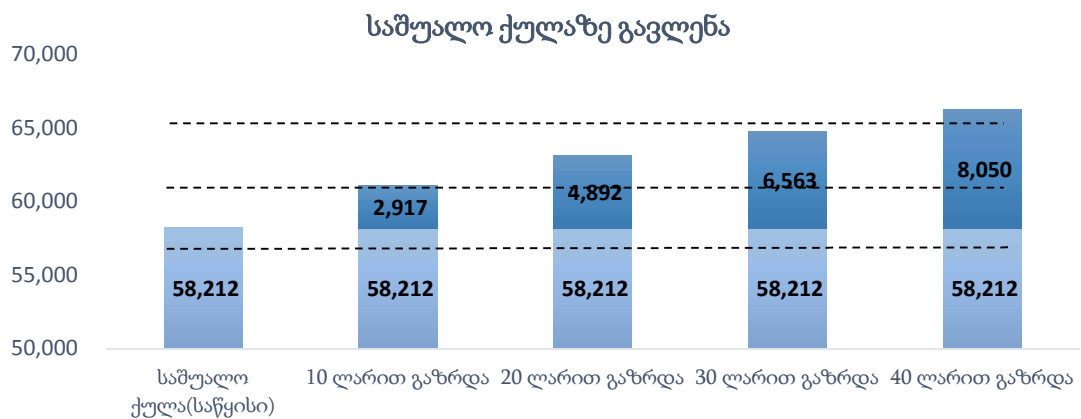
აუდიტის ჯგუფმა სარეიტინგო ქულაზე ბუნებრივი აირის მოხმარების მაჩვენებლის გავლენის შესაფასებლად და შესაბამისი ინფორმაციის სიზუსტის მნიშვნელობის განსაზღვრისათვის ჩატარა სიმულაციური ანალიზი, რომლის ფარგლებში, სხვა თანაბარ პირობებში, გაანალიზა სარეიტინგო ქულასა და გადასახდელ თანხაზე ბუნებრივი აირის მაჩვენებლის გავლენა.

ბუნებრივი აირის მაჩვენებლის გავლენა სარეიტინგო ქულაზე

სიმულაციური ანალიზი ჩატარდა საარსებო შემწეობის მიმღები ბენეფიციარების სრულ ბაზაზე, რომელთა შეფასება მოხდა 2015 წლის 1 მაისიდან 2016 წლის 1 ოქტომბრამდე პერიოდში, შეფასების ახალი მეთოდოლოგიის საფუძველზე

(დეტალები იხ. დანართში №1). აუდიტის ჯგუფმა იმ დაშვებით, რომ მაძიებელს შესაძლებლობა ჰქონდა რეალურთან შედარებით, შემცირებული თანხა წარედგინა სააგენტოსათვის, ყველა ბენეფიციარის ბუნებრივი აირის წლიური გადასახადის მაჩვენებელი გაზარდა 10, 20, 30 და 40 ლარით (შესაბამისად, თვეში 0,83 ლარი, 1,67 ლარი, 2,05 ლარი, 3.33 ლარი), რათა შეეფასებინა გავლენა სარეიტინგო ქულასა და სააგენტოს მიერ გადასახდელ თანხაზე. გრაფიკებზე: №2.1 და №2.2 წარმოდგენილია, ოჯახის მიერ ბუნებრივი აირის გადასახადის შესაბამისი ოდენობით შემცირების შემთხვევაში, შერჩეული ბენეფიციარების საშუალო ქულისა და მათზე გადასახდელი თანხის ცვლილება.

გრაფიკი № 2.1: საშუალო ქულის ცვლილება ბუნებრივი აირის გადასახადის მაჩვენებლის ცვლილების მიხედვით



გრაფიკი № 2.2: გადასახდელ თანხაზე ბუნებრივი აირის მაჩვენებლის გავლენა¹³



¹³ სიმულაციამდე გადასახდელი თანხის შემთხვევაში არ არის გამოყენებული სააგენტოს მიერ ერთ კონკრეტულ თვეში ფაქტობრივად გადახდილი თანხა, არამედ დათვლილია სიმულაციამდე არსებული ქულის შემთხვევაში ბენეფიციარზე გადასახდელი თანხა.

წარმოდგენილი სიმულაცია აჩვენებს, რომ ბუნებრივი აირის გადასახადის შესახებ ინფორმაციის მინიმალური ცვლილებაც კი, სხვა თანაბარ პირობებში, მნიშვნელოვან გავლენას ახდენს საშუალო სარეიტინგო ქულაზე და მნიშვნელოვნად იზრდება გადასახდელი საბიუჯეტო სახსრები (10 ლარის შემთხვევაში – თვეში 445.9 ათასი ლარით მეტი, 20 ლარის შემთხვევაში – 808.7 ათასი ლარით მეტი, 30 ლარის შემთხვევაში – 1.1 მილიონი ლარით მეტი, 40 ლარის შემთხვევაში – 1.4 მილიონი ლარით მეტი). გამომდინარე აქედან, საარსებო შემწეობის პროგრამის ადმინისტრირებისათვის კრიტიკულად მნიშვნელოვანია, სააგენტოს შეეძლოს ბუნებრივი აირის მოხმარების შესახებ ინფორმაციის ვალიდაცია.

არსებული მდგომარეობით, ვინაიდან სააგენტოს არ შეუძლია ოჯახის მიერ მოწოდებული ინფორმაციის ვალიდაცია, არსებითია რისკები, რომ:

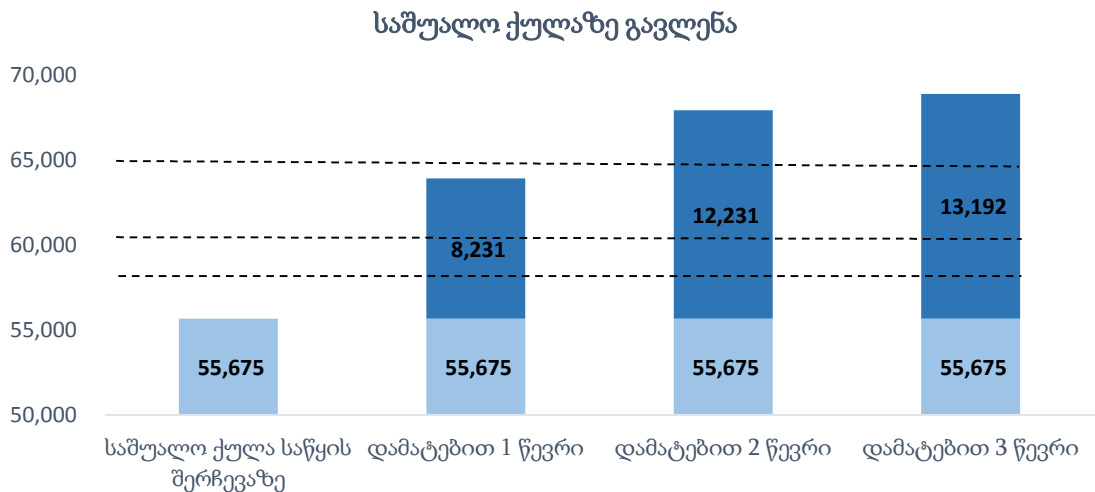
- › სააგენტო ვერ უზრუნველყოფს უფლებამოსილი მაძიებელი ოჯახისათვის კუთვნილი საარსებო შემწეობის დანიშვნას, მაძიებელი ოჯახის მიერ არაზუსტად, ზედმეტად დაფიქსირებული ბუნებრივი აირის გადასახადის შემთხვევაში;
- › მაძიებელ ოჯახს გააჩნია მოტივაცია სააგენტოს არ მიაწოდოს ზუსტი ინფორმაცია მოხმარებული ბუნებრივი აირის შესახებ და შეამციროს ფაქტობრივი გადახდების მაჩვენებლები, რაც გამოიწვევს სარეიტინგო ქულის შემცირებას. შესაბამისად, მოცემულ სიტუაციაში სააგენტო ვერ უზრუნველყოფს არაუფლებამოსილი ბენეფიციარისათვის საბიუჯეტო სახსრების ჩარიცხვის პრევენციას;
- › მაღალია რისკი, რომ ბუნებრივი აირის შესახებ მონაცემების მიღების შემდეგ, იდენტიფიცირებულ იქნება ბენეფიციარებისათვის ზედმეტად გადახდილი საბიუჯეტო სახსრები, რაც საბოლოო ჯამში გამოიწვევს აღნიშნული თანხების ლეგალიზების საჭიროებას. ამასთანავე, მაღალია რისკი, რომ მონაცემების მიღებისა და ვალიდაციის დაგვიანებით გაიზრდება ლეგალიზაციის თანხები.

2.1.3 განათლების დონის მაჩვენებლის გავლენა სარეიტინგო ქულაზე

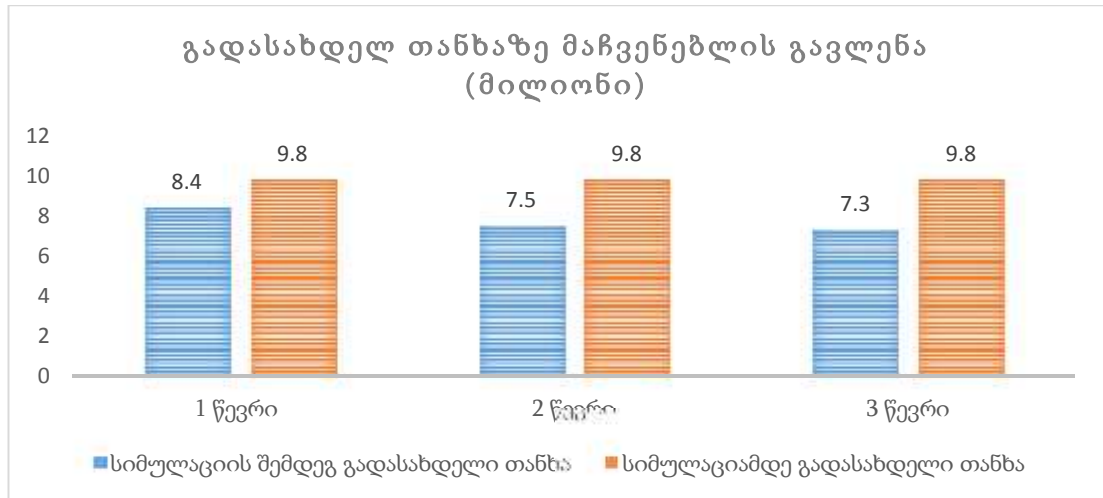
ბუნებრივი აირის მოხმარების ქულის გავლენის სიმულაციური ანალიზის მსგავსად, აუდიტის ჯგუფმა შეაფასა მამიებელი/ბენეფიციარი ოჯახის წევრების განათლების დონის მაჩვენებლის გავლენა სარეიტინგო ქულაზე, სხვა თანაბარ პირობებში. კერძოდ, აუდიტის ჯგუფის მიერ შეირჩა ახალი მეთოდოლოგიით გადაფასებული ბენეფიციარები (დეტალები იხ. დანართში №1). სარეიტინგო ქულის დათვლისას, გაითვალისწინება უმაღლესი განათლება მხოლოდ 22-დან 65 წლამდე ასაკის მქონე ბენეფიციარებში, შესაბამისად, სიმულაციური ანალიზისათვის შეირჩა აღნიშნულ დიაპაზონში მყოფი ბენეფიციარები.

სიმულაციური ანალიზის ფარგლებში აუდიტის ჯგუფმა შეაფასა, სხვა თანაბარ პირობებში, რა გავლენა ექნებოდა შერჩეული ოჯახების სარეიტინგო საშუალო ქულასა და გადასახდელ თანხაზე უმაღლესი განათლების მქონე წევრების დამატებას. კერძოდ, შეფასდა ოჯახის შემადგენლობაში 1, 2 და 3 წევრისათვის უმაღლესი განათლების არსებობა და მისი გავლენა. გრაფიკებზე: №2.3 და №2.4 წარმოდგენილია აღნიშნული ანალიზის შედეგები.

