



ეფექტიანობის აუდიტის ანგარიში





სახელმწიფო აუდიტის სამსახური

„ვამბეკიშვილი“

ეფექტიანობის აუდიტის
დეპარტამენტის უფროსი

გიორგი კაპანაძე

29 აპრილი 2020 წელი

N 17/36

ეგზ.: N2

სახელმწიფო პენსიის
ადმინისტრირების
ინფორმაციული სისტემა

საჩივრი

ტერმინთა განმარტებები.....	4
შემაჯამებელი მიმოხილვა და რეკომენდაციები	5
1. შესავალი	8
1.1 აუდიტის მოტივაცია.....	8
1.2 აუდიტის მიზანი.....	9
1.3 შეფასების კრიტერიუმები	9
1.4 აუდიტის მასშტაბი და მეთოდოლოგია	10
2. ზოგადი ინფორმაცია.....	12
2.1 სახელმწიფო პენსიის ადმინისტრირების სისტემის მნიშვნელობა	12
2.1.1 სისტემის განვითარებასთან დაკავშირებული ინფორმაცია	13
აუდიტის მიგნებები	14
3.1 პენსიის ადმინისტრირების სისტემა	14
3.1.1 პროდუქტიულობასთან დაკავშირებული ნაკლოვანებები	14
3.1.2 სისტემის არქიტექტურა და ტექნიკური მახასიათებლები.....	17
3.1.3 IT მმართველობა და ფუნქციების გადანაწილება.....	19
დასკვნა	22
რეკომენდაცია	22
3.2 ინფორმაციული უსაფრთხოება	23
3.2.1 სისტემის ხელმისაწვდომობა.....	25
3.2.2 ინფორმაციის მიმოცვლის უსაფრთხოება.....	26
3.2.3 დამუშავებული ინფორმაციის უსაფრთხოება	28
დასკვნა	34
რეკომენდაცია	35
ბიბლიოგრაფია	37

ტერმინთა განმარტება

სამინისტრო	საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო.
სააგენტო	სსიპ – სოციალური მომსახურების სააგენტო.
სსგს ბანკი	სსიპ – სერვისების განვითარების სააგენტო. სს „ლიბერთი ბანკი“.
ტერიტორიული ერთეული რაიონული ცენტრი	/ სოციალური მომსახურების სააგენტოს ტერიტორიული სამსახურები, რომლებიც ჩართულნი არიან პენსიის ადმინისტრირების პროცესში.
ინფორმაციული სისტემა	ინფორმაციული ტექნოლოგიებისა (IT) და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადანაცვების მიღებას.
„პენსია 2005“	სახელმწიფო პენსიის ადმინისტრირების პროცესში გამოყენებული ინფორმაციული სისტემა
SAESA	საარსებო შემწეობის პროგრამის ადმინისტრირების ფარგლებში გამოყენებული ინფორმაციული სისტემა.
ვალიდაცია	სისტემაში ასახული ინფორმაციის დადასტურება მესამე მხარესთან ან კონტროლის სხვა მექანიზმებით.
იუმს	ინფორმაციული უსაფრთხოების მართვის სისტემა
საბოლოო მომხმარებელი	პირი/თანამშრომელი, რომელიც თავის საქმიანობაში იყენებს ინფორმაციულ სისტემას.
სამუშაო სადგური	ინფორმაციული სისტემის საბოლოო მომხმარებლის პერსონალური კომპიუტერი.
პროქსი სერვერი	შუალედური სერვერი, რომელიც უზრუნველყოფს მომხმარებლების დაშვებას წინასწარ განსაზღვრულ ვებრესურსებზე.
დომენი	ოპერაციული სისტემის მომხმარებლების ცენტრალიზებული მართვის სისტემა.



შემაჯავებელი მიმოხილვა და ჩაპოვნისასიები

ხელმისაწვდომი, ხარისხიანი ჯანმრთელობის დაცვა და სოციალური უზრუნველყოფა ქვეყნის ერთ-ერთი მთავარი პრიორიტეტია. აღნიშნული პრიორიტეტის შესაბამისად, მთავრობა ახორციელებს „მოსახლეობის სოციალური დაცვის“ პროგრამას, რომლის ქვეპროგრამა – „მოსახლეობის საპენსიო უზრუნველყოფა“ საზოგადოებისთვის ერთ-ერთ ძირითად სოციალურ გარანტიას წარმოადგენს.

წლების განმავლობაში ქვეპროგრამაზე გათვალისწინებული დაფინანსების წილი მზარდი ტენდენციით გამოირჩევა და 2019 წელს 1,9 მლრდ ლარი შეადგინა, ხოლო ბენეფიციართა რაოდენობამ 762 ათას ადამიანს გადააჭარბა. სახელმწიფო პენსიის ფინანსური მოცულობის, ბენეფიციარების რაოდენობისა და პროგრამის მნიშვნელობის გათვალისწინებით, სახელმწიფო აუდიტის სამსახურმა ჩაატარა სახელმწიფო პენსიის ადმინისტრირების ინფორმაციული სისტემის 2014-2019 წლების ეფექტიანობის აუდიტი. აუდიტის ობიექტებს წარმოადგენენ სსიპ – სოციალური მომსახურების სააგენტო (შემდგომ – სააგენტო) და საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო (შემდგომ – სამინისტრო).

აუდიტის ფარგლებში შესწავლილ იქნა სახელმწიფო პენსიის ადმინისტრირების სისტემა და მასთან დაკავშირებული კონტროლები. კერძოდ, აუდიტისას შეფასდა ინფორმაციული სისტემისა და პენსიის ადმინისტრირების პროცესის პროდუქტიულობა. ასევე აუდიტის ჯგუფმა შეაფასა პენსიის ადმინისტრირების პროცესში გამოყენებული მონაცემების უსაფრთხოება და პერსონალური ინფორმაციის დამუშავების პრაქტიკა. აუდიტის შედეგად გამოვლინდა, რომ:

- სახელმწიფო პენსიის ადმინისტრირების ინფორმაციული სისტემა („პენსია 2005“) მოძველებულია და ვერ უზრუნველყოფს სააგენტოს სხვა სისტემებთან ინტეგრაციას. სისტემა არ არის ცენტრალიზებული, რაც გულისხმობს, რომ იგი დამოუკიდებლად არის დაინსტალირებული ყველა სამუშაო სადგურზე (პერსონალურ კომპიუტერზე) და ერთმანეთს არ უკავშირდება. სხვადასხვა მომხმარებლის მიერ დამუშავებული მონაცემების ცენტრალიზება ხდება ხელით და საჭიროებს რამდენიმე ნაბიჯს. აღნიშნული მოიცავს როგორც ბაზების გაერთიანებას, ასევე ინფორმაციის გადამოწმებას (ვალიდაციას). შესაბამისად, დეცენტრალიზებული არქიტექტურის გათვალისწინებით, სახელმწიფო პენსიის ადმინისტრირების ბიზნესპროცესი არ არის პროდუქტიული და საჭიროებს ინტენსიურ ხელით შესრულებულ პროცესებს, რაც, თავის მხრივ, ზრდის მონაცემთა დამუშავების სიზუსტისა და სანდოობის რისკებს. გემოაღნიშნული გამოწვევულია სააგენტოს არაერთგვაროვანი მიდგომით ინფორმაციული სისტემების განვითარების მიმართ. კერძოდ, სააგენტოს სისტემების კომპლექსურობისა და კრიტიკულობის გათვალისწინებით, სააგენტოს არ გააჩნია სტანდარტიზებული მიდგომა ინფორმაციულ სისტემებთან დაკავშირებით. სააგენტოს მფლობელობაში მყოფი ორი მსხვილი სისტემა – სახელმწიფო პენსიის ადმინისტრირების სისტემა („პენსია 2005“) და საარსებო შემწეობის ადმინისტრირების სისტემა (SAESA) მნიშვნელოვანად განსხვავებული შესაძლებლობებისაა. „პენსია 2005“ მნიშვნელოვნად ჩამორჩება სააგენტოს მიერ ადმინისტრირებულ მეორე სისტემას – SAESA-ს, ავტომატიზაციისა და უსაფრთხოების ხარისხით;
- სააგენტო ვერ უზრუნველყოფს ინფორმაციული უსაფრთხოების საკანონმდებლო მოთხოვნების შესრულებას. აუდიტის პერიოდში სააგენტოს არ ჰქონდა შესრულებული „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მოთხოვნები;
- სახელმწიფო პენსიის ადმინისტრირების სისტემის მოძველებული პლატფორმის გათვა-



ლისწინებით, სააგენტოს არ აქვს შეფასებული სისტემის უწყვეტობასთან დაკავშირებული რისკები და დანერგილი შესაბამისი კონტროლის მექანიზმები. აღნიშნული კონტროლები სააგენტოს საშუალებას მისცემდა წინასწარ განსაზღვრული გეგმის შესაბამისად ემოქმედა სისტემის ფუნქციონირების წყვეტის შემთხვევაში;