გრაფიკი № 2.3: საშუალო ქულის ცვლილება განათლების დონის მაჩვენებლის მიხედვით



გრაფიკი № 2.4: გადასახდელი თანხის ცვლილება განათლების დონის მაჩვენებლის მიხედვით¹⁴



მოცემული სიმულაციის შედეგები ცხადყოფს, რომ განათლების დონის მაჩვენებელი მნიშვნელოვან გავლენას ახდენს ოჯახის სარეიტინგო ქულასა და გადასახდელი თანხის მოცულობაზე (ერთი თვის განმავლობაში 1 წევრის შემთხვევაში ზედმეტად გადასახდელია 1.4 მილიონი ლარი, 2 წევრის შემთხვევაში - 2.3 მილიონი ლარი, 3 წევრის შემთხვევაში - 2.5 მილიონი ლარი). შესაბამისად, არსებითია რისკი, რომ მაძიებელმა ოჯახმა განზრახ დამალოს ოჯახის წევრების უმაღლესი განათლების შესახებ ინფორმაცია, რის შედეგადაც სააგენტო ვერ უზრუნველყოფს მხოლოდ უფლებამოსილი პირებისათვის სოციალური დახმარების დანიშვნას.

აღსანიშნავია, რომ განათლების დონის შესახებ ცენტრალიზებულად ინფორმაციის მიღება დაკავშირებულია ქვეყნის დონეზე არსებულ პრობლემებთან. კერძოდ, განათლების სამინისტროში არ არსებობს საქართველოს მოსახლეობის სრულყოფილი მონაცემთა ბაზა, რომლის მიხედვით შესაძლებელია პიროვნების უმაღლესი განათლების შესახებ უტყუარი ინფორმაციის მოპოვება. თუმცა აღსანიშნავია, რომ საქართველოს განათლების, მეცნიერების, კულტურისა და

¹⁴ სიმულაციამდე გადასახდელი თანხის შემთხვევაში არ არის გამოყენებული სააგენტოს მიერ ერთ კონკრეტულ თვეში ფაქტობრივად გადახდილი თანხა, არამედ დათვლილია სიმულაციამდე არსებული ქულის შემთხვევაში ბენეფიციარზე გადასახდელი თანხა.

სპორტის სამინისტრომ აღნიშნული მიმართულებით მნიშვნელოვანი ნაბიჯები გადადგა 2013 წლიდან.

2.2 ასაკის მაჩვენებლის გავლენა სარეიტინგო ქულაზე

სარეიტინგო ქულის დათვლის პროცესში ერთ-ერთი მნიშვნელოვანი კომპონენტია მაძიებელი/ბენეფიციარი ოჯახის წევრთა ასაკი. ქულის გამოთვლისა და შესაბამისად, საარსებო შემწეობის შესაბამისი თანხის გაცემისათვის მნიშვნელოვანია, რომ ინფორმაციული სისტემა იყენებდეს გადამოწმებულ მაჩვენებლებს.

სისტემაში ოჯახის დეკლარაციის ასახვის შემდეგ სააგენტოს ინფორმაციული სისტემა ავტომატურ რეჟიმში გამოითვლის მაძიებელი პირის ასაკს. სააგენტოში არსებული პრაქტიკის შესაბამისად, ბაზაში ოჯახის წევრების ასაკის ცვლილების პროცესი არ არის ავტომატური და დამოკიდებულია სოციალური აგენტის ვიზიტზე. გამომდინარე იქიდან, რომ ოჯახში სოციალური აგენტის განმეორებითი ვიზიტი 4 წელიწადში ერთხელ არის სავალდებულო, თუ რაიმე ცვლილება არ განხორციელდა ოჯახის სოციალურ-ეკონომიკურ მდგომარეობაში, ასაკის მაჩვენებელი ზოგიერთ შემთხვევაში არ შეესაბამება რეალობას.

შესაბამისად, ზემოთ განხილულ პრაქტიკას უარყოფითი გავლენა აქვს სარეიტინგო ქულის ადეკვატურ კალკულაციაზე. როგორც აღინიშნა, არის შემთხვევები, როდესაც მაძიებელი პირის ფაქტობრივი ასაკი უფრო მაღალია, ვიდრე ეს სისტემაშია დაფიქსირებული, რაც თავის მხრივ გავლენას ახდენს სხვადასხვა ფაქტორსა (შინამეურნეობის საჭიროების ინდექსი, დემოგრაფიული ინდექსი, ფაქტორები ასაკობრივი ზღვრები) და საბოლოოდ, ოჯახის სარეიტინგო ქულაზე.

არსებულ სიტუაციაში მნიშვნელოვანია იმის გათვალისწინება, რომ მარეგულირებელი დადგენილების¹⁵ შესაბამისად სარეიტინგო ქულა მყარი

¹⁵ საქართველოს მთავრობის №126 დადგენილება „ქვეყანაში სიღატაკის დონის შემცირებისა და მოსახლეობის სოციალური დაცვის სრულყოფის ღონისძიებათა შესახებ, 2010 წლის 24 აპრილი“.

ერთეულია და მისი შეცვლა შესაძლებელია მინიჭებიდან 1 წლის შემდეგ, მაგრამ ამავე დადგენილების ფარგლებში სააგენტო უფლებამოსილია რეაგირება მოახდინოს მიღებულ ინფორმაციაზე, რომელიც გავლენას ახდენს ოჯახის სარეიტინგო ქულაზე.

აუდიტის ჯგუფმა გადაითვალა სააგენტოს ინფორმაციულ სისტემაში არსებული სარეიტინგო ქულები ფაქტობრივი ასაკის გათვალისწინებით. ქულის გადათვლა ფაქტობრივი ასაკის გამოყენებით მოხდა ყველა ბენეფიციარისათვის, რომელთა გადაფასებაც განხორციელდა 2015 წლის 1 მაისიდან 2016 წლის 1 ოქტომბრამდე შუალედში, ახალი მეთოდოლოგიის ფარგლებში (დეტალები იხ. დანართში №1). საყურადღებოა, რომ შერჩევაში არ მოხვდნენ ისეთი ოჯახები, სადაც ერთ პირს მაინც უნდა შესრულებოდა საპენსიო ასაკი (რადგან ამ შემთხვევაში, ქულაზე ასაკობრივი კოეფიციენტის გარდა მოქმედებს პენსიაც).

შესწავლის შედეგად გამოვლინდა, რომ 110,258 ოჯახიდან 23,433 ოჯახისათვის, ფაქტობრივი ასაკის გათვალისწინების შემთხვევაში, შეიცვლებოდა სარეიტინგო ქულა. აღნიშნული ოჯახებიდან ქულის კატეგორია (ქულების რანჟირება იხ.: ზოგადი ინფორმაცია, ქვეთავი 1.5.2.4 – საარსებო შემწეობის ოდენობა და თანხის გაცემა) შეიცვლებოდა 1,796 ოჯახს (1,342 ოჯახს გაეზრდებოდა სარეიტინგო ქულა და შესაბამისად, გადავიდოდა სხვა ქულით კატეგორიაში, ხოლო 790 ოჯახს – შეუმცირდებოდა), რაც თავის მხრივ გამოიწვევდა საარსებო შემწეობის ოდენობის ცვლილებას.

დასკვნა

აუდიტის ჯგუფმა შეისწავლა საარსებო შემწეობის მაძიებელი და ბენეფიციარი ოჯახების სარეიტინგო ქულის გამოთვლის პროცესი. საკითხის შესწავლისას აუდიტის ჯგუფის ყურადღება დაეთმო სარეიტინგო ქულის დათვლისა და ვალიდაციისას გამოყენებული ინფორმაციის სიზუსტესა და დროულობას. შედეგად, გამოიკვეთა კონტროლის სისტემის და არსებული გარემო პირობების რიგი სუსტი მხარეებისა, რის გამოც, საარსებო შემწეობის გაცემის ბიზნესპროცესში ბენეფიციარების შესახებ განათლების დონისა და ბუნებრივი აირის მოხმარების შესახებ ინფორმაციის ვალიდაციის მექანიზმი არ არის ქმედითი, რაც უარყოფით

გავლენას ახდენს სარეიტინგო ქულის გამოთვლაზე. ასევე საარსებო შემწეობის ბიზნესპროცესში გამოყენებული აპლიკაციების კონტროლები ვერ უზრუნველყოფს დროთა განმავლობაში ბენეფიციარის ასაკის შესაბამისობას ფაქტობრივ მაჩვენებელთან.

არსებული კონტროლები ზემოთ აღნიშნულ შემთხვევებში გავლენას ახდენს ბენეფიციარების ადეკვატურ შეფასებაზე და რისკის ქვეშ აყენებს სოციალურად დაუცველი ოჯახების სარეიტინგო ქულის სიზუსტესა და ერთიანი ბაზის ფორმირებას.

შედეგად, ზემოაღნიშნული ფაქტორები გავლენას ახდენს გასაცემი საარსებო შემწეობის ოდენობაზე, რაც წარმოქმნის საბიუჯეტო რესურსების არასათანადოდ განკარგვის რისკს. ამასთანავე, მაღალია აღნიშნული თანხის ლეგალიზებისა და სახელმწიფოს მიერ ბიუჯეტში მისაღები ზედმეტად გადახდილი თანხების დათმობის რისკი.

ზემოთ აღნიშნული გარემოებების პირობებში, მნიშვნელოვანია სააგენტოს მიერ მოხდეს არსებული ნაკლოვანებების გაანალიზება და არსებული რესურსების პირობებში, ქულის მაქსიმალურად ადეკვატური გამოთვლის უზრუნველყოფა.

რეკომენდაცია

არსებული გამოწვევების პირობებში, სააგენტომ უზრუნველყოს სარეიტინგო ქულის ოდენობაზე გავლენის მქონე მონაცემების შესაძლო მაქსიმალური სიზუსტე. აღნიშნული მოიცავს შემდეგი მიმართულებების განვითარებას:

- › არსებული გამოწვევების პირობებში, ბუნებრივი აირის მოხმარებისა და განათლების დონის მაჩვენებლების შემთხვევაში მნიშვნელოვანია, სააგენტომ განიხილოს პრობლემის გადაჭრის სხვადასხვა გზები და შეიმუშაოს ქმედითი მექანიზმები ბენეფიციარის მიერ დეკლარირებული ინფორმაციის ვალიდაციისათვის;
- › სააგენტომ, არსებული რესურსების გათვალისწინებით, განიხილოს ქულის დათვლის პროცესში გამოყენებული ასაკის ველის შესაბამისობა არსებულ მდგომარეობასთან, კერძოდ, ქულის მუდმივი სისწორის უზრუნველსაყოფად, აპლიკაციაში შესაბამისი ბრძანების მოდიფიცირება, რომელიც პერიოდულად ან წელიწადში ერთხელ მაინც, განაახლებს ასაკის ველს.

2.3 ინფორმაციულ უსაფრთხოებასთან დაკავშირებული ნაკლოვანებები

საერთაშორისოდ აღიარებული პრაქტიკის მიხედვით, ინფორმაციული უსაფრთხოება წარმოადგენს ორგანიზაციის ფარგლებში არსებული ინფორმაციული სისტემის შესაძლებლობას, უზრუნველყოს ორგანიზაციის ინფორმაციული აქტივების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დაცვა შესაბამისი წესებისა და კონტროლის მექანიზმების გამოყენებით. ინფორმაციული უსაფრთხოება გულისხმობს არა მხოლოდ მონაცემთა დაცვას არაავტორიზებული წვდომისაგან, არამედ ავტორიზებული მომხმარებლების უზრუნველყოფას სერვისის მუდმივი ხელმისაწვდომობით. დიაგრამაზე №2.1 წარმოდგენილია ინფორმაციული უსაფრთხოების შემადგენელი კომპონენტები.

დიაგრამა № 2.1: ინფორმაციული უსაფრთხოების კომპონენტები



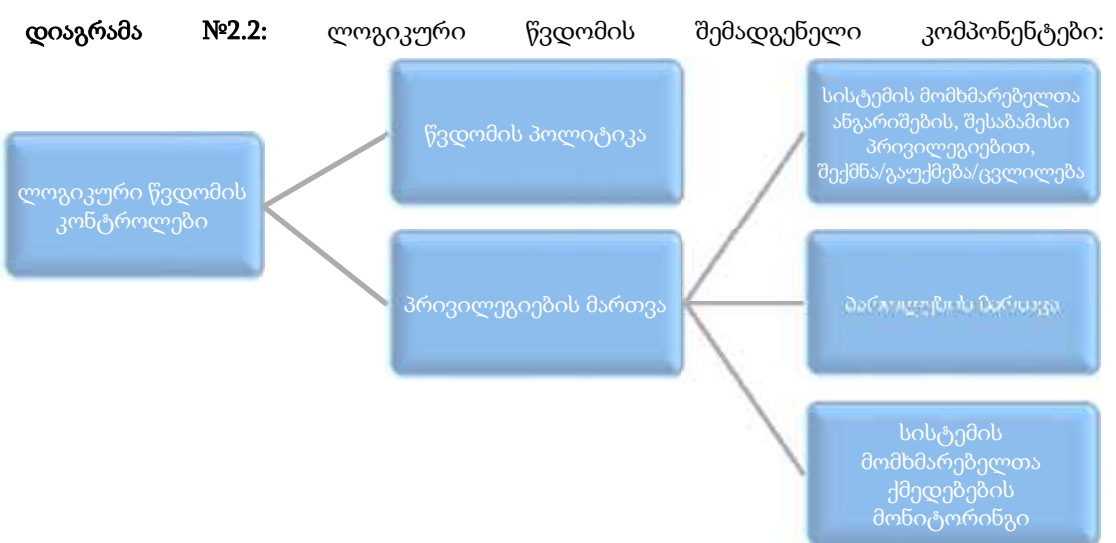
ინფორმაციული აქტივების დაცვა არაავტორიზებული წვდომის ან მოდიფიკაციისაგან უნდა მოხდეს მათი შენახვის, დამუშავებისა და გადაცემის ეტაპებზე. ორგანიზაცია, რომელიც შესაბამისად ვერ უზრუნველყოფს ინფორმაციულ უსაფრთხოებას, დგას ისეთი რისკების წინაშე, როგორიცაა, ინფორმაციაზე არაავტორიზებული წვდომა და ცვლილება, სენსიტიური ინფორმაციის გაჟონვა ან მოპარვა, რაც იწვევს მარეგულირებელი საკანონმდებლო

ნორმების დარღვევას, ორგანიზაციის რეპუტაციის შელახვას და შეუძლებელს ხდის ორგანიზაციული მიზნების მიღწევას.

ინფორმაციული უსაფრთხოების უზრუნველყოფისათვის ორგანიზაციამ უნდა შეიმუშაოს ეფექტიანი და ქმედითი ინფორმაციული უსაფრთხოების პოლიტიკა და პროცედურები, რომლებიც უზრუნველყოფს სტრუქტურირებული და ინფორმირებული გადაწყვეტილებების მიღებას ინფორმაციული ტექნოლოგიებისა და ინფორმაციული სისტემების მართვის პროცესში. აღნიშნული პრაქტიკა ხელს უწყობს ინფორმაციული უსაფრთხოების დარღვევასთან დაკავშირებული რისკების შემცირებასა და კონფიდენციალურობის, ხელმისაწვდომობისა და მთლიანობის პრინციპების უზრუნველყოფას ორგანიზაციაში.

2.3.1 სააგენტოს სისტემაზე ლოგიკური წვდომის კონტროლებთან დაკავშირებული ხარვეზები

ინფორმაციული უსაფრთხოების მინიმალური პირობების უზრუნველყოფისათვის ერთ-ერთ მნიშვნელოვან პირობას წარმოადგენს ორგანიზაციაში ლოგიკური წვდომის ეფექტიანი კონტროლების დანერგვა. დიაგრამაზე №2.2 წარმოდგენილია ლოგიკური წვდომის კონტროლების შემადგენელი კომპონენტები.

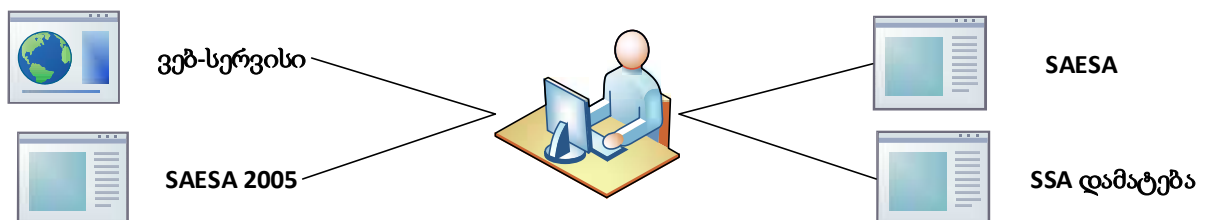


ლოგიკური წვდომის კონტროლები უზრუნველყოფს, რომ სისტემის მომხმარებლებს გააჩნდეთ ინფორმაციაზე ავტორიზებული წვდომა, რაც თავის მხრივ, ორგანიზაციას აძლევს რწმუნებას, რომ მინიმუმამდე შემცირდება მონაცემების წინასწარგანსაზღვრული, თუ უნებლიე მოდიფიცირება, დაკარგვა, გამჟღავნება ან განადგურება. ლოგიკური წვდომის კონტროლები მოიცავს სისტემისა და აპლიკაციის მომხმარებლების სავალდებულო ავტორიზაციას, ავთენტიფიკაციას და აძლევს მათ შესაბამისი პრივილეგიებით ოპერაციების განხორციელების საშუალებას.

ლოგიკური წვდომის კონტროლების სისუსტემ შესაძლოა გამოიწვიოს ინფორმაციული უსაფრთხოების მთავარი პრინციპების დარღვევა. ლოგიკური წვდომის კონტროლების ეფექტიანობისათვის მნიშვნელოვანია ორგანიზაციაში მკაფიოდ იყოს განსაზღვრული შესაბამისი პოლიტიკა და პროცედურები. აღნიშნულის ფარგლებში გამიჯნული უნდა იყოს ნებისმიერი თანამშრომლის ფუნქცია-მოვალეობები ამა თუ იმ პროცესში, რის საფუძველზე უნდა ხდებოდეს შესაბამისი წვდომის მინიჭება (მაგალითად, წაკითხვა, მოდიფიცირების შესაძლებლობა, წაშლა და სხვ.) სხვადასხვა აპლიკაციასა და სისტემაში¹⁶.

დიაგრამაზე №2.3 წარმოდგენილია ტერიტორიული ერთეულების თანამშრომლების მიერ საარსებო შემწეობის პროგრამის ადმინისტრირებაში გამოყენებული სისტემები.

დიაგრამა №2.3: საარსებო შემწეობის პროგრამის ადმინისტრირებაში ტერიტორიული ერთეულების მიერ გამოყენებული სისტემები.



¹⁶ US GAO, FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM), 2009 წელი.

აღნიშნული სისტემებისათვის მნიშვნელოვანია განსაზღვრული იყოს ლოგიკური წვდომის შესაბამისი კონტროლები, რომლებიც სხვა დანარჩენთან ერთად, მოიცავს ინდივიდუალური მომხმარებლების არსებობას, სისტემაში მათი ქმედების მონიტორინგის ადეკვატური სისტემის დანერგვასა და სხვა მნიშვნელოვან საკითხებს.

2.3.1.1 სააგენტოს თანამშრომლებს აქვთ მოვალეობის შესრულებისათვის საჭიროზე მეტი ინფორმაციაზე დაშვება

კონფიდენციალურობის პრინციპი გულისხმობს ინფორმაციაზე ავტორიზებული წვდომის მინიჭებას¹⁷. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი არეგულირებს პერსონალური მონაცემების დამუშავებისას ადამიანის უფლებების დაცვასა და პირადი ინფორმაციის გაუმჟღავნებლობის უზრუნველყოფას.

ზემოთ მითითებული მიზნების მისაღწევად, მნიშვნელოვანია, რომ ორგანიზაციამ სწორად შეაფასოს ინფორმაციის კატეგორია, რომელიც საჭიროა სისტემის მომხმარებლისათვის საკუთარი მოვალეობის შესრულებისას. კერძოდ, წვდომის უფლებები მომხმარებლებს უნდა მიენიჭოს მინიმალური პრივილეგიების პრინციპითა (Least Privilege Approach) და წვდომის უფლებების კონტროლის პოლიტიკის გათვალისწინებით¹⁸.

საკანონმდებლო მოთხოვნების არსებობის მიუხედავად¹⁹, სააგენტოს თანამშრომლებს დაშვება აქვთ ისეთ მოქალაქეთა პერსონალურ ინფორმაციაზე, რომელიც არ არის საჭირო საარსებო შემწეობის პროგრამის ადმინისტრირებისათვის.

კერძოდ, სააგენტო ყოველთვის იღებს განახლებულ ინფორმაციას სსიპ - შემოსავლების სამსახურიდან საქართველოს ყველა მოქალაქის დეკლარირებული

¹⁷ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის №2 ბრძანება „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“.

¹⁸ მონაცემთა გაცვლის სააგენტო, მგს 27002:2011 ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების მართვის წესები და ნორმები, 8 ნოემბერი, 2011 წელი.

¹⁹ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“.

შემოსავლების შესახებ²⁰, რომელიც განთავსდება სოციალურად დაუცველი მოსახლეობის ერთიან ბაზაში და გამოიყენება მაძიებლის ან ბენეფიციარის ინფორმაციის ვალიდაციის მიზნით. აღსანიშნავია, რომ აპლიკაციის მეშვეობით (SSA-დამატება), პირადი ნომრის მითითებით, შემოსავლების სრულ ბაზაზე წვდომა აქვს ტერიტორიული ერთეულის მიერ შესაბამისი ბრძანებით განსაზღვრულ თანამშრომელს - პრივილეგირებულ მომხმარებელს.

არსებული ბიზნესპროცესი და რეგულაციები არ მოითხოვს სააგენტოს პრივილეგირებული მომხმარებლების დაშვებას მონაცემებზე, რომელიც არ არის საჭირო სააგენტოს საქმიანობის განსახორციელებლად (ყველა მოქალაქის შემოსავლების შესახებ ინფორმაცია). შესაბამისად, სააგენტოს თანამშრომლების მხრიდან არსებითია ზემოთ მითითებულ პერსონალურ ინფორმაციაზე არაავტორიზებული დაშვების რისკი.

დამატებით საყურადღებოა, რომ პრივილეგირებული მომხმარებლების არსებითი რაოდენობა ზრდის კონფიდენციალური ინფორმაციის არაავტორიზებული წვდომის რისკს. ამასთანავე, ტერიტორიულ ერთეულებში არ არის ერთიანი მიდგომა, რომლის ფარგლებში განისაზღვრება მომხმარებელთა დონეები, რომელთაც წვდომა უნდა ჰქონდეთ შემოსავლების ბაზაზე.

2.3.1.2 ლოგირებასა და მიკვეთებადობასთან დაკავშირებული ხარვეზები

მოვალეობის შესრულებისათვის საჭიროზე მეტ ინფორმაციაზე დაშვებისა და მომხმარებელთა ავტორიზაციასთან დაკავშირებული ხარვეზების მაკომპენსირებელი კონტროლია ლოგირების სისტემის დანერგვა, თუმცა სააგენტოს არ გააჩნია საარსებო შემწეობის ადმინისტრირების პროცესში გამოყენებული ინფორმაციული სისტემების ლოგირების ადეკვატური მექანიზმი.

სისტემის ლოგების წარმოება და მისი მუდმივი მონიტორინგი საჭიროა ინფორმაციის დამუშავებისას არაავტორიზებული ქმედებების აღმოჩენისათვის. სისტემის მონიტორინგი უნდა გამოიყენებოდეს იმ მიზნით, რომ შემოწმდეს

²⁰ აღნიშნულ ბაზაში არ ფიქსირდებიან მხოლოდ იმ სამსახურის თანამშრომლები, რომლებიც საკუთარ სახელფასო განაკვეთებს კონფიდენციალურ სტატუსს ანიჭებენ, მაგალითად, შინაგან საქმეთა სამინისტრო.

კონტროლის დამტკიცებული მექანიზმების ეფექტიანობა და აგრეთვე წვდომის
არსებული პრაქტიკა²¹.