- სახელმწიფო პენსიის მიმღებ უფლებამოსილ პირთა წრის განსაზღვრის პროცესში, სააგენტო ვერ უზრუნველყოფს სპეციალური პენიტენციური სამსახურიდან განსაკუთრებული კატეგორიის პერსონალური მონაცემების მიღებას დაცული საკომუნიკაციო არხის საშუალებით;
- სააგენტო ვერ უზრუნველყოფს ქვეყნის მასშტაბით 69 რაიონულ ოფისში არსებული სამუშაო სადგურების უსაფრთხოების მინიმალურად დაცვას. კერძოდ, სამუშაო სადგურების მართვა ცენტრალურად არ ხორციელდება, რაც გულისხმობს მომხმარებლების უფლებების განერასა და მართვას, პაროლების პოლიტიკის გატარებას და ანგარიშების მართვას. ასევე, სამუშაო სადგურებზე დაყენებული მავნე კოდისგან დაცვის საშუალებების კონფიგურაცია არასათანადოა;
- სააგენტო ვერ უზრუნველყოფს სახელმწიფო პენსიის ადმინისტრირების პროცესში გამოყენებულ მონაცემებზე ეფექტიან კონტროლს. ქვეყნის მასშტაბით არსებულ რაიონულ ოფისებში სააგენტოს თანამშრომლებს დაშვება აქვთ იმაზე მეტ ინფორმაციაზე, ვიდრე ეს საჭიროა მათი ფუნქცია-მოვალეობების შესასრულებლად. ასევე, სააგენტოს არ გააჩნია ტექნიკური კონტროლები, რომელთა საშუალებითაც მიიღწეოდა არასანქცირებული მოქმედებების აღმოჩენა და პრევენცია. შესაბამისად, პერსონალური და განსაკუთრებული კატეგორიის პერსონალური მონაცემები სათანადო ხარისხით არ არის დაცული.

ჩაქოვნდასიიბი

აუღიფი მღგნაბიის ბათვალისწინაბით მოგზადღა ჩაქოვნდასიიბი:

სახელმწიფო პენსიის ადმინისტრირების ბიზნესპროცესის გაუმჯობესების მიზნით, სააგენტომ, თავის მფლობელობაში არსებული სისტემებისა და გამოცდილების გათვალისწინებით:

- უზრუნველყოს პენსიის ადმინისტრირების სისტემის განვითარების გეგმის შემუშავება, რომელიც უნდა ითვალისწინებდეს პენსიის ადმინისტრირების სისტემის ცენტრალიზებული მართვის შესაძლებლობას და თავსებადობას სოციალური უზრუნველყოფის სფეროს სხვა სისტემებთან;
- პენსიის ადმინისტრირების ბიზნესპროცესის პროდუქტიულობისა და საიმედოობის გაზრდის მიზნით, უზრუნველყოს პენსიის ადმინისტრირების ინფორმაციული სისტემის ავტომატიზაცია, რაც პირველ რიგში გულისხმობს სათავო ოფისსა და ტერიტორიულ ერთეულებს შორის მონაცემთა ავტომატურ მიმოცვლას. ასევე უზრუნველყოს პენსიის ადმინისტრირების ეტაპების ავტომატიზაცია, რაც გულისხმობს მანუალურად (ხელით) ჩატარებული პროცედურების შემცირებას.

სახელმწიფო პენსიის ადმინისტრირების პროცესისა და დაქაუშირბაუღი სისტემის უწყვეტად ფუნქციონირებას მღიუზნალობის ბათვალისწინაბით, სააგენტომ:

- შეაფასოს სისტემის უწყვეტ ფუნქციონირებასთან დაკავშირებული რისკები და შეიმუშაოს ამ რისკების მოპყრობის გეგმა;



- შეიმუშაოს სახელმწიფო პენსიის ბიზნესუწყვეტობისა¹ და პენსიის ადმინისტრირების სისტემის კატასტროფიდან აღდგენის გეგმები.² უზრუნველყოს ამ გეგმების პერიოდული ტესტირება და განახლება.

საკანონმდებლო მოთხოვნების შესაბამისად, სააგენტომ უზრუნველყოს გარე წყაროებიდან მიღებული ინფორმაციის უსაფრთხოება, რაც გულისხმობს სპეციალური პენიტენციური სამსახურიდან მოწოდებული ინფორმაციის მიღებას დაცული საკომუნიკაციო არხის გამოყენებით.

სააგენტო უზრუნველყოს საბოლოო მომხმარებელთა სამუშაო სადგურების მინიმალური უსაფრთხოება, რაც მოიცავს შემდეგ ასპექტებს:

- მაქსიმალურად სწრაფად უზრუნველყოს რაიონული ოფისის ყველა სამუშაო სადგურის ჩართვა დომენში;
- მაქსიმალურად სწრაფად შეიმუშაოს და გაავრცელოს დომენში ჩართული სამუშაო სადგურების მომხმარებლების ჯგუფური პოლიტიკები, რომელიც, მინიმუმ, უნდა მოიცავდეს პაროლების პოლიტიკას, ანგარიშების პოლიტიკას, როლებისა და დაკავშირებული პრივილეგიების განსაზღვრას;
- დანერგოს მავნე კოდისგან დაცვის ქმედითი მექანიზმი (მაგალითად, მუდმივად განახლებადი ანტივირუსი) და უზრუნველყოს სისტემების პერიოდული სკანირება;
- განიხილოს საბოლოო მომხმარებლების საჭიროებები და დანერგოს მოქმედი კონტროლები ვებრესურსებზე წვდომისათვის, უზრუნველყოს წვდომის შეზღუდვა მავნე რესურსებსა და ფაილების გაცვლის სერვისებზე.

სახელმწიფო პენსიის ადმინისტრირების პროცესში პერსონალური მონაცემების დამუშავების პრინციპების დასაყვად, სააგენტო:

- განსაზღვროს ინფორმაციაზე დაშვების წესები მინიმალური პრივილეგიებისა³ და ცოდნის საჭიროებაზე⁴ დაფუძნებული პრინციპის გათვალისწინებით;
- შეიმუშაოს წვდომის კონტროლები ფაილების გაცვლის (FTP) სერვერისათვის, რომელიც უზრუნველყოფს მომხმარებლების იდენტიფიკაციისა და ავთენტიფიკაციის სათანადო პრაქტიკის ჩამოყალიბებას. ასევე, განახორციელოს სისტემაზე წვდომის ლოგების ანალიზი არავტორიზებული ქმედებების აღმოსაჩენისა და აღმოფხვრის მიზნით.

1 Business Continuity Plan (BCP)

2 Disaster Recovery Plan (DRP)

3 least privilege approach

4 need-to-know



1. შესავალი

1.1 აუდიტის მოტივაცია

ხელმისაწვდომი, ხარისხიანი ჯანმრთელობის დაცვა და სოციალური უზრუნველყოფა ქვეყნის ერთ-ერთი მთავარი პრიორიტეტია. ამ პრიორიტეტის ფარგლებში, საპენსიო ასაკს მიღწეული პირების პენსიით უზრუნველყოფის მნიშვნელოვან ქვეპროგრამას – „მოსახლეობის საპენსიო უზრუნველყოფა“ წარმოადგენს.

ქვეპროგრამის ფარგლებში ხორციელდება ქვეყნის ხანდაზმულ მოქალაქეთა (ქალები – 60 წლიდან, მამაკაცები – 65 წლიდან) პენსიით და სპეციფიკური კატეგორიების პირთა (ძალოვანი სტრუქტურების, პროკურატურის, საქართველოს პარლამენტის ყოფილი წევრების და სხვ.) სახელმწიფო კომპენსაციით უზრუნველყოფა.

წლების განმავლობაში აღნიშნულ ქვეპროგრამაზე გათვალისწინებული ხარჯების წილი სახელმწიფო ბიუჯეტში სტაბილურად მზარდი ტენდენციით გამოირჩევა და 2019 წელს გამოყოფილმა დაფინანსებამ 1,9 მლრდ ლარი⁵ შეადგინა. პენსიონერთა რაოდენობა კი 2019 წლის დეკემბრის მდგომარეობით – 762,621 მოქალაქეა, რაც საქართველოს მოსახლეობის 20%-ს შეადგენს.

2019 წლიდან ქვეყანაში ამოქმედდა დაგროვებითი პენსია, რომელშიც ჩართულია 911,897 მოქალაქე.⁶ „დაგროვებითი პენსიის შესახებ“ საქართველოს კანონის თანახმად, 40 წლისა და უფრო მეტი ასაკის მოქალაქეთათვის საპენსიო სქემაში ჩართვა არჩევითია, რის გამოც, სქემა დატოვა 40 წელს გადაცილებულმა 162,103 მოქალაქემ. შესაბამისად, იმ პირთათვის, რომლებმაც დატოვეს ან არ არიან ჩართული დაგროვებითი პენსიის სქემაში, საპენსიო ასაკში სოციალური უზრუნველყოფის ერთადერთ გარანტს სახელმწიფო პენსია წარმოადგენს. შესაბამისად, სახელმწიფო პენსია და მისი ადმინისტრირების პროცესი საშუალოვადიან პერსპექტივაში არ დაკარგავს მნიშვნელობასა და აქტუალობას.