სააგენტოში აპლიკაციებისათვის (ვებგვერდი) შექმნილი და დანერგილი
ლოგირების მექანიზმის საშუალებით, შესაძლებელია აპლიკაციაში
დაფიქსირებული ოპერაციის დაკავშირება მხოლოდ კონკრეტულ პროგრამასა
(საყოველთაო ჯანდაცვა, სოციალური დაცვა და ა.შ.) და კონკრეტულ IP
მისამართთან. თუმცა, აღსანიშნავია, რომ ქსელში ჩართული მომხმარებლის
კომპიუტერისათვის IP მისამართის მინიჭება ხდება დინამიკურად (ცვალებადია),
რაც ართულებს ან ზოგჯერ შეუძლებელს ხდის კონკრეტული მომხმარებლის
იდენტიფიკაციას.

ასევე აღსანიშნავია, რომ აპლიკაციებისათვის (SAESA, SAESA2005, SSA-დამატება)
მიუხედავად იმისა, რომ არსებობს ლოგირების გარკვეული მექანიზმები, არ
ხორციელდება მომხმარებელთა ქმედების მონიტორინგი. კერძოდ კი, სააგენტოს
არ ჰყავს განსაზღვრული პირი, რომელიც ვალდებული იქნება მონიტორინგი
გაუწიოს მომხმარებლების ქმედებებს.

სააგენტოში არსებული პრაქტიკა და კონტროლის მექანიზმები ვერ
უზრუნველყოფს ინფორმაციული უსაფრთხოების პრინციპების დაცვას. კერძოდ,
საჭიროების შემთხვევაში არ არის მიკვლევადი, რომელი მომხმარებლის მიერ
მოხდა სენსიტიური ინფორმაციის, მოთხოვნა. შედეგად, ინფორმაციული
უსაფრთხოების დარღვევისას, რთულია და რიგ შემთხვევაში შეუძლებელია
გამომწვევი წყაროს იდენტიფიცირება.

²¹ მონაცემთა გაცვლის სააგენტო, ინფორმაციული უსაფრთხოება - უსაფრთხოების
მექანიზმები - ინფორმაციული უსაფრთხოების მართვის წესები და ნორმები, მგს
27002:2011, 8 ნოემბერი, 2016.

2.3.1.3 აპლიკაციის მომხმარებელთა მართვასთან და პერსონიფიცირებული მომხმარებლის არსებობასთან დაკავშირებული ხარვეზები

ბიზნესპროცესში გამოყენებული აპლიკაციის მეშვეობით შესაძლებელი უნდა იყოს სხვადასხვა დონის მომხმარებლების იდენტიფიცირება²². ინფორმაციულ სისტემაში განხორციელებული კონკრეტული აქტივობა დაკავშირებული უნდა იყოს კონკრეტულ მომხმარებელთან და შესაძლებელი იყოს თითოეული აქტივობის განმახორციელებელი პირის იდენტიფიცირება. საკანონმდებლო და უსაფრთხოების მოთხოვნებიდან გამომდინარე, მნიშვნელოვანია, კონტროლდებოდეს არსებულ ინფორმაციაზე წვდომა. დამატებით, მიზანშეწონილია არსებობდეს მომხმარებელთა რეგისტრაციისა და მათი ანგარიშების გაუქმების ფორმალური პროცედურები. თუმცა, აუდიტის მიმდინარეობისას, სააგენტოში დანერგილი შიდა კონტროლის მექანიზმები ვერ აკმაყოფილებდა ზემოთ მითითებულ მოთხოვნებს.

SAESA აპლიკაციების მომხმარებელთა მართვასთან დაკავშირებული ხარვეზები

სააგენტოს მიერ საარსებო შემწეობის გაცემის ბიზნესპროცესში გამოყენებულ აპლიკაციებში (SAESA 2005, SAESA, SSA-დამატება) განსაზღვრულია სხვადასხვა სახის მომხმარებელი (user), სხვადასხვა წვდომის უფლებით. თუმცა, ტერიტორიულ ერთეულებში არ არის ყველა თანამშრომლისათვის განსაზღვრული ინდივიდუალური მომხმარებლის ანგარიშები. შესაბამისად, თანამშრომლები სარგებლობენ საერთო/საზიარო მომხმარებლის ანგარიშით, რომელიც ცნობილია ყველა ჩართული მხარისათვის.

აღსანიშნავია, რომ აუდიტის პერიოდში, მხოლოდ შესაბამისი აუდიტორული პროცედურების განხორციელების შემდეგ, სააგენტოს ინფორმაციული ტექნოლოგიების დეპარტამენტის წერილის²³ საფუძველზე, სააგენტოს

²² მგს 27002:2011, ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების მართვის წესები და ნორმები, მონაცემთა გაცვლის სააგენტო.

²³ სოციალური მომსახურების სააგენტოს ინფორმაციული ტექნოლოგიების დეპარტამენტის უფროსის წერილი (რეგისტრაციის ნომერი და თარიღი: N04/31785; 18.05.2017).

ტერიტორიულ ერთეულებს დაევალებათ დოკუმენტურად განესაზღვრათ SAESA აპლიკაციებში თითოეული თანამშრომლისათვის საჭირო პრივილეგიების აღრიცხვა და ინფორმაციული ტექნოლოგიების დეპარტამენტისათვის მიწოდება. აღნიშნული პრივილეგიების საფუძველზე კი თითოეულ თანამშრომელს აპლიკაციაში მიენიჭებოდა ინდივიდუალური მომხმარებლის ანგარიში, რომელიც უნიკალური იქნებოდა და ის გამოყენებულ იქნებოდა შესაბამისი უფლებამოსილი პირის მიერ.

აუდიტის მიმდინარეობისას აღნიშნული მოთხოვნა – ყველასთვის შექმნილიყო ინდივიდუალური მომხმარებლის ანგარიში, არ ყოფილა დანერგილი და ტერიტორიულ ერთეულებში კვლავ არსებობდა მომხმარებლის ანგარიში, რომლის გამოყენება ყველა თანამშრომელს შეეძლო.

ვებგვერდისათვის პერსონიფიცირებული მომხმარებლის არარსებობა

სააგენტოს ტერიტორიულ ერთეულებში შემწეობის მაძიებელი/ბენეფიციარი ან სხვა ოჯახის შესახებ პერსონალური ინფორმაციის გადამოწმებისათვის SAESA აპლიკაციებთან ერთად გამოიყენება ვებგვერდი, რომელიც განკუთვნილია მხოლოდ შიდა მომხმარებლისათვის.

აღნიშნული სერვისი საბოლოო მომხმარებლისათვის წარმოადგენს საშუალებას, პირადი ნომრის მითითებით მოძებნოს კონკრეტულ პიროვნებაზე შემდეგი სახის პერსონალური ინფორმაცია: მისამართი, სახელი, გვარი, დაბადების თარიღი, მოქალაქეობა, სახელმწიფო გასაცემლები, სტატუსი სოციალურად დაუცვეულობის შესახებ, პირის დაზღვევისა და დევნილობის სტატუსის შესახებ. აღსანიშნავია, რომ სერვისის გამოყენებით ინფორმაციის ნახვა შესაძლებელია არა მხოლოდ ბენეფიციართა ან შემწეობის მაძიებელთა შესახებ, არამედ საქართველოს ყველა მოქალაქის შესახებ.

მიუხედავად იმისა, რომ გამჭვირვალობისა და ანგარიშვალდებულების პრინციპების უზრუნველსაყოფად მნიშვნელოვანია თითოეული განხორციელებული ქმედების კონკრეტულ საბოლოო მომხმარებელთან დაკავშირება, აღნიშნულ სერვისზე წვდომისათვის არ არის მოთხოვნილი ინდივიდუალური მომხმარებლის არსებობა. აღნიშნული იწვევს სერვისის

ხელმისაწვდომობას ტერიტორიული ერთეულის ყველა თანამშრომლისათვის, მიუხედავად მათი მოვალეობებისა.

პერსონიფიცირებული მომხმარებლების არარსებობის პირობებში, არ არის მიკვლევადი ცალკეული მომხმარებლის მიერ აღნიშნულ პორტალზე და აპლიკაციის მეშვეობით განხორციელებული ქმედება. შესაბამისად, შეუძლებელია მომხმარებელთა ქმედების მონიტორინგის განხორციელება.

ზემოთ აღნიშნული შემთხვევების გათვალისწინებით, სააგენტო ვერ უზრუნველყოფს ინფორმაციის კონფიდენციალურობის პრინციპის დაცვას. აღნიშნული გამოწვეულია იმ ფაქტით, რომ მკაფიოდ არ არის განსაზღვრული კონკრეტულ ინფორმაციაზე ავტორიზებული მომხმარებლები და არ ხდება მხოლოდ საქმიანობისათვის საჭირო ინფორმაციაზე წვდომის მინიჭება.

ასევე აღსანიშნავია, რომ სააგენტოში არ არსებობს ერთიანი მიდგომა და წინასწარ განსაზღვრული ფორმალური პროცედურები მომხმარებელთა რეგისტრაციისა და მათი ჩანაწერის გაუქმებისათვის. კერძოდ, არსებული პრაქტიკიდან გამომდინარე, მომხმარებლის ანგარიში შესაძლოა შექმნას როგორც სააგენტოს ინფორმაციული ტექნოლოგიების დეპარტამენტმა, ასევე ტერიტორიული ერთეულის ტექნიკური უზრუნველყოფის თანამშრომელმა.

აუდიტის ობიექტის განმარტებით²⁴ პერსონიფიცირებული მომხმარებლის არარსებობასთან დაკავშირებული ხარვეზები აღმოფხვრილია აუდიტორული პროცედურების დასრულების შემდეგ.

²⁴ სსიპ – სოციალური მომსახურების სააგენტოს დირექტორი, საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის მინისტრის მოადგილის წერილი (რეგისტრაციის ნომერი და თარიღი: №04/41495, 19.07.2018).

2.3.1.4 წვდომის კონტროლების სისუსტე - სააგენტოში არ არსებობს მოთხოვნები პაროლების სირთულეზე

პაროლი წარმოადგენს მომხმარებლების ნამდვილობის შესამოწმებელ საშუალებას მანამ, სანამ მათ მიეცემათ წვდომა ინფორმაციულ სისტემაზე ან მომსახურებაზე²⁵. სისტემის მომხმარებლებს უნდა მოეთხოვოთ საუკეთესო პრაქტიკის დაცვა პაროლების შერჩევისა და გამოყენების დროს, რათა ორგანიზაციამ უზრუნველყოს არავტორიზებული წვდომის მინიმუმამდე შემცირება და კონფიდენციალურ ინფორმაციაზე დაშვება. საუკეთესო პრაქტიკის მიხედვით, პაროლების მართვის კონტროლი უნდა მოიცავდეს პაროლის სირთულის მინიმალურ მოთხოვნებს, პაროლის განახლების ვადას, შეზღუდვებს იმავე პაროლის გამოყენებასთან დაკავშირებით და მცდარი პაროლის რამდენჯერმე გამოყენების შემთხვევაში, სისტემის დაბლოკვის ფუნქციას.

სააგენტოს ტერიტორიულ ერთეულებში ვიზიტის ფარგლებში, დაკვირვების შედეგად აუდიტის ჯგუფმა გამოავლინა, რომ სააგენტოს არ აქვს ძლიერი პაროლების მოთხოვნები აპლიკაციის მომხმარებლების მიმართ. კერძოდ, სააგენტოს თანამშრომლების მიერ სისტემასთან დაკავშირებისათვის ხდება სუსტი და მცირე რაოდენობის სიმბოლოიანი პაროლების გამოყენება.

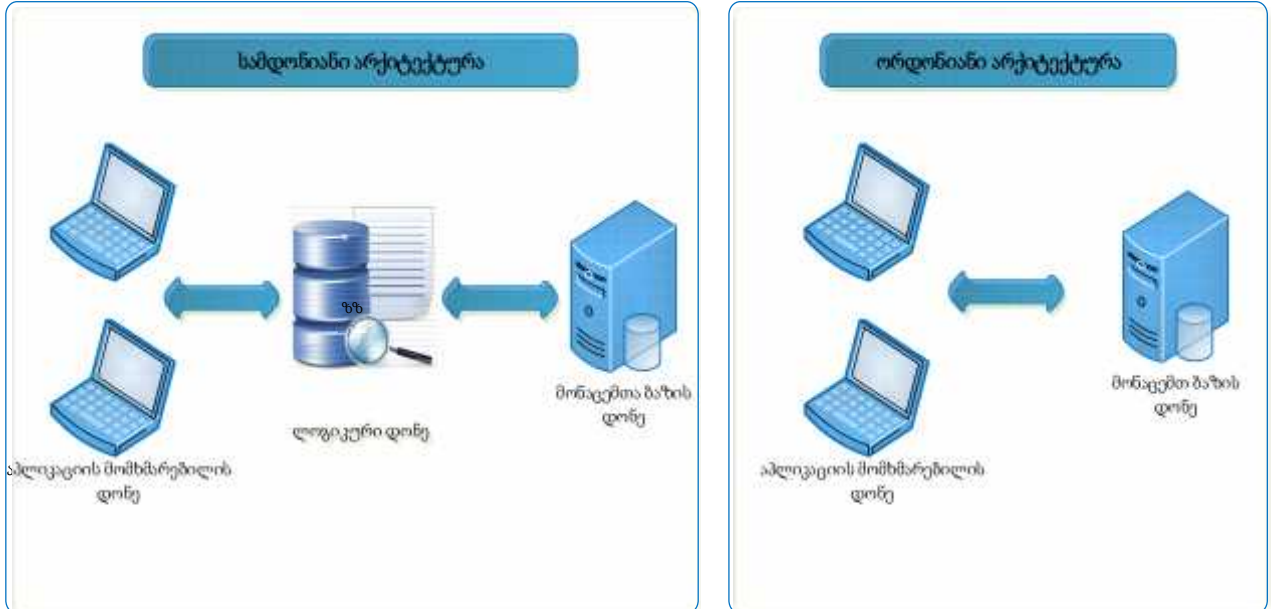
2.3.1.5 სისტემის არქიტექტურასთან დაკავშირებული რისკები

ტერიტორიული ერთეულები სოციალურად დაუცველი მოსახლეობის ბაზასთან დასაკავშირებლად იყენებენ 2-დონიან (Tier 2) აპლიკაციას (იხ. 1.5 ზოგადი ინფორმაცია ბიზნესპროცესში გამოყენებული სისტემები). 2- დონიანი აპლიკაცია 3 - დონიანისაგან (Tier 3) განსხვავებით, გულისხმობს აპლიკაციის მომხმარებლის პირდაპირ (შუალედური რგოლის გარეშე) წვდომას მონაცემთა ბაზასთან. შესაბამისად, საბოლოო მომხმარებელს, ყოველგვარი დამცავი დონის გარეშე, წვდომა აქვს სოციალურად დაუცველი მოსახლეობის ერთიან ბაზასთან, სადაც განთავსებულია მოქალაქეთა პერსონალური ინფორმაცია. სურათზე №2.1

²⁵ მგს 27002:2011, ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების მართვის წესები და ნორმები, მონაცემთა გაცვლის სააგენტო.

შედარებისათვის წარმოდგენილია 2-დონიანი და 3-დონიანი არქიტექტურის მოდელები.

სურათი №2.1: 2-დონიანი და 3-დონიანი არქიტექტურის მოდელები



იმის გათვალისწინებით, რომ აპლიკაციის მომხმარებლის დონე პირდაპირ უკავშირდება მონაცემთა ბაზას, აღნიშნული არქიტექტურა ვერ უზრუნველყოფს სააგენტოში არსებულ მონაცემთა ადეკვატურ დაცვას. კერძოდ, 2-დონიანი აპლიკაციის შემთხვევაში მომხმარებლის მხრიდან მარტივადაა შესაძლებელი მონაცემთა ბაზაზე შეტევის განხორციელება და იქ არსებული კონფიდენციალური ინფორმაციის მიტაცება, განადგურება ან შეცვლა. აღნიშნული გამოწვეულია იმით, რომ ამ შემთხვევაში არ არსებობს შუალედური, ლოგიკური დონე, სადაც უნდა მოხდეს ასეთი საფრთხის შეცველი მოთხოვნების გაფილტვრა. გარდა ამისა, ბაზას საფრთხე შეიძლება შეექმნას მესამე/არასანქცირებულ პირთა მხრიდან, გამომდინარე იქიდან, რომ სააგენტოში დანერგილი პაროლები არ აკმაყოფილებს პაროლების მინიმალურ მოთხოვნებს და მარტივადაა შესაძლებელი საბოლოო მომხმარებლის ანგარიშზე არასანქცირებული წვდომა, შემდეგ კი ბაზაში არსებული კონფიდენციალური მონაცემების დაკარგვა/ცვლილება.

2.3.2 ოპერაციული სისტემებისა და მონაცემთა ბაზების მართვის სისტემის მოწყვლადობის ტესტირება

ინფორმაციული სისტემის მოწყვლადობის შეფასების (vulnerability assessment) პროცედურის მიზანია გამოავლინოს სისტემის სისუსტეები და შეაფასოს მასთან დაკავშირებული საფრთხეების დონე. აღნიშნული პროცედურა შესაძლოა ჩატარდეს როგორც სპეციალური პროგრამული ინსტრუმენტის (tool) საშუალებით, ასევე გამოცდილი სპეციალისტის მიერ შედგენილი ტესტების საშუალებით. ტესტირების შედეგად, ინფორმაციული სისტემის შესახებ იდენტიფიცირებული მოწყვლადობების საპასუხოდ, მზადდება შესაბამისი რეკომენდაციები.

სამინისტროსა და სააგენტოს შორის ჩამოყალიბებულია „ინფრასტრუქტურა, როგორც სერვისი“ (IAAS') - აუთოსინგის მოდელი. სერვერისა და მასზე განთავსებული მონაცემთა ბაზის მართვის სისტემის ადმინისტრირებას ახორციელებს სააგენტოს ინფორმაციული ტექნოლოგიების დეპარტამენტი, ხოლო სერვერის ვირტუალური მანქანისა და გამოთვლითი რესურსების მართვას - სამინისტროს ინფორმაციული ტექნოლოგიების დეპარტამენტი.

აუდიტის მიზნებიდან გამომდინარე, სისტემის მოწყვლადობის ტესტირების ჩასატარებლად შეირჩა ვირტუალური სერვერი, რომელზეც სხვა ბაზებთან ერთად განთავსებულია სოციალურად დაუცველი ოჯახების ერთიანი ბაზა. პროცედურის დაგეგმვის საწყის ეტაპზე, სააგენტოსა და სამინისტროს IT დეპარტამენტების წარმომადგენლებს, აუდიტის ჯგუფმა გააცნო ტესტირების მასშტაბი და ხასიათი. შედეგად, განისაზღვრა ტესტირებისთვის საჭირო ინფორმაცია, რომელიც მოწოდებულ იქნა სამინისტროს სისტემური ადმინისტრატორის მიერ.

კერძოდ, პროცედურისათვის შერჩეულ სერვერზე ინსტალირებული იყო:

- › Microsoft Windows server 2003 - ოპერაციული სისტემა;
- › Microsoft SQL 2005 - მონაცემთა ბაზების მართვის სისტემა;
- › განუახლებელი ანტივირუსი - Kaspersky.

შეხვედრისას განხილული საკითხებისა და მოწოდებული ინფორმაციის გათვალისწინებით, აუდიტის ჯგუფმა შეიმუშავა მოწყვლადობის ტესტირების პროცედურის აღწერილობა, რომელშიც განსაზღვრულია:

- › ტესტირების არეალი;
- › ტესტირების მეთოდები;
- › ტესტირების ინსტრუმენტები;
- › მხარეთა უფლება-მოვალეობა;
- › თანდაყოლილი რისკები.

ამასთანავე, აუდიტის ჯგუფის ყურადღება მიიპყრო ტესტირებისათვის შერჩეული სერვერის ოპერაციული სისტემისა და მონაცემთა ბაზების მართვის სისტემის ძველმა ვერსიებმა. საყურადღებოა, რომ ზემოაღნიშნული ვერსიების მხარდაჭერას აღარ აწარმოებს Microsoft (მწარმოებელი), ხოლო Microsoft-თან გაფორმებული სამთავრობო ხელშეკრულების²⁶ ფარგლებში სამინისტროსა და სააგენტოს შესყიდული ჰქონდა ახალი ვერსიის პროგრამული პაკეტი²⁷. დამატებით, ზემოაღნიშნულ მონაცემთა ბაზის მართვის სისტემაში იდენტიფიცირებულ იქნა 80-ზე მეტი სხვადასხვა ბაზა²⁸. შედეგად, ტესტირებისთვის შერჩეული სერვერი შეფასდა მაღალი რისკის მქონე ინფორმაციულ სისტემად.

მოწყვლადობის ტესტირების პროცედურების დაგეგმვის პროცესში, სააგენტოს IT დეპარტამენტის მენეჯმენტს განემარტა ტესტირების დეტალები, მასთან დაკავშირებული პროცედურები, გამოსაყენებელი ინსტრუმენტები და აუდიტორების კვალიფიკაცია. თუმცა სააგენტოს IT მენეჯმენტმა არ მისცა საშუალება აუდიტის ჯგუფს დროულად ჩაეტარებინა დაგეგმილი პროცედურა.

²⁶ საქართველოს მთავრობასა და კომპანია Microsoft-ს შორის 2015 წელს გაფორმებული ხელშეკრულება. წყარო: <http://www.license.gov.ge/>

²⁷ Microsoft SQL Server Enterprise. წყარო: <http://www.license.gov.ge/>

²⁸ სააგენტოს წარმომადგენლების განმარტებით, ბაზების დიდი ნაწილი მემკვიდრეობითი ბაზებია, რომლებიც აქტიურ სისტემებში აღარ გამოიყენება, თუმცა საჭიროა ძველი მონაცემების მიღებისა და ვალიდაციისათვის.

ტესტირების დაწყებამდე, პროცედურის შეთანხმებულ დროს, აუდიტის ჯგუფმა აღმოაჩინა, რომ შერჩეული სერვერის ოპერაციული სისტემის, მონაცემთა ბაზის მართვის სისტემისა და ანტივირუსული პროგრამული უზრუნველყოფის ვერსიები არ ემთხვეოდა წინასწარ შესწავლილ ვერსიებს. როგორც ანალიზისას გაირკვა, სააგენტოსა და სამინისტროს IT დეპარტამენტების თანამშრომლებმა ტესტირების პროცედურამდე 4 დღით ადრე დააყენეს ოპერაციული სისტემისა და მონაცემთა ბაზების მართვის სისტემის ახალი ვერსია (Microsoft Windows Server 2012 R2, Microsoft SQL Server), რის შემდეგ გადაიტანეს მონაცემები ძველი სერვერიდან ახალზე. აღნიშნული საკითხი არ იყო ცნობილი აუდიტის ჯგუფისათვის და შესაბამისად, შეცვლილ გარემოსა და ტექნიკური პარამეტრების პირობებში აუდიტის ჯგუფმა ვეღარ შეაფასა აუდიტის პერიოდში გამოყენებული სერვერების ოპერაციული სისტემების უსაფრთხოება/დაცულობა. კერძოდ:

- › სერვერის ოპერაციული სისტემის, მონაცემთა ბაზის მართვის სისტემისა და ანტივირუსული პროგრამული უზრუნველყოფის განახლების შედეგად შეუძლებელი გახდა აუდიტის მასშტაბით გათვალისწინებულ პერიოდში მოქმედი მონაცემთა ბაზის უსაფრთხოების გარემოზე შეფასების გაკეთება. ამასთანავე საყურადღებოა, რომ ზემოთ მითითებული სისტემების მართვა წარმოადგენს დინამიურ პროცესს და გარემო იცვლება სისტემის კონფიგურაციის მახასიათებლების შეცვლისას.