სახელმწიფო პენსიის ადმინისტრირების პროცესს ახორციელებს სსიპ – სოციალური მომსახურების სააგენტო. სააგენტო ემსახურება საქართველოს ყველა მოქალაქეს,⁷ რომელიც კანონმდებლობის შესაბამისად უფლებამოსილია მიიღოს პენსია. აღნიშნულ პროცესში, მოქალაქეებისა და ბენეფიციარების აღრიცხვა, მათი მონაცემების დამუშავება და პენსიის დანიშვნის შესახებ გადაწყვეტილება მიიღება ინფორმაციული (ელექტრონული) სისტემის გამოყენებით. ინფორმაციული სისტემა პენსიის ადმინისტრირების ძირითადი საშუალებაა და არ გააჩნია ალტერნატივა, რის გამოც სააგენტოსთვის კრიტიკულად მნიშვნელოვანია. ასევე ინფორმაციულ სისტემას იყენებს ქვეყნის მასშტაბით არსებული 69 რაიონული სერვისცენტრი.

5 მოსახლეობის პენსიით უზრუნველყოფის 94%-ს სახელმწიფო პენსია (პროგრამული კოდი: 27 02 01), ხოლო 6%-ს – სახელმწიფო კომპენსაცია შეადგენს. აუდიტის ფარგლებში მხოლოდ ქვეპროგრამაში სახელმწიფო პენსიის წილი იქნა შესწავლილი.

6 მიმდინარე მდგომარეობით, აღნიშნული არ მოიცავს საპენსიო ასაკს მიღწეულ პირებს. კერძოდ, დაგროვებით საპენსიო სისტემაში ჩართვა სავალდებულო გახდა 40 წლამდე ასაკის ყველა დასაქმებული პირისათვის.

7 გარდა საქართველოს მოქალაქეებისა, სახელმწიფო პენსიის მიღების უფლება აქვთ:

- საქართველოში სტატუსის მქონე მოქალაქეობის არმქონე პირებს;

- პენსიის დანიშვნის თაობაზე განცხადების შეტანის მომენტისათვის ბოლო 10 წლის განმავლობაში საქართველოს ტერიტორიაზე კანონიერ საფუძველზე მუდმივად მცხოვრებ უცხო ქვეყნის მოქალაქეებს.



შესაბამისად, საპენსიო სისტემის სოციალურ-ეკონომიკური მნიშვნელობა, სახელმწიფო ბიუჯეტში საპენსიო უზრუნველყოფის ქვეპროგრამის წილის სიდიდე, ბენეფიციართა რაოდენობა და ელექტრონული სისტემის გამართული ფუნქციონირების მნიშვნელობა სახელმწიფო პენსიის ადმინისტრირების ინფორმაციული სისტემის შესწავლის საფუძველია.

1.2 აუდიტის მიზანი

აუდიტის მიზანია სახელმწიფო პენსიის ადმინისტრირების ინფორმაციული სისტემის, მისი მმართველობისა და უსაფრთხოების არსებული პრაქტიკის შეფასება. შესაბამისად, აუდიტმა უპასუხა შემდეგ კითხვას:

რამდენად უზრუნველყოფილია პენსიის მართვის ინფორმაციული სისტემის პროდუქტიულობა და მისი უსაფრთხოება?

კითხვა ჩამოყალიბდა შემდეგი ქვეკითხვების სახით:

1. რამდენად უზრუნველყოფს სახელმწიფო პენსიის ინფორმაციული სისტემის მონაცემთა სახელმწიფო პენსიის ადმინისტრირების პროცესის პროდუქტიულობას?
2. რამდენად უზრუნველყოფილია სახელმწიფო პენსიის ადმინისტრირების სისტემის უწყვეტი ფუნქციონირება?
3. რამდენად უზრუნველყოფილია სახელმწიფო პენსიის ინფორმაციულ სისტემაში არსებული მონაცემების უსაფრთხოება?
4. რამდენად დაცულია პერსონალურ მონაცემთა დამუშავების პრინციპები სახელმწიფო პენსიის ინფორმაციულ სისტემაში?

აუდიტის შედეგებზე დაყრდნობით გაიცა შესაბამისი რეკომენდაციები, რომლებიც ხელს შეუწყობს გამოვლენილი ნაკლოვანებების გამოსწორებას.

შენიშვნა:

აუდიტის მიზანი არ არის დაგროვებითი საპენსიო სისტემის შეფასება. აუდიტის ფარგლებში შესწავლილი იყო სახელმწიფო პენსიის ადმინისტრირების/მართვის ინფორმაციული სისტემა და მასთან დაკავშირებული საკითხები.

1.3 შეფასების კრიტერიუმები

სახელმწიფო პენსიის ადმინისტრირების სისტემის ზოგადი IT და აპლიკაციის კონტროლების შეფასების მიზნით, აუდიტის პროცედურების ჩატარებისას გამოყენებულ იქნა შემდეგი კრიტერიუმები:

მარეგულირებელი ნორმატიული აქტები:



- საქართველოს კანონი „სახელმწიფო პენსიის შესახებ“;
- საქართველოს კანონი „სოციალური დახმარების შესახებ“;
- საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“;
- საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“;
- მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის N2 ბრძანება „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“.

საერთაშორისო სტანდარტები და უკეთესი პრაქტიკის მაგალითები:

- სააგენტოს ინფორმაციული სისტემა SAESA, რომელიც გამოიყენება საარსებო შემწეობის პროგრამის ადმინისტრირებისთვის. აღნიშნული სისტემის აუდიტი⁸ ჩატარდა 2018 წელს და სისტემა შეირჩა როგორც უკეთესი პრაქტიკის მაგალითი სახელმწიფო პენსიის ადმინისტრირების სისტემის შესაფასებლად;
- ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ შემუშავებული ჩარჩო დოკუმენტი (framework) COBIT 5;
- ISO/IEC 27001:2013 ინფორმაციული უსაფრთხოების მართვის სისტემა – მოთხოვნები.⁹

1.4 აუდიტის მასშტაბი და მეთოდოლოგია

აუდიტის ობიექტია საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო და სსიპ – სოციალური მომსახურების სააგენტო. აუდიტის ფარგლებში შეფასდა 2014-2019 წლები.¹⁰

იმის გათვალისწინებით, რომ პენსიის ადმინისტრირების სისტემაზე წვდომა სააგენტოს გარდა აქვთ რაიონულ ცენტრებს, აუდიტის ჯგუფმა შეისწავლა სისტემის სხვადასხვა ტიპის მომხმარებლისათვის ხელმისაწვდომი ფუნქციონალი. აღნიშნული მიზნის მისაღწევად, აუდიტის ჯგუფის მიერ შესწავლის პირველ ეტაპზე განხორციელდა ვიზიტი სააგენტოს 6, ხოლო მეორე ეტაპზე – 3 ტერიტორიულ ერთეულში, რა დროსაც განხილულ იქნა სხვადასხვა ტიპის მომხმარებლის (user) დაშვებები სისტემაზე და სისტემის შესაბამისი ფუნქციონალი. ასევე მონაცემების დაცულობის შეფასების მიზნით, ჩატარდა საბოლოო მომხმარებლების სამუშაო სადგურების სკანირება მავნე კოდის შემცველ ფაილებზე.

აუდიტორული პროცედურების დაგეგმვისა და განხორციელებისას, აუდიტის ჯგუფმა იხელმძღვანელა აუდიტის შემდეგი სტანდარტებითა და სახელმძღვანელოებით:

- უმაღლესი აუდიტორული ორგანიზაციების აუდიტის საერთაშორისო სტანდარტები (ISSAIs):
 - ინფორმაციული ტექნოლოგიების აუდიტის სახელმძღვანელო – ISSAI 5100;
 - ეფექტიანობის აუდიტის სტანდარტი – ISSAI 3000;

8 სოციალურად დაუცველი ოჯახებისთვის საარსებო შემწეობის ადმინისტრირების ინფორმაციული სისტემების ეფექტიანობის აუდიტი.

9 ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements

10 2017 წელს სახელმწიფო აუდიტის სამსახურმა დაიწყო სახელმწიფო პენსიის მართვის ინფორმაციული სისტემის ეფექტიანობის აუდიტი, რომელიც მოიცავდა 2014-2016 წლებს. სააგენტოსა და თავად საპენსიო სისტემაში მიმდინარე ცვლილებების გათვალისწინებით, საჭირო გახდა მასშტაბის გაზრდა და 2017-2019 წლების შეფასება. შედეგად აუდიტმა მოიცვა 2014-2019 წლები.