ამრიგად, ზემოაღნიშნულზე დაყრდნობით:

1. სააგენტოს IT დეპარტამენტის მენეჯმენტმა ვერ უზრუნველყო კანონით დაკისრებული ვალდებულების შესრულება და შეაფერხა²⁹ აუდიტის პროცედურები, ხოლო საბოლოოდ აუდიტის პროცედურის ჩატარება შეუძლებელი გახდა აუდიტის მასშტაბით გათვალისწინებული საკითხების შესწავლა.
2. სააგენტოს კრიტიკული ინფორმაციული სისტემების უსაფრთხოებისათვის, არსებითად მნიშვნელოვანია სააგენტოს IT დეპარტამენტის

²⁹ სახელმწიფო აუდიტის შესახებ კანონი, მუხლი 23, აუდიტის ობიექტის უფლებები და მოვალეობები.

მენეჯმენტის კვალიფიკაციის ამაღლება. კერძოდ, ტესტირების პროცედურების დაგეგმვისას, დეპარტამენტის მენეჯმენტის მხრიდან არასათანადოდ და არაზუსტად იქნა შეფასებული დაგეგმილი პროცედურის მიერ მოსატანი სარგებელი და მის ჩატარებასთან დაკავშირებული რისკები. ამასთანავე, მენეჯმენტის მიერ მიღებული გადაწყვეტილება სისტემების განახლების შესახებ და ჩატარებული პროცედურები ცალსახად ხასიათდება ინფორმაციული უსაფრთხოების მაღალი რისკებით.

3. აუდიტის ჯგუფი ვერ გამოთქვამს მოსაზრებას სააგენტოს სერვერზე არსებული აუდიტის მასშტაბით გათვალისწინებული ინფორმაციის დაცულობის შესახებ. აღნიშნული სისტემა წლების მანძილზე ფუნქციონირებდა (ზუსტი პერიოდი ვერ იქნა მოპოვებული) მოძველებულ ვერსიაზე, რომელიც შესაძლოა მოწყვლადი იყო სხვადასხვა ცნობილი საფრთხეების მიმართ³⁰. ამასთანავე, აუდიტის ჯგუფი მიიჩნევს, რომ მაღალია ზემოაღნიშნული სისტემის დაინფიცირების რისკი, რაც მოიცავს სისტემაში მავნე კოდის არსებობას, ჯამშურ პროგრამებსა და სხვადასხვა ვირუსებს. შესაბამისად, მოწყვლადობის ტესტირების მიზანი იყო შესწავლილ იყო სისტემასთან დაკავშირებული ანომალიები და გაანალიზებულიყო პოტენციური საფრთხეების წარმომავლობა, ხასიათი და გაცემულიყო შესაბამისი რეკომენდაციები. თუმცა, სააგენტოს IT დეპარტამენტის მენეჯმენტის გადაწყვეტილების შედეგად, განადგურდა ზემოთ მითითებული ციფრული კვალი და შესაბამისად, აუდიტის ჯგუფი ვერ გამოთქვამს მოსაზრებას, თუ რამ განაპირობა აღნიშნული გადაწყვეტილება და რამდენად იყო მოწყვლადი ძველი ოპერაციული სისტემა.

4. საქართველოს მთავრობასა და კომპანია Microsoft-ს შორის გაფორმებული ხელშეკრულების ფარგლებში, სამინისტროსთვის განსაზღვრული **Microsoft SQL Server-ის** ლიცენზიების წლიური ღირებულება შეადგენს 119,850 აშშ დოლარს. ხელშეკრულების მოქმედების 3-წლიან პერიოდში აღნიშნული ლიცენზიების ჯამური ღირებულებაა 359,550 აშშ დოლარი. ანალოგიურად, Microsoft Windows Server-ის ლიცენზიის მოქმედების 3- წლიან პერიოდში გამოყოფილია 102,915 აშშ

³⁰ აუდიტის მიმდინარეობისას, მსოფლიოს მრავალ ქვეყანაში გავრცელდა გამომძაღველი „კრიპტო ვირუსი“ (Ransomware), რომელმაც დააინფიცირა, მაგალითად, ბრიტანეთის ჯანდაცვის სისტემები.

დოლარი³¹. თუმცა, როგორც აუდიტის მიმდინარეობისას გაირკვა, შესასწავლი სერვერი და მონაცემთა ბაზა იყენებდა ძველ ვერსიებს. შესაბამისად, სამინისტროს მიერ შესყიდული პროდუქტები არ იყო გამოყენებული აუდიტისას შესწავლილი სისტემებისათვის.

2.3.3 სააგენტოს არ აქვს შემუშავებული ინფორმაციული უსაფრთხოების მართვის სისტემა

სააგენტოს, როგორც კრიტიკული ინფორმაციული სისტემის სუბიექტს³², ევალება³³ ინფორმაციული უსაფრთხოების მართვის სისტემის (შემდგომში - იუმს) შექმნა.

იუმს წარმოადგენს მართვის სისტემის ნაწილს, რომელიც დაფუძნებულია ბიზნესის რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონირება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება. იუმს-ის ფარგლებში ორგანიზაციამ უნდა შეიმუშაოს ინფორმაციული უსაფრთხოების პოლიტიკა და დანერგოს კონტროლის მექანიზმები ინფორმაციის კონფიდენციალურობის, ხელმისაწვდომობისა და მთლიანობის უზრუნველსაყოფად. ამასთანავე, კრიტიკული ინფორმაციული სისტემის სუბიექტები ვალდებული არიან ორგანიზაციულად განსაზღვრონ ინფორმაციული უსაფრთხოების მართვის განხორციელებაზე პასუხისმგებელი პირი ან პირები³⁴.

მონაცემთა გაცვლის სააგენტომ, როგორც აღნიშნული მიმართულების კოორდინატორმა უწყებამ, შეაფასა კრიტიკული ინფორმაციული სისტემის სუბიექტების, მათ შორის, სააგენტოს მიმდინარე მდგომარეობა იუმს-ის კრილში.

³¹ წყარო: <http://www.license.gov.ge/>

³² საქართველოს მთავრობის 2014 წლის 29 აპრილის №312 დადგენილება „კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ“.

³³ საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“.

³⁴ მაგალითად, ინფორმაციული უსაფრთხოების საბჭო, რომელიც შედგება ინფორმაციული უსაფრთხოების მენეჯერისა და საკვანძო, დარგობრივი ან მიმართულების ხელმძღვანელი პირებისაგან.

მინიმალური მოთხოვნების შესრულების შესახებ სააგენტოს შედეგები წარმოდგენილია ქვემოთ მოყვანილ ცხრილში³⁵.

ცხრილი №2.1: სოციალური მომსახურების სააგენტოს მიერ მინიმალური მოთხოვნების შესრულების შესახებ მონაცემთა გაცვლის სააგენტოს მონაცემები

მოთხოვნები	შესრულების მდგომარეობა
ინფორმაციული უსაფრთხოების მენეჯერი	✓
კომპიუტერული უსაფრთხოების სპეციალისტი	×
ორგანიზაციაში ინფორმაციული უსაფრთხოების აუცილებლობის გაცნობიერება და ხელმძღვანელობის მხრიდან მხარდაჭერა	×
ორგანიზაციული მოწყობა (ინფორმაციული უსაფრთხოების საბჭო)	×
გავრცელების სფერო	×
იუმს-ის პოლიტიკა	×
აქტივების მართვა	×
რისკების მართვა	×
კონტროლის მექანიზმების გამოყენებადობის განაცხადი	×
ორგანიზაციის მიერ იუმს-ის დოკუმენტაციის მართვა	×

როგორც ზემოთ წარმოდგენილი ცხრილიდან ჩანს, სააგენტო ვერ უზრუნველყოფს ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებთან შესაბამისობას. აღნიშნული საკითხები ასევე განხილული იყო სააგენტოსთან, თუმცა აუდიტის ჯგუფმა ვერ მიიღო კონკრეტული პასუხი, ვინ არის ინფორმაციული უსაფრთხოების მენეჯერი. ასევე აღსანიშნავია, რომ მონაცემთა გაცვლის სააგენტოს

³⁵ მოცემული ინფორმაცია მიღებულ იქნა მონაცემთა გაცვლის სააგენტოსაგან 2017 წლის მაისში.

მიერ ჩატარებულ ინფორმაციული უსაფრთხოების მენეჯერის გადამზადების ტრენინგზე სააგენტომ ყოველ ჯერზე სხვადასხვა კანდიდატი წარადგინა. აღნიშნული ფორმალური დოკუმენტებისა და პროცედურების არარსებობა დაკავშირებულია ინფორმაციული უსაფრთხოების დარღვევის რისკთან, რომელიც, თავის მხრივ, იწვევს არაეფექტიანი ოპერაციებისა და IT ინვესტიციების განხორციელების საფრთხეს.

2.3.4 ტერიტორიულ ერთეულებში საბოლოო მომხმარებლის სკანირების შედეგად გამოვლენილი ხარვეზები

საარსებო შემწეობის პროგრამის ადმინისტრირების პროცესში ჩართულია სააგენტოს რეგიონული ოფისები. ოფისებში არსებულ კომპიუტერებში განთავსებულია ბენეფიციარების შესახებ სენსიტიური ინფორმაცია. შესაბამისად, არსებული კომპიუტერების სათანადო დაცვა და ტექნიკური მხარდაჭერა განსაკუთრებით მნიშვნელოვანია. ასევე იმ ფაქტის გათვალისწინებით, რომ ცენტრალურ ოფისში დანერგილია დამატებითი დაცვის მექანიზმები, ხოლო ტერიტორიული ერთეულები ამ მიმართულებით წარმოადგენენ მაღალი რისკის შემცველ ობიექტებს, აუდიტის ფარგლებში შეფასდა თბილისის ხუთივე და გარდაბნის რეგიონული ოფისები. შემოწმდა საბოლოო მომხმარებლის კომპიუტერების დაცულობა მავნე კოდის შემცველ პროგრამებზე/ფაილებზე. გამოვლინდა, რომ რეგიონულ ოფისებში არასაკმარისი კომპიუტერული რესურსების პირობებში, სოციალურ აგენტებს, რომლებიც ახდენენ ბენეფიციარებისაგან მიღებული მონაცემების გადამოწმებას, უწევთ ერთი და იმავე კომპიუტერის გამოყენება. ამასთანავე, ოპერაციული სისტემის დონეზე, რიგ შემთხვევაში³⁶, რეგიონული ცენტრის თანამშრომელთათვის არ არის განსაზღვრული ინდივიდუალური მომხმარებლის ანგარიშები. შესაბამისად, არასაკმარისი რესურსების პირობებში, სააგენტოში არსებობს ინფორმაციული უსაფრთხოების დარღვევის რისკი.

ასევე უნდა აღინიშნოს, რომ რეგიონულ ოფისებში არსებულ კომპიუტერებზე კვლავ გამოიყენება მოძველებული ოპერაციული სისტემა WINDOWS XP

³⁶ შემოწმებული მომხმარებლებიდან მხოლოდ ერთ შემთხვევაში იყო განსაზღვრული ინდივიდუალური მომხმარებლის ანგარიში.

(შერჩეული 16 კომპიუტერიდან 10 შემთხვევაში), რომლის ოფიციალური მხარდაჭერა მწარმოებლის მიერ აღარ ხორციელდება და შესაბამისად, მოწყვლადია საფრთხეების მიმართ. აგრეთვე ოფისებში გამოიყენება WINDOWS 7 ოპერაციული სისტემა, რომელიც აღჭურვილია უსაფრთხოების მინიმალური პაკეტით - ანტივირუსით (Microsoft Security Essential), თუმცა, სისტემის შესაბამისი მხარდაჭერა არ ხდება. კერძოდ, არ არის გააქტიურებული სისტემური განახლებები და აღნიშნული ანტივირუსით კომპიუტერების გეგმური სკანირება არ მიმდინარეობს. აუდიტის ფარგლებში მოხდა რეგიონულ ოფისებში არსებული კომპიუტერების სისტემის მავნე კოდზე სკანირება, რის შედეგადაც გამოვლინდა, რომ სკანირებული 17 კომპიუტერიდან 10-ში აღმოჩნდა საფრთხის შემცველი მავნე კოდები. აღნიშნული კომპიუტერები შეიცავს სხვადასხვა ტიპის მავნე კოდს (WORM, PUP, PUM, HIJACK), რამაც შეიძლება საფრთხე შეუქმნას საბოლოო მომხმარებელთა კომპიუტერებში არსებულ ინფორმაციას.