- ინფორმაციული ტექნოლოგიების აუდიტის სახელმძღვანელო უმაღლესი აუდიტორული ორგანიზაციებისთვის.¹¹

აუდიტის კითხვებზე პასუხის გასაცემად გამოყენებულ იქნა შემდეგი მეთოდები:

- მარეგულირებელი ნორმების შესწავლა და ანალიზი;
- საერთაშორისო პრაქტიკის გაცნობა;
- დოკუმენტური ინფორმაციის ანალიზი;
- სახელმწიფო პენსიის ადმინისტრირების ინფორმაციული სისტემის ანალიზი;
- სახელმწიფო პენსიის ადმინისტრირების ინფორმაციული სისტემის უსაფრთხოების კონტროლების ტესტირება;
- ინტერვიუები აუდიტის ობიექტებთან.

აუდიტის ფარგლებში ასევე განხორციელდა სახელმწიფო პენსიის ადმინისტრირების პროცესის შეფასება საერთაშორისოდ აღიარებული ჩარჩო დოკუმენტის (framework) COBIT 5-ის მიხედვით.

2. ზოგადი ინფორმაცია

სახელმწიფო პენსიის ადმინისტრირებაზე პასუხისმგებელია საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო (შემდგომ – სამინისტრო) და მის სახელმწიფო კონტროლს დაქვემდებარებული საჯარო სამართლის იურიდიული პირი – სოციალური მომსახურების სააგენტო (შემდგომ – სააგენტო). პენსიის ადმინისტრირების პროცესში სამინისტროს ძირითადი ფუნქციებია: სახელმწიფო პოლიტიკების შემუშავება, განხორციელების ხელშეწყობა და პროცესისათვის საჭირო სასერვერო ინფრასტრუქტურის უზრუნველყოფა.

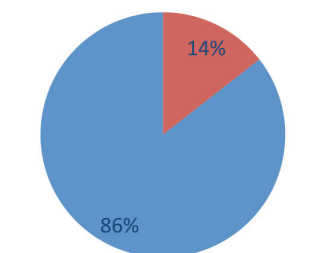
უშუალოდ პროცესის ადმინისტრირებას ახორციელებს სააგენტო, რომელიც შიდა სტრუქტურული ერთეულის – სახელმწიფო გასაცემლების დეპარტამენტის მეშვეობით ორგანიზებას უწევს პენსიის მართვასთან დაკავშირებულ ძირითად პროცესებს. საქართველოს მასშტაბით მოსახლეობის პენსიით უზრუნველყოფასთან დაკავშირებული მომსახურების განევა ხორციელდება 69 ტერიტორიული ერთეულის მეშვეობით. ტერიტორიული ერთეულები უზრუნველყოფენ კონკრეტულ სამოქმედო ტერიტორიაზე სახელმწიფო პენსიის დანიშვნასა და შეწყვეტას, საქმისწარმოებას და სხვ.

2.1 სახელმწიფო პენსიის ადმინისტრირების სისტემის მნიშვნელობა

როგორც უკვე აღინიშნა, მოსახლეობის საპენსიო უზრუნველყოფა, სამინისტროს მიერ მართული ყველაზე მოცულობითი პროგრამაა. წლების განმავლობაში, ქვეპროგრამაზე გათვალისწინებული დაფინანსების წილი სახელმწიფო ბიუჯეტში სტაბილურად მზარდი ტენდენციით გამოირჩევა და 2019 წელს 1,9 მლრდ ლარი შეადგინა.

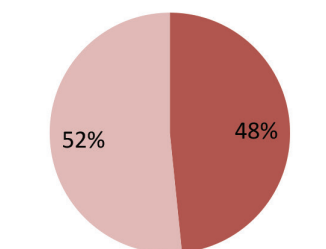
დიაგრამა N1. საპენსიო უზრუნველყოფის ქვეპროგრამის წილი სახელმწიფოსა და სამინისტროს ბიუჯეტში

სახელმწიფო ბიუჯეტი



■ საპენსიო უზრუნველყოფა
■ სხვა პროგრამები

სამინისტროს ბიუჯეტი



■ საპენსიო უზრუნველყოფა
■ სხვა პროგრამები

საპენსიო პროგრამის მასშტაბურობისა და მასზე დამოკიდებულების გათვალისწინებით, მნიშვნელოვანია პროგრამის ადმინისტრირებისათვის შემუშავებული ინფორმაციული სისტემა ფუნქციონირებდეს უწყვეტად, საიმედოდ და გამართულად. ასევე საქართველოს მთავრობის N312 დადგენილებით, სააგენტო და სამინისტრო განსაზღვრულია როგორც კრიტიკული ინფორმაციული სისტემის სუბიექტები, ვინაიდან მათი ელექტრონული სისტემების უწყვეტი ფუნქ-



ციონირება სახელმწიფოსთვის პრიორიტეტულია. შესაბამისად, აღნიშნული სისტემა (პენსიის ადმინისტრირების ინფორმაციული სისტემა) აკმაყოფილებს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით დადგენილ კრიტერიუმებს და შესაძლოა განხილულ იქნეს,¹² როგორც სახელმწიფოს კრიტიკული ინფორმაციული სისტემა.

2.1.1 სისტემის განვითარებასთან დაკავშირებული ინფორმაცია

ფულადი გასაცემლების ადმინისტრირების გაუმჯობესების მიზნით, 2005 წელს სოციალური მომსახურების სააგენტოს სახელმწიფო გასაცემლების დეპარტამენტმა შექმნა მართვის ავტომატიზებული სისტემა („პენსია 2005“). დეპარტამენტის თანამშრომლებმა შეიმუშავეს სისტემის პროგრამული კოდი და თავად ახორციელებენ მის მხარდაჭერას.

სისტემის დანერგვისა და განვითარების შედეგად, შესაძლებელი გახდა პენსიის მართვის პროცესის ავტომატიზაცია. ამ პროცესის ინფორმაციულ სისტემაში გადატანით, შეიქმნა ბენეფიციართა ელექტრონული ბაზა, რამაც გაამარტივა მონაცემთა დამუშავება და ანალიზი. თუმცა, ამ მიმართულებით წინ გადადგმული ნაბიჯების მიუხედავად, ვერ განხორციელდა პროცესების სრული ავტომატიზაცია და აუდიტის პერიოდში პენსიის ადმინისტრირებისას პროცესების გარკვეული ნაწილი კვლავ მანუალურად (ხელით), ადამიანური რესურსების ხარჯზე ხორციელდებოდა. არქიტექტურული მოწყობიდან და ტექნიკური მახასიათებლებიდან გამომდინარე, სისტემა დგას რიგი გამოწვევებისა და რისკების წინაშე. სისტემის ადმინისტრირების პროცესი, არსებული რისკები და გამოწვევები განხილულია აუდიტის მიგნებების თავში.

12 ინფორმაციული სისტემის კრიტიკულობის კლასიფიცირებას უნდა ახორციელებდეს თავად კრიტიკული ინფორმაციული სისტემის სუბიექტი (სააგენტო), თუმცა, სააგენტოს აღნიშნული არ განუხორციელებია.

3. აუდიტის მიზნები

3.1 პენსიის ადმინისტრირების სისტემა

3.1.1 პროექტულობასთან დაკავშირებული ნაკლავანებები

სახელმწიფო პენსიის ადმინისტრირების მნიშვნელოვანი კომპონენტია პენსიის დანიშვნის თაობაზე გადაწყვეტილების მიღება. კერძოდ, პენსიის დანიშვნისთვის აუცილებელია, მაძიებელმა პირმა მიმართოს სააგენტოს ნებისმიერ რაიონულ ოფისს და შეავსოს განაცხადი. განაცხადს განიხილავს სააგენტო და იღებს გადაწყვეტილებას პენსიის დანიშვნის თაობაზე.

აღნიშნული პროცესის პროდუქტიულობის შესაფასებლად, აუდიტის ჯგუფმა კრიტერიუმად გამოიყენა სააგენტოს ანალოგიური პროცესი, რომელიც უზრუნველყოფს საარსებო შემწეობის მაძიებელთათვის სოციალური დახმარების დანიშვნას. შესაბამისად, წინამდებარე ქვეთავში განხილულია სახელმწიფო პენსიისა და საარსებო შემწეობის დანიშვნის შესახებ გადაწყვეტილების მიღების პროცესები¹³ და შეფასებულია სახელმწიფო პენსიის მართვის პროდუქტიულობის საკითხები.