ზემოთ აღნიშნული გარემოებების გათვალისწინებით, ტერიტორიულ ერთეულებში დაინფიცირებული კომპიუტერებისა და არასათანადო კონტროლების პირობებში მაღალია ბენეფიციართა შესახებ არსებულ პირად და კონფიდენციალურ ინფორმაციაზე არაავტორიზებული წვდომისა და გამჟღავნების რისკი.

გარდა აღნიშნულისა, ინფორმაციული უსაფრთხოების საკითხებს ასევე რისკს უქმნის სააგენტოს რიგი ტერიტორიული ერთეულების ფიზიკური უსაფრთხოების მდგომარეობა. კერძოდ, აღსანიშნავია, რომ *სოციალური მომსახურების სააგენტოს* რეგიონულ ოფისებში ვიზიტების ფარგლებში გაირკვა, რომ ყველა რაიონული ცენტრი არ არის უზრუნველყოფილი შესაბამისი ფიზიკური დაცვის (ფიზიკური დაცვის მექანიზმები მოიცავს ვიდეო კამერებს, ბარიერებით კონტროლირებად შესასვლელს და სხვ.), მექანიზმებით და ადეკვატური სამუშაო პირობებით.

შესაბამისად, სააგენტო ვერ უზრუნველყოფს არაავტორიზებული ფიზიკური წვდომის შეზღუდვას ინფორმაციული აქტივების დამუშავების პროცესსა და შესაბამის ინფრასტრუქტურაზე.

დასკვნა

სააგენტოს მიერ არ არის შემუშავებული აპლიკაციის მომხმარებელთათვის მინიმალური პრივილეგიების პრინციპით წვდომის უფლებები და შესაბამისად, სააგენტოს თანამშრომლებს დაშვება აქვთ საჭიროზე მეტ ინფორმაციაზე. აღნიშნული გარემოება იწვევს კონფიდენციალურობის პრინციპის დარღვევას და საკანონმდებლო მოთხოვნების უგულებელყოფას³⁷. არსებული გარემოება მომატებული რისკის მატარებელია მაშინ, როდესაც სააგენტოში არ არის დანერგილი მომხმარებელთა მონიტორინგის ქმედითი სისტემა და სააგენტოს თანამშრომლები რიგ შემთხვევაში იყენებენ საერთო მომხმარებლის ანგარიშს. შესაბამისად, აღნიშნულ პირობებში შეუძლებელია სისტემაში კონკრეტული ქმედების განმახორციელებელი მომხმარებლის იდენტიფიცირება. შესაბამისად, მონაცემთა ბაზაში არსებული ინფორმაციის არაკანონიერი მითვისებისა და გამჟღავნების შემთხვევაში, სააგენტო მოკლებულია შესაძლებლობას განსაზღვროს კონკრეტული პასუხისმგებელი პირი. პაროლების სირთულეზე მოთხოვნების არარსებობა, აპლიკაციის არსებული არქიტექტურის პირობებში, ზრდის კონფიდენციალურობის პრინციპის დარღვევისა და მოქალაქეთა შესახებ პერსონალური ინფორმაციის მიტაცების, დაკარგვისა და განადგურების რისკს.

ზემოთ აღნიშნული გარემოებები მნიშვნელოვნად განპირობებულია იმ ფაქტით, რომ სააგენტოში არ არის დანერგილი ინფორმაციული უსაფრთხოების მართვის სისტემა. ფორმალური პროცედურებისა და პოლიტიკების არარსებობა, აღნიშნული მიმართულებით, იწვევს საკანონმდებლო მოთხოვნების შეუსრულებლობას და ზრდის ინფორმაციულ უსაფრთხოებასთან დაკავშირებულ საფრთხეებს.

³⁷ საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“.

რეკომენდაცია

სააგენტომ, როგორც კრიტიკული ინფორმაციული სისტემის სუბიექტმა, უზრუნველყოს არსებული საკანონმდებლო ნორმების გათვალისწინებით ინფორმაციული უსაფრთხოების მართვის სისტემის შემუშავება და პრაქტიკაში დანერგვა. მათ შორის, გამოვლენილი ნაკლოვანებების შესაბამისად, მნიშვნელოვანია:

- › შემუშავდეს პოლიტიკა და პროცედურები წვდომისა და პრივილეგიების განსაზღვრის მიზნით;
- › დაინერგოს სისტემაში მომხმარებელთა მიერ განხორციელებული ქმედებების მონიტორინგის ქმედითი სისტემა;
- › უზრუნველყოფილ იქნეს ბიზნესპროცესში გამოყენებული ინფორმაციული სისტემების დაცულობის მუდმივი ტექნიკური მხარდაჭერა.

2.4 სააგენტოს მიერ შემუშავებული მექანიზმები ვერ უზრუნველყოფს ბენეფიციარებზე თანხის გადარიცხვის ეფექტიან/ადეკვატურ პროცესს

საარსებო შემწეობის პროგრამის ადმინისტრირების ერთ-ერთ მნიშვნელოვან კომპონენტს ბენეფიციართათვის თანხის გადარიცხვა წარმოადგენს, რომლის მართვა კონტრაქტორის მეშვეობით ხდება. კონტრაქტორის მხარეს წარმოადგენს სს „ლიბერთი ბანკი“, რომელთან გაფორმებულ ხელშეკრულებაში³⁸ განსაზღვრულია სერვისის ფარგლებში სააგენტოსათვის მისაღები პირობები და პარამეტრები. შესაბამისად, მნიშვნელოვანია მუდმივად ხდებოდეს ხელშეკრულებით გათვალისწინებული პირობების შესრულების მონიტორინგი და გადახრების არსებობისას, შესაბამისი რეაგირება, რათა უზრუნველყოფილ იყოს პროგრამით განსაზღვრული მიზნების მიღწევა და კონტრაქტორთან დაკავშირებული რისკების სწორი მართვა.

ცხრილი №2.2: ბანკის მიერ შესასრულებელი ხელშეკრულებით გათვალისწინებული პირობები

ხელშეკრულების პირობები	განსაზღვრება
ხელშეკრულებით გათვალისწინებული ვადების კონტროლი	ბენეფიციარებზე თანხის გადარიცხვა; ბენეფიციარისათვის ანგარიშის გახსნა; ბენეფიციარის ანგარიშზე მოძრაობები; 6-თვიანი და 12-თვიანი უმოძრაობის მქონე ბენეფიციარებზე ინფორმაციის მიწოდება; არასწორად ჩარიცხული თანხების დაბრუნება.
კონფიდენციალურობის მოთხოვნის კონტროლი	მხარეები ვალდებული არიან დაიცვან ერთობლივი საქმიანობის შედეგად მათთვის ცნობილი მეორე მხარის კონფიდენციალური ინფორმაცია.
მინდობილობის არსებობის და განახლების კონტროლი	არ გაცეს თანხა ბენეფიციარზე თუ მინდობილობა 6 თვის მანძილზე არ განუახლებია; ერთი წლის მერე სავაჭრო ობიექტებში

³⁸ ფულადი გასაცემლების გაცემის/დარიცხვის უსასყიდლო საბანკო მომსახურების თაობაზე ხელშეკრულება, 2014 წლის 23 დეკემბერი.

		საკრედიტო ბარათის გამოყენება არ უნდა იყოს შესაძლებელი.
თანხის განკარგვის მიზნობრიობის კონტროლი		თანხის ჩარიცხვა უნდა მოხდეს მხოლოდ ბენეფიციართათვის საარსებო შემწეობის თანხის ანაზღაურების მიზნობრიობით.
ბენეფიციართათვის საზღაურის გარეშე მომსახურების კონტროლი		ბენეფიციარისათვის საბანკო ოპერაციების უსასყიდლოდ განხორციელება.

ცხრილში №2.2 წარმოდგენილია სს „ლიბერთი ბანკთან“ გაფორმებული ხელშეკრულების ფარგლებში ბანკის მიერ ნაკისრი ვალდებულებები. ასევე ხელშეკრულებით არის გათვალისწინებული სააგენტოს უფლებამოსილება აღნიშნული პირობების შესრულების მონიტორინგის განხორციელებაზე. უნდა აღინიშნოს, რომ ხელშეკრულების გარკვეული მოთხოვნების მონიტორინგი 2014 წლამდე მიმდინარეობდა ინსპექტირების ჯგუფის მიერ. კერძოდ, 2010 წელს სააგენტოს ბრძანების საფუძველზე, შეიქმნა სს „ლიბერთი ბანკთან“ გაფორმებული ხელშეკრულების ინსპექტირების ჯგუფი, თუმცა აღნიშნული ბრძანება 2014 წლის ბოლოს ძალადაკარგულად გამოცხადდა და შესაბამისად, გაუქმდა ინსპექტირების ჯგუფი. აღნიშნული ჯგუფი მონიტორინგს უწევდა ბენეფიციარების ანგარიშზე თანხის მოძრაობას და მინდობილობების არსებობის საკითხს.

აუდიტის პერიოდში სააგენტოში აღარ ხორციელდება სს „ლიბერთი ბანკის“ მონიტორინგისათვის საჭირო პროცედურები. შესაბამისად, დღევანდელი მდგომარეობით, სააგენტოში არ არის სტრუქტურული ერთეული ან ჯგუფი, რომელიც პასუხისმგებელი იქნება ხელშეკრულების პირობების შესრულების მონიტორინგზე.

სს „ლიბერთი ბანკის“ მონიტორინგის თემას აქტუალობას მატებს ისიც, რომ 2013-2014 წლებში კონტროლის დეპარტამენტის მიერ იდენტიფიცირებულია ბანკის მიერ მოქმედი ხელშეკრულებით გათვალისწინებული მოთხოვნების დარღვევის

შემთხვევები თანხების დაგვიანებით გადარიცხვის გამო და აღნიშნულისათვის პირგასამტეხლოს დარიცხვა³⁹.

დამატებით აღსანიშნავია, რომ დღემდე მიმდინარეობს 2014 წელს დაწყებული სასამართლო დავა სს „ლიბერთი ბანკსა“ და სააგენტოს შორის სადავო თანხებზე, რომელიც მოიცავს მხოლოდ 7 ბენეფიციარის საქმის განხილვის შედეგად სს „ლიბერთი ბანკზე“ დაკისრებულ 486,758.06 ლარის პირგასამტეხლოს, ხელშეკრულების პირობის დარღვევისათვის. კონკრეტულად, ბენეფიციარების ანგარიშზე თანხის 6-თვიანი და 12-თვიანი უმოძრაობის შესახებ ინფორმაციის მიწოდების ხელშეკრულებით გათვალისწინებული ვადის დარღვევისათვის.

ქმედითი მონიტორინგის მექანიზმების არარსებობა გავლენას ახდენს პროგრამით გათვალისწინებული მიზნების მიღწევაზე. მუდმივი მონიტორინგის არარსებობა ზრდის არაინფორმირებული გადაწყვეტილების მიღების, საბოლოო მომხმარებლის უკმაყოფილებისა და საბიუჯეტო სახსრების არამიზნობრივად და არაპროდუქტიულად განკარგვის რისკს.

დასკვნა

სს „ლიბერთი ბანკთან“ გაფორმებული ხელშეკრულების პირობების შესრულებისას მონიტორინგის მექანიზმის არარსებობის შედეგად, სააგენტოს არ გააჩნია რწმუნება საბიუჯეტო სახსრების მიზნობრივ და დროულ ხარჯვაზე.

³⁹ სააგენტოს 2013 და 2014 წლების წლიური ანგარიშები.

რეკომენდაცია

- › საბიუჯეტო რესურსების მიზნობრივი ხარჯვისა და პროგრამით გათვალისწინებული შედეგების ეფექტიანად მიღწევისათვის *სოციალური მომსახურების სააგენტომ* უზრუნველყოს სს „ლიბერთი ბანკთან“ გაფორმებული ხელშეკრულებით გათვალისწინებული პირობების ქმედითი მონიტორინგის მექანიზმების შემუშავება და დანერგვა. სხვა დანარჩენთან ერთად, აღნიშნულის ფარგლებში, უნდა განისაზღვროს მონიტორინგის შედეგების ანგარიშგების პერიოდულობა, ფორმატი და შესაბამისი პასუხისმგებელი პირები/ სტრუქტურული ერთეული.

დანართი N1 : გამოყენებული მეთოდოლოგია

აუდიტი ჩატარდა სახელმწიფო აუდიტის სამსახურსა და აშშ-ის უმაღლესი აუდიტორული ორგანიზაციის (US Government Accountability Office) აუდიტის სასწავლო ცენტრს (Center For Audit Excellence) შორის თანამშრომლობის ფარგლებში. აღნიშნული აუდიტისათვის, აუდიტის ჯგუფმა გაიარა ამერიკელი ექსპერტების მიერ მომზადებული ტრენინგკურსი. ამასთანავე, აუდიტის მიმდინარეობისა და ანგარიშების პროცესში ჩართული იყო სასწავლო ცენტრის აუდიტორთა ჯგუფი, რომელიც მონიტორინგს უწევდა აუდიტის პროცედურებისა და ანგარიშის შესაბამისობას უმაღლესი აუდიტორული ორგანოების საერთაშორისო სტანდარტებთან.

ინფორმაცია მოპოვებულ იქნა რიგი ინტენსიური კვლევებით, დოკუმენტებისა და საარსებო შემწეობის ადმინისტრირების პროცესში გამოყენებული ინფორმაციული სისტემის ანალიზითა და ჩატარებული გასაუბრებების შედეგად. გამოიკითხნენ: სამინისტროს წარმომადგენლები, სააგენტოს ცენტრალური ადმინისტრაციისა და სხვადასხვა სამმართველოების წარმომადგენლები, სოციალური აგენტები, სპეციალისტები და ოპერატორები.

აუდიტორული პროცედურების განხორციელებისათვის გამოყენებულ იქნა შემდეგი მიდგომები:

- › მარეგულირებელი ნორმების შესწავლა და ანალიზი;
- › საერთაშორისო პრაქტიკის გაცნობა;
- › დოკუმენტური ინფორმაციის ანალიზი;
- › სოციალურად დაუცველი ოჯახების ერთიანი ბაზის ანალიზი;
- › ზოგადი და აპლიკაციის კონტროლების ტესტირება;
- › ოპერაციული სისტემისა და მონაცემთა ბაზის მართვის სისტემის მოწყვლადობის ანალიზი;
- › სააგენტოს რეგიონულ ცენტრებში არსებული კომპიუტერების მავნე კოდზე სკანირება;
- › ინტერვიუები სსიპ - სოციალური მომსახურების სააგენტოსა და სამინისტროს წარმომადგენლებთან.

აუდიტის თითოეულ ქვეკითხვაზე პასუხის გასაცემად გამოყენებულ იქნა შემდეგი მეთოდები და პროცედურები:

- › რამდენად ეფექტიანი პროცედურებია დანერგილი ოჯახის სოციალურ-ეკონომიკური მდგომარეობის შეფასებისათვის და რამდენად ადეკვატურად უზრუნველყოფს არსებული ინფორმაციული სისტემა ბენეფიციარებისათვის პროგრამით გათვალისწინებული შემწეობის მოცულობის განსაზღვრას? - აღნიშნულ შეკითხვაზე პასუხის გასაცემად

შესწავლილ იქნა საარსებო შემწეობის გაცემის პროცესში სააგენტოს მიერ გამოყენებული აპლიკაციები (SAESA2005, SAESA, SSA-დამატება). აღნიშნული მიზნით გაიმართა შეხვედრები სააგენტოს რეგიონული ცენტრის წარმომადგენლებთან და უშუალოდ ბიზნესპროცესის გავლისა და დაკვირვების მეშვეობით შეფასდა სისტემა. ამასთანავე, იმ მიზნით, რომ შეფასებულყო რეგიონულ ცენტრებში საბოლოო მომხმარებლების კომპიუტერების დაცულობა, განხორციელდა მათი სკანირება მავნე კოდის სკანირების ინსტრუმენტის - Malwarebytes version 3.1-ის მეშვეობით. ასევე სარეიტინგო ქულაზე გავლენის მქონე ცვლადების ანალიზის მიზნით, შესწავლილ იქნა ბენეფიციარების ასაკი. აღნიშნულ კრიტერიუმთან შესაბამისობის შეფასებისათვის, შეირჩნენ ახალი მეთოდოლოგიით გადაფასებული ბენეფიციარები (სრულად, 2015 წლის 1 მაისიდან 2016 წლის 1 ოქტომბრამდე პერიოდი) რეინტეგრაციის შემწეობის, სოციალური პაკეტის მიმღები ბენეფიციარებისა და საპენსიო ასაკს მიღწეული პირების გარდა. ჯამში 139,285 ოჯახიდან შეირჩა 110,258 ოჯახი. აღნიშნული ბენეფიციარების გამოკლება მოხდა იმ მიზნით, რომ სარეიტინგო ქულის გადათვლისათვის საჭირო იყო დამატებითი მონაცემები, ხოლო 2016 წლის 1 ოქტომბერი განისაზღვრა შემდეგი ლოგიკის საფუძველზე: ოჯახის შეფასებისა და სარეიტინგო ქულის მინიჭებისათვის საშუალოდ საჭიროა 3-თვიანი პერიოდი. აუდიტის ჯგუფს სოციალურად დაუცველი მოსახლეობის ერთიანი ბაზა ჰქონდა 24 იანვრის მდგომარეობით. შესაბამისად, იმისათვის, რომ შერჩეულ ბენეფიციარებში არ მოხვედრილიყო ისეთი ოჯახები, რომელთაც ჯერ არ ჰქონდათ მინიჭებული ქულა, განისაზღვრა 2016 წლის ოქტომბრამდე პერიოდის მონაცემები.

- ბუნებრივი აირის მოხმარების ინფორმაციის გავლენის სიმულაციური ანალიზისათვის 139,285 ოჯახიდან შეირჩა 112,565 ოჯახი, პერიოდი მსგავსად ასაკისა, განისაზღვრა 2015 წლის 1 მაისიდან 2016 წლის 1 ოქტომბრამდე და გამოირიცხა რეინტეგრაციის შემწეობისა და სოციალური პაკეტის მიმღები ბენეფიციარები. ხოლო განათლების დონის შემთხვევაში, განისაზღვრა 2015 წლის 1 მაისიდან 2016 წლის 1 ოქტომბრამდე პერიოდში არსებული მხოლოდ ის ბენეფიციარები, რომელთა ოჯახზეც შესაძლებელი იყო გავლენა მოეხდინა განათლების დონეს. კერძოდ, ოჯახები, რომლებსაც ჰყავდათ 22-65 წლის ფარგლებში ოჯახის წევრები, 105,543 ოჯახიდან - 79,630 ოჯახი. ამ შემთხვევაშიც მოხდა რეინტეგრაციის შემწეობისა და სოციალური პაკეტის მიმღები ბენეფიციარების გამოორიცხვა. ასევე ორგანიზაციის ქსელში მონაცემთა მართვის გაანალიზების მიზნით, გამოთხოვილ იქნა ქსელის ლოგიკური ტოპოლოგია. გამომდინარე იქიდან, რომ სააგენტოს არ ჰქონდა შემუშავებული ლოგიკური ტოპოლოგიის მოდელი, აღწერილ იქნა და

სააგენტოს მიერ დადასტურდა ლოგიკური ტოპოლოგიის მოდელი. პროგრამის მართვის პროცესის დეტალური ანალიზისათვის ჩატარდა გასაუბრებები სამინისტროსა და სააგენტოს წარმომადგენლებთან. ასევე გაანალიზდა ინსტრუქციები და რეგულაციები, რომლებიც არეგულირებს საარსებო შემწეობის გაცემის პროცესს;

- › **რამდენად უზრუნველყოფილია ინფორმაციული უსაფრთხოება და მესამე მხარეებისაგან მოქალაქეთა შესახებ მიღებული მონაცემების კონფიდენციალურობისა და მთლიანობის დაცვა ინფორმაციის მიმოცვლისა და ტერიტორიულ ერთეულებთან კომუნიკაციის პროცესში?** - მოცემულ შეკითხვასთან მიმართებით შეფასდა სააგენტოს მიერ ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით გატარებული ღონისძიებები. კერძოდ: რამდენად უზრუნველყო სააგენტომ „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის ფარგლებში განსაზღვრული ვალდებულებებისა და ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დაცვა. ასევე გაიმართა შეხვედრები ბიზნესპროცესში ჩართულ მხარეებთან და განხილულ იქნა შესაბამისი დოკუმენტაცია მათი როლებისა და პასუხისმგებლობების იდენტიფიცირებისა და მათთვის განსაზღვრული წვდომის უფლების მინიჭების პროცედურების შეფასების მიზნით. განხილულ იქნა საარსებო შემწეობის პროგრამის ადმინისტრირების ფარგლებში ზოგად ინფორმაციაში (ქვეთავი 1.5.2, მესამე მხარეები) წარმოდგენილ მესამე მხარესთან გაფორმებული ხელშეკრულებები;
- › **რამდენად უზრუნველყოფს სააგენტო ბენეფიციარებზე თანხის გადარიცხვის ეფექტიან/ადეკვატურ პროცესს?** აღნიშნულ შეკითხვაზე პასუხის გაცემისათვის შესწავლილ იქნა სს „ლიბერთი ბანკთან“ გაფორმებული ხელშეკრულება და აღნიშნული ხელშეკრულების პირობების შესრულების მონიტორინგის საკითხები. მოთხოვნილი იყო სს „ლიბერთი ბანკის“ მონიტორინგის დამადასტურებელი აქტები და ანგარიშები, ასევე სამუშაო ჯგუფის შესახებ ბრძანებები. განხილულ იქნა ბანკთან არსებული დავის სარჩელი.

ბიბლიოგრაფია

კანონები

- › საქართველოს კანონი „სოციალური დახმარების შესახებ“;
- › საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“;
- › საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“.

ბრძანებები

- › საქართველოს მთავრობის №758 დადგენილება „სოციალურად დაუცველი ოჯახების (შინამეურნეობების) სოციალურ-ეკონომიკური მდგომარეობის შეფასების მეთოდოლოგიის დამტკიცების შესახებ, 2014 წლის 31 დეკემბერი“;
- › საქართველოს მთავრობის №145 დადგენილება „სოციალური დახმარების შესახებ“, 2006 წლის 28 ივლისი;
- › საქართველოს მთავრობის №126 დადგენილება „ქვეყანაში სიღატაკის დონის შემცირებისა და მოსახლეობის სოციალური დაცვის სრულყოფის ღონისძიებათა შესახებ, 2010 წლის 24 აპრილი“;
- › საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის მინისტრის №141/ნ ბრძანება „სოციალურად დაუცველი ოჯახების სოციალურ-ეკონომიკური მდგომარეობის შეფასების წესის დამტკიცების თაობაზე, 2010 წლის 20 მაისი“;
- › საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის მინისტრის №225/ნ ბრძანება „მიზნობრივი სოციალური დახმარების დანიშვნისა და გაცემის წესის დამტკიცების შესახებ, 2006 წლის 22 აგვისტო“;
- › მონაცემთა გაცვლის სააგენტოს თავმჯდომარის №2 ბრძანება „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ, 2013 წლის 4 თებერვალი“.

პუბლიკაციები/დოკუმენტები

- › WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions, 2014 წელი.
- › US GAO, FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM), 2009 წელი.

აუდიტორთა ხელმოწერა:
სახელი, გვარი

ხელმოწერა

დავით შავგულიძე
(ინფორმაციული ტექნოლოგიების
აუდიტის სამსახურის უფროსი)

მარიამ მაღრაძე
(ინფორმაციული ტექნოლოგიების
აუდიტორი)

გიორგი ჭოხონელიძე
(ინფორმაციული ტექნოლოგიების
მთავარი აუდიტორი)

თამარ ივანიძე
(ინფორმაციული ტექნოლოგიების
აუდიტორი)

ნია გურგენიძე
(ინფორმაციული ტექნოლოგიების
აუდიტორი)