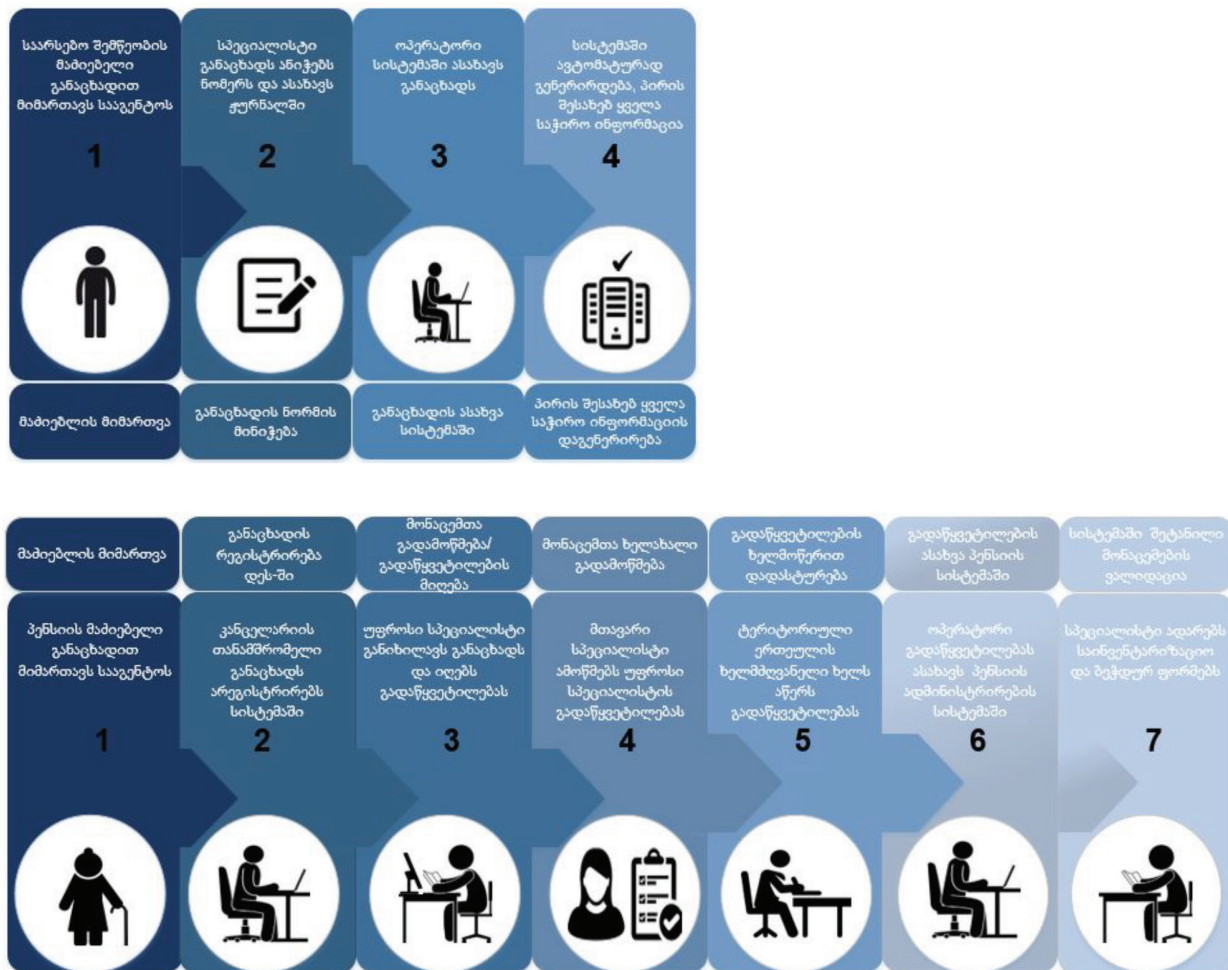
სააგენტოს მიერ ადმინისტრირებული საარსებო შემწეობის დანიშვნის პროცესი შემდეგნაირად წარმართება:

1. ბენეფიციარი სააგენტოს ნებისმიერ ტერიტორიულ ერთეულში ავსებს აპლიკაციას, საარსებო შემწეობის დანიშვნის თაობაზე.
2. სპეციალისტი განაცხადს ხელით ანიჭებს ნომერს და ასახავს ჟურნალში.
3. შევსებული განაცხადი მიეწოდება ოპერატორს, რომელიც სისტემაში ასახავს განაცხადს.
4. სისტემაში ხელით შესრულებული პროცედურების გარეშე ხდება ამ კონკრეტულ პირზე ყველა საჭირო ინფორმაციის (მაგალითად, ასაკი, კომუნალური გადასახადები, უძრავი ქონება, საზღვრის კვეთა, პატიმრობა და სხვ.) თავმოყრა და გენერაციის ფორმის ამოღება.

¹³ საარსებო შემწეობისა და სახელმწიფო პენსიის ბიზნესპროცესები თვისობრივად განსხვავდება. შედარებისთვის, შერჩეული დანიშვნის პროცესში არ არის გათვალისწინებული სოციალური აგენტის ვიზიტი და მაძიებლის საცხოვრებელი პირობების შეფასების პროცედურა.



სქემა N1. პენსიის და საარსებო შემწეობის მაძიებლის მიმართვა და აპლიკაციების განხილვის პროცესი



შედარებისთვის, სახელმწიფო პენსიის დანიშვნის პროცესი შემდეგნაირად წარიმართება:

1. პენსიის მაძიებელი პირი მიმართავს სოციალური მომსახურების სააგენტოს ნებისმიერ ოფისს, განცხადებით პენსიის დანიშვნის თაობაზე.
2. ტერიტორიული ერთეულის კანცელარიის თანამშრომლის მიერ განაცხადის ასახვა ხორციელდება დეს¹⁴ პროგრამაში.
3. განაცხადი მატერიალური და ელექტრონული ფორმით ეგზავნება უფროს სპეციალისტს, რომელიც განიხილავს დოკუმენტს, სხვადასხვა მონაცემთა ბაზასთან დადარებით (საინფორმაციო პორტალის¹⁵ ან „რესპუბლიკის ბაზის“¹⁶ გამოყენებით).
4. უფროსი სპეციალისტის შემდეგ, იმავე პროცედურას ასრულებს მთავარი სპეციალისტი.

14 დოკუმენტბრუნვის ელექტრონული სისტემა.

15 საინფორმაციო პორტალი არის ვებსერვისი, რომლის საშუალებით შესაძლებელია შემდეგი ინფორმაციის მიღება: პირის პირადი რეკვიზიტები, პირის მიერ ნებისმიერი ტიპის სახელმწიფო გასაცემლისა და საარსებო შემწეობის მიღება, მაღალმთიან დასახლებაში მუდმივად მაცხოვრებლის სტატუსი და სხვა მრავალი ტიპის ინფორმაცია კონკრეტული პიროვნების შესახებ.

16 რესპუბლიკის ბაზა - მოქალაქეთა შესახებ ინფორმაცია, მათ მიერ ნებისმიერი ტიპის გასაცემლის მიღების შესახებ.

5. საბოლოოდ, ტერიტორიული ერთეულის ოფისის უფროსი ხელმოწერით ადასტურებს გადაწყვეტილებას.
6. გადაწყვეტილება სისტემაში აისახება¹⁷ ტერიტორიული ერთეულის ოპერატორის მიერ და ხორციელდება საინვენტარიზაციო ფორმის გენერირება.
7. ოპერატორის მიერ ამობეჭდილ საინვენტარიზაციო ფორმას, უფროსი სპეციალისტი ადარებს საქმის მატერიალური ფორმით არსებულ დოკუმენტებს, სისტემაში შეტანილი მონაცემების სიზუსტის დადასტურების მიზნით.

როგორც მოცემულ სქემაზეა წარმოდგენილი, საარსებო შემწეობის შემთხვევაში, საწყისი ეტაპი – ბენეფიციარის მიმართვა, მიმართვის დამუშავება და სისტემაში ასახვა, გაცილებით ნაკლებ დროით და ადამიანურ რესურსთანაა დაკავშირებული. კერძოდ, SAESA სისტემაში განაცხადის რეგისტრაციის (ასახვის) შემდგომ, სისტემა ავტომატურად ამუშავებს მონაცემებს, ადარებს გაწე წყაროებიდან მიღებულ მონაცემებს და ამზადებს ანგარიშს (გენერაცია) დახმარების მაძიებლის შესახებ. მაგალითად, საკმარისია მაძიებელი პირის პირადი ნომერი იმისათვის, რომ სისტემამ ავტომატურად გადაამოწმოს და გამოითვალოს პირის საშუალო წლიური შემოსავალი, განსაზღვროს ასაკი, აჩვენოს ოჯახის კომუნალური ხარჯები, უძრავი ქონება, საზღვრის კვეთა და პატიმრობა. ასევე სისტემა ავტომატურად ადგენს რამდენიმე ოფისში პარალელურად, ხომ არ ითხოვს მაძიებელი საარსებო შემწეობას.

შედარებისთვის, საპენსიო სისტემაში („პენსია 2005“) განაცხადის შეყვანის შემდგომ, თანამშრომლების მიერ რამდენიმე ეტაპად მოწმდება პირის შემოსავლებისა და პატიმრობის შესახებ ინფორმაცია. ასევე ხელით ხდება იმის გადამოწმება, გაიარა თუ არა მაძიებელმა რეგისტრაცია ქვეყნის მასშტაბით არსებულ სხვა რაიონულ ერთეულში და იღებს თუ არა სახელმწიფო პენსიას. აღნიშნული გადამოწმების (ვალიდაციის) პროცესი მიმდინარეობს ყოველ ახალ განაცხადზე და ყოველთვიურად. პროცესში ჩართულია როგორც რაიონული მომსახურების, ასევე სათავო ოფისიც.

გემოხსენებული შედარება ცხადყოფს, რომ სააგენტოს ერთი პროცესი (საარსებო შემწეობის დანიშვნა) უფრო ავტომატიზებულია და შესაბამისად, უფრო პროდუქტიულია, ვიდრე მეორე (სახელმწიფო პენსიის დანიშვნა). სააგენტო უფრო კომპლექსურ ბიზნესპროცესს (საარსებო შემწეობა) წარმართავს უფრო ნაკლები ადამიანური რესურსით, ვიდრე ნაკლებად რთულ ბიზნესპროცესს (სახელმწიფო პენსია). ასევე საარსებო შემწეობის ადმინისტრირების პროცესი უფრო ზუსტი და საიმედოა, ვინაიდან ინფორმაციის გადამოწმება ხდება სისტემის მიერ და გამორიცხულია ადამიანური ფაქტორით გამოწვეული უზუსტობები. ასევე მნიშვნელოვანი განსხვავებაა სისტემის მდგრადობისა და უწყვეტი ფუნქციონირების მიმართულებით, რაც დეტალურადაა განხილული ანგარიშის მომდევნო ქვეთავებში.

¹⁷ აღსანიშნავია, რომ სათავო ოფისის მიერ ბაზების კონსოლიდაციისა და მონაცემთა საბოლოო ვალიდაციისას, შესაძლოა გამოვლინდეს ისეთი გარემოებები, რომ ბენეფიციარს უარი ეთქვას პენსიის დანიშვნაზე (გამომდინარე იქიდან, რომ ტერიტორიულ ერთეულებს არ აქვთ წვდომა სასჯელაღსრულებისა და შემოსავლების სამსახურის მიერ მოწოდებულ ერთიან მონაცემებთან).



3.1.2 სისტემის არქიტექტურა და ტექნიკური მახასიათებლები

სახელმწიფო პენსიის მართვის პროცესში ჩართულია როგორც სააგენტოს სათავო ოფისი, ასევე ქვეყნის მასშტაბით არსებული 69 რაიონული სერვისცენტრი. სისტემაში – „პენსია 2005“ თავმოყრილია საქართველოს მოქალაქეების შესახებ სხვადასხვა სახის ინფორმაცია, რომელიც საჭიროა პენსიის დანიშვნისა და გაცემისათვის. პენსიის ადმინისტრირების პროცესში, სააგენტოს სათავო ოფისსა და ტერიტორიულ ერთეულებს შორის ხდება ინფორმაციის გაცვლა და ამ ინფორმაციის გადამოწმება (ვალიდაცია).

სისტემის არქიტექტურისა და ტექნიკური მახასიათებლების შესაფასებლად, აუდიტის ჯგუფმა ჩამოაყალიბა მინიმალური კრიტერიუმები, რომელსაც უნდა აკმაყოფილებდეს სახელმწიფო პენსიის მართვის სისტემა. კერძოდ, სისტემის მნიშვნელობის, პენსიის წლიური მოცულობის, გეოგრაფიული არეალისა და სისტემის მომხმარებლების რაოდენის გათვალისწინებით, სისტემა უნდა აკმაყოფილებდეს შემდეგ კრიტერიუმებს:

- სისტემის ცენტრალიზებული მართვის შესაძლებლობა;
- სისტემის მდგრადი ფუნქციონირება.

ზემოთ მითითებული კრიტერიუმების განსაზღვრისას აუდიტის ჯგუფმა იხელმძღვანელა სააგენტოს სოციალური შემწეობის ადმინისტრირების სისტემით (SAESA), როგორც უკეთესი პრაქტიკის მაგალითით.

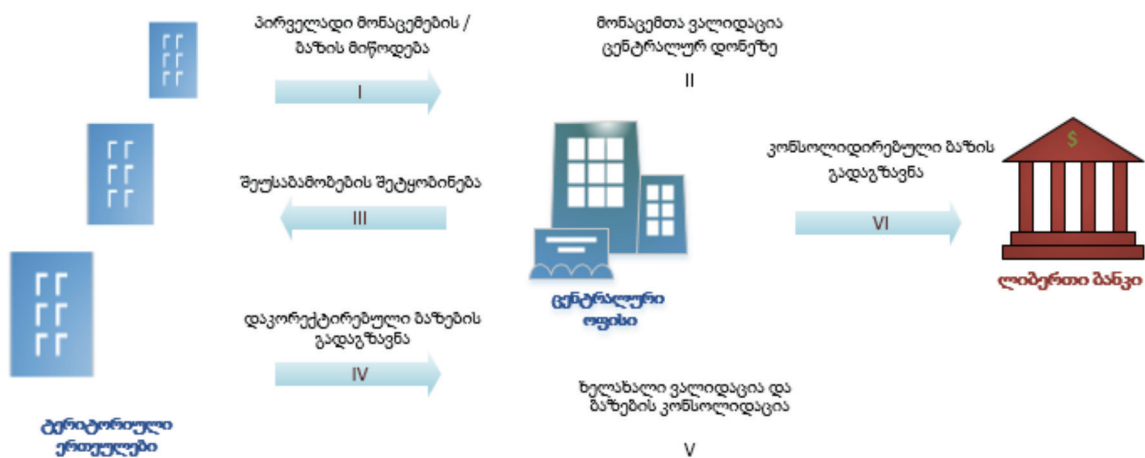
ცხრილი N1. სისტემების შედარების კრიტერიუმები

შედარების კრიტერიუმი		სახელმწიფო პენსიის სისტემა („პენსია 2005“)	საარსებო შემწეობის სისტემა (SAESA)
ცენტრალიზებული მართვა			
•	სისტემის მომხმარებლების მართვა	X	✓
•	რაიონულ ოფისებსა და სათავო ოფისში არსებული ბაზების ავტომატური კონსოლიდაცია	X	✓
•	მონაცემების ავტომატური გადამოწმება (ვალიდაცია)	X	✓
სისტემის მდგრადი ფუნქციონირება			
•	თანამედროვე ოპერაციული სისტემების მხარდაჭერა და თავსებადობა სხვა პლატფორმებთან	X	✓
•	მწარმოებლის მხარდაჭერა პროდუქტზე	X	✓
•	პროდუქტის სასიცოცხლო ციკლი (end-of-life)	2015 წელი	2027 წელი

სახელმწიფო პენსიის ადმინისტრირების ინფორმაციული სისტემა შემუშავებულია Microsoft Visual FoxPro (VFP) პლატფორმაზე და გამოირჩევა დეცენტრალიზებული არქიტექტურით. იგი ინდივიდუალურადაა ინსტალირებული თითოეული მომხმარებლის კომპიუტერზე. ცენტრალურ ოფისსა და ტერიტორიულ ერთეულებს შორის მონაცემების მიმოცვლის პრაქტიკა წარმოდგენილია ქვემოთ მოცემულ სქემაზე:



სქემა N2. სახელმწიფო პენსიის ადმინისტრირების პროცესი - ტერიტორიულ ერთეულებსა და ცენტრალურ ოფისს შორის მონაცემების მიმოცვლა



შედარებისათვის, საარსებო შემწეობის ადმინისტრირების სისტემა (SAESA) შემუშავებულია Microsoft SQL Server პლატფორმაზე და ხასიათდება ცენტრალიზებული არქიტექტურით. მონაცემების მიმოცვლა ტერიტორიულ ერთეულსა და ცენტრალურ ოფისს შორის სისტემის საშუალებით, ავტომატურად ხორციელდება.

სქემა N3. საარსებო შემწეობის ადმინისტრირების პროცესი - ტერიტორიულ ერთეულებსა და ცენტრალურ ოფისს შორის მონაცემების მიმოცვლა



საპენსიო სისტემის („პენსია 2005“) დეცენტრალიზებული არქიტექტურის გამო, საარსებო შემწეობის სისტემისგან (SAESA) განსხვავებით, სახელმწიფო პენსიის ადმინისტრირების პროცესში:

- ბაზების ფორმირება ხორციელდება ლოკალურად, ტერიტორიულ ერთეულებში;
- საჭიროა ცენტრალურ დონეზე სათავო ოფისის მიერ ბაზების კონსოლიდაცია, რაც დამატებით რესურსებთანაა დაკავშირებული;
- ვერ ხერხდება სისტემაში მონაცემების ასახვა და დაკორექტირება რეალურ დროში;
- ვერ ხერხდება პირველადი მონაცემების ავტომატურად გადამოწმება (ვალიდაცია), რაც ასევე საჭიროებს დამატებით რესურსს.

გარდა ზემოხსენებული ფაქტორებისა, ასევე მნიშვნელოვანია სისტემის მდგრადობა და ფუნქციონირება. Microsoft SQL Server-სგან განსხვავებით, Microsoft Visual FoxPro არ არის თანამედროვე და გავრცელებული პლატფორმა, რის გამოც, საჭიროების შემთხვევაში სააგენტოსათვის შესაძლოა არ იყოს ხელმისაწვდომი კვალიფიციური კადრები. სახელმწიფო პენსიის ადმინისტრირების („პენსია 2005“) მდგრადობაზე მნიშვნელოვან გავლენას ახდენს გამოყენებული პლატფორმის მდგრადობა. კერძოდ, კომპანია Microsoft-მა Visual FoxPro-ს ახალი ვერსიების გამოშვება შეწყვიტა 2007 წელს, ხოლო მხარდაჭერა 2015 წელს, რაც იმას ნიშნავს, რომ მწარმოებელი აღარ ახორციელებს ამ პროდუქტის უსაფრთხოების სისუსტეების გამოსწორებას. შესაბამისად, პროგრამა დაუცველია ახლად გამოვლენილი საფრთხეების მიმართ, რაც შესაძლოა კრიტიკულად აისახოს სისტემის ფუნქციონირებაზე. დამატებითი ინფორმაცია სისტემის მოწყვლადობასთან დაკავშირებით წარმოდგენილია ინფორმაციული უსაფრთხოების თავში.

3.1.3 IT მმართველობა და ფუნქციების გადანაწილება

აუდიტისას შეფასდა სააგენტოს IT მმართველობის პრაქტიკა და მისი ზეგავლენა პენსიის სისტემის ადმინისტრირების პროცესზე. კერძოდ, ინფორმაციული ტექნოლოგიების მმართველობის შეფასებისას გამოყენებულ იქნა საერთაშორისო ჩარჩო დოკუმენტი (framework) COBIT 5.¹⁸

COBIT 5-ის ძირითადი მიზანია ორგანიზაციაში ინფორმაციული ტექნოლოგიების მართვის უკეთესი პრაქტიკის ჩამოყალიბება, რათა მათ შეძლონ სტრატეგიული მიზნების მიღწევა ინფორმაციული ტექნოლოგიების გამოყენებით. COBIT 5 თანმიმდევრობით აყალიბებს ზოგად ნაბიჯებს (მიზნების კასკადი), თუ როგორ უნდა იქნეს მიღწეული ორგანიზაციისთვის განსაზღვრული მიზნები. დოკუმენტი ეყრდნობა 5 ძირითად პრინციპს, რომელთა შორის აღსანიშნავია:

- მართვის პროცესში უმაღლესი მენეჯმენტისა (მმართველი რგოლი) და საშუალო მენეჯმენტის როლების გამიჯვნა;
- ორგანიზაციაში (მმართველობის) ერთიანი მიდგომის ჩამოყალიბება.

უმაღლესი მენეჯმენტის (მმართველი რგოლი) ძირითადი ფუნქციებია ორგანიზაციული მიზნების/მიმართულებების განსაზღვრა, მიზნების მისაღწევად გატარებული ღონისძიებების მონიტორინგი და შეფასება; ხოლო მეორე მხრივ, საშუალო რგოლის მენეჯმენტი განსაზღვრული მიზნების მისაღწევად გეგმავს, ახორციელებს და მონიტორინგს უწევს დეტალურ აქტივობებს.

ერთიანი მიდგომა ითვალისწინებს მმართველობის სხვადასხვა დონეზე ერთიანი/კოორდინირებული მიდგომის ჩამოყალიბებას. ამ პრინციპის მისაღწევად ორგანიზაციებმა უნდა უზრუნველყონ:

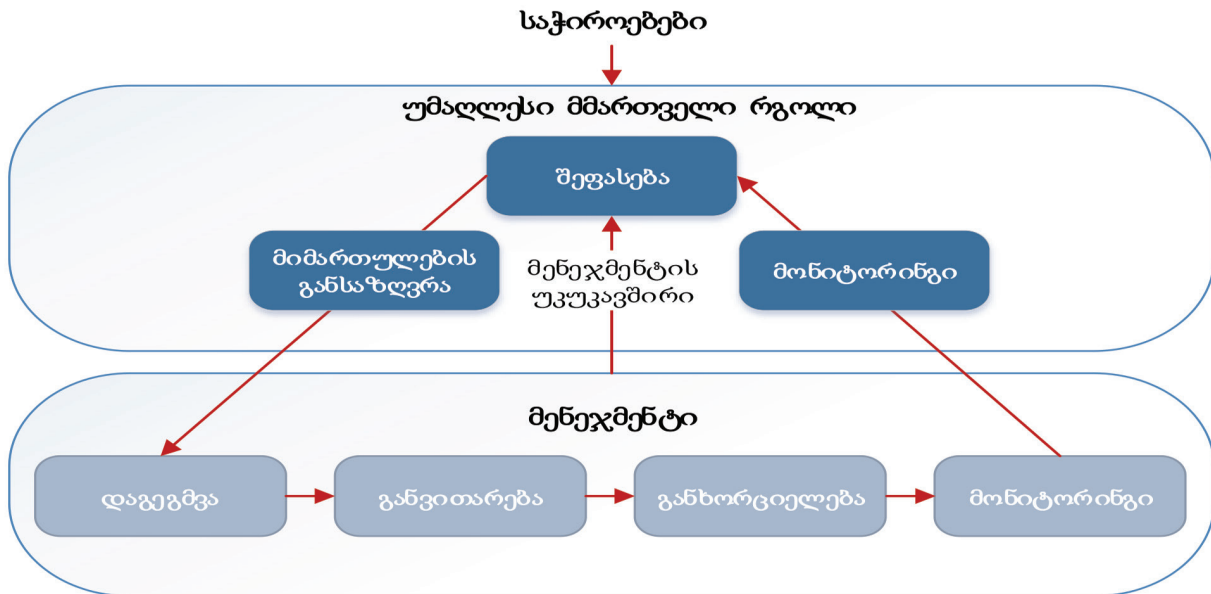
- ქმედითი ორგანიზაციული სტრუქტურის ჩამოყალიბება;
- ყველა მნიშვნელოვანი მიმართულებით ადამიანური რესურსების/კომპეტენციების სათანადო გადანაწილება;
- ინფრასტრუქტურისა და აპლიკაციების მხარდაჭერა;
- ინფორმაციის მართვის გამართული პრაქტიკის ჩამოყალიბება;
- ორგანიზაციაში არსებული პროცესების ფორმალიზება და ამ პროცესებზე შესაბამისი პასუხისმგებელი რგოლის განსაზღვრა.

¹⁸ ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ შემუშავებული ჩარჩო დოკუმენტი COBIT (control objectives for information and related technology)



COBIT 5 დეტალურად აყალიბებს პროცესებს, მათ თანმიმდევრობას და ამ პროცესებზე როლებისა და პასუხისმგებლობების განაწილებას, მმართველობის სხვადასხვა რგოლის მიხედვით.

სქემა N4. COBIT 5 – მმართველობისა და მენეჯმენტის გამიჯვნა

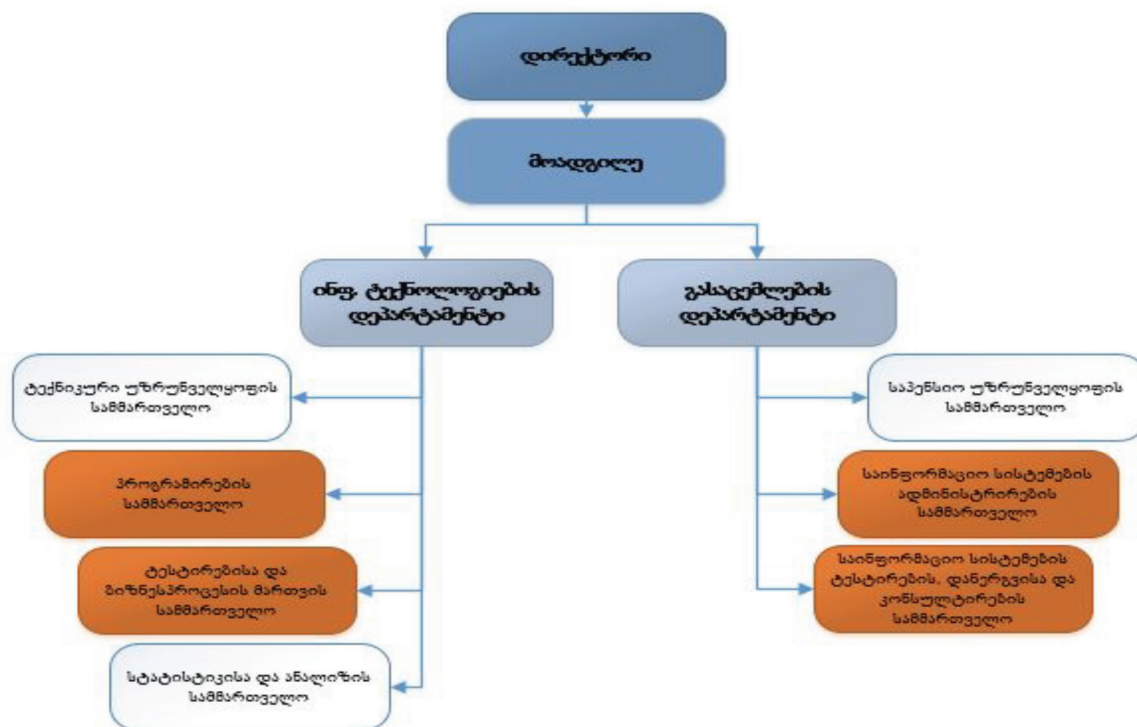


შედეგად, ორგანიზაციაში დანერგილი ინფორმაციული სისტემები თავსებადია ერთმანეთთან, ხასიათდება მსგავსი არქიტექტურით, ადეკვატურად და თანაბრად უზრუნველყოფილია კომპეტენტური კადრებით, აკმაყოფილებს ინფორმაციული უსაფრთხოების ერთი და იმავე დონის მოთხოვნებს და საბოლოოდ, ხელს უწყობს ორგანიზაციული მიზნების შესრულებას. **აღნიშნულის მისაღწევად, ორგანიზაციის უმაღლესი მენეჯმენტი უნდა აყალიბებდეს საკუთარ მოთხოვნებს, გასცემდეს დავალებებს მენეჯმენტის მიმართ და შემდგომ უნდა უზრუნველყოფდეს განხორციელებული საქმიანობის მონიტორინგს.**

სოციალური მომსახურების სააგენტოს ადმინისტრირების სფეროში შემავალი სოციალური, ჯანმრთელობის დაცვისა და დასაქმების პროგრამების საჭირო პროგრამული უზრუნველყოფის შემუშავებაზე/შექმნაზე პასუხისმგებელი სტრუქტურული ერთეულია ინფორმაციული ტექნოლოგიების დეპარტამენტი და მისი სამმართველოები. თუმცა, სახელმწიფო გასაცემლებისა და სახელმწიფო პენსიის ადმინისტრირება და ტექნიკური მხარდაჭერა, სხვა სისტემებისგან დამოუკიდებლად, გასაცემლების დეპარტამენტის მიერ ხორციელდება. კერძოდ, გასაცემლების დეპარტამენტში არსებობს „საინფორმაციო სისტემების ტესტირების, დანერგვის და კონსულტირების სამმართველო“ და „საინფორმაციო სისტემების ადმინისტრირების სამმართველო“, რომელთა ძირითადი მიზანია პენსიის მართვის პროცესში გამოყენებული ინფორმაციული სისტემის ადმინისტრირება და მხარდაჭერა. ზემოაღნიშნული დეპარტამენტები ექვემდებარება სააგენტოს დირექტორის ერთსა და იმავე მოადგილეს.



სქემა N5. სააგენტოს ინფორმაციული ტექნოლოგიებისა და გასაცემლების დეპარტამენტები



საპენსიო უზრუნველყოფის ინფორმაციული სისტემის ადმინისტრირება ხორციელდება სხვა სისტემებისგან დამოუკიდებლად და სისტემა არ არის ინტეგრირებული სააგენტოს სხვა ინფორმაციულ სისტემებთან (მაგალითად, საარსებო შემწეობის სისტემა, საყოველთაო ჯანდაცვის სისტემა და ა.შ.). ასევე, პენსიის ადმინისტრირების სისტემა, როგორც ანგარიშის მომდევნო თავშია განხილული, აკმაყოფილებს ინფორმაციული უსაფრთხოების უფრო დაბალ სტანდარტს.

სააგენტოს სოციალური პროგრამები ერთმანეთთან მჭიდროდ უკავშირდება და საჭიროებენ მონაცემთა ერთმანეთში მიმოცვლას. მაგალითად, საარსებო შემწეობის გაცემის პროცესში, პენსიონერთა მონაცემების მიწოდების მიზნით, გასაცემლების დეპარტამენტი Microsoft Access ბაზის ფაილს განათავსებს ფაილების გაზიარების სერვერზე, ინფორმაციული ტექნოლოგიების დეპარტამენტის სტატისტიკისა და ანალიზის სამმართველოს კი ეს ბაზა გადააქვს საკუთარ გარემოში და შემდგომ დაამუშავებს მას.

გემოთ მითითებული არსებითი სხვაობები სააგენტოს მფლობელობაში მყოფ სისტემებს შორის გამოწვეულია იმით, რომ სააგენტოს არ გააჩნია ერთგვაროვანი მიდგომა ინფორმაციული სისტემების მიმართ. ასევე შეუსაბამოაა კრიტერიუმის (COBIT 5) სხვა მოთხოვნებშიც (ორგანიზაციული სტრუქტურა, საკადრო რესურსები, მონაცემთა მართვა). აღნიშნული სხვაობები გამოწვეულია იმით, რომ სააგენტოს მაღალი რგოლის მენეჯმენტს არ აქვს ჩამოყალიბებული მოთხოვნები მისთვის საჭირო კრიტიკული ინფორმაციული სისტემების მიმართ.

დასკვნა

სახელმწიფო პენსიის ადმინისტრირების სისტემის შესწავლისას განხილულ იქნა უკეთესი პრაქტიკის მაგალითი (საარსებო შემწეობის ადმინისტრირების სისტემა) და საუკეთესო პრაქტიკის მაგალითი (COBIT 5). უკეთესი პრაქტიკის მაგალითი ცხადყოფს, რომ სახელმწიფო პენსიის ადმინისტრირების პროცესში მნიშვნელოვანი ადამიანური და დროის რესურსი იხარჯება ისეთ პროცესებზე, რომლის ავტომატიზება შესაძლებელია სააგენტოს ხელთ არსებული რესურსებით. ხელით შესრულებული პროცესები და განმეორებითი გადამოწმებები (ვალიდაციები) მნიშვნელოვნად ზრდის ადამიანური ფაქტორით გამოწვეული შეცდომის რისკებს. ამასთანავე, სისტემის დეცენტრალიზებული მოწყობა, მომხმარებლების რაოდენობა, გეოგრაფიული გავრცელების არეალი ართულებს მის ცენტრალიზებულ მართვას.

მნიშვნელოვანი გაუმჯობესების პოტენციალი არსებობს პენსიის ადმინისტრირების სისტემის არქიტექტურის, სხვა სისტემებთან ინტეგრაციისა და მდგრადობის მიმართულებით. აუდიტი ცხადყოფს, რომ პენსიის ადმინისტრირების სისტემა მოძველებულია (legacy system), არ აქვს მწარმოებლის მხარდაჭერა და მოწყვლადია ახლად გამოვლენილი საფრთხეების მიმართ.

ზემოაღნიშნული არსებითი მიგნებები განჭვრეტადი და გამოსწორებადია ორგანიზაციაში ინფორმაციული ტექნოლოგიების მმართველობის დანერგვით. სააგენტოს დაქვემდებარებაში მყოფი ინფორმაციული ტექნოლოგიების დეპარტამენტი და სახელმწიფო გასაცემლების დეპარტამენტი ხელმძღვანელობს ინდივიდუალური მიდგომით საარსებო შემწეობის ადმინისტრირებისა და სახელმწიფო პენსიის ადმინისტრირების სისტემის განვითარებისას და მხარდაჭერისას. აღნიშნული განსხვავებული მიდგომა ზემოთ მითითებული ნაკლოვანებების (არაპროდუქტიული ბიზნესპროცესი, არაინტეგრირებული სისტემები, არაცენტრალიზებული მართვა) მთავარი გამომწვევი მიზეზია, რაც თავის მხრივ, გამოწვეულია სააგენტოს უმაღლესი რგოლის მენეჯმენტის მმართველობის არსებული პრაქტიკით. კერძოდ, სააგენტოს მმართველ რგოლს არ აქვს შეფასებული სააგენტოს ინფორმაციული სისტემების მიმართ საჭირო მინიმალური მოთხოვნები და არ განსაზღვრავს ცენტრალიზებულ მიმართულებას, რომელსაც უნდა მიყვებოდნენ სააგენტოს დეპარტამენტები. ასევე სააგენტოს უმაღლესი მენეჯმენტი არ აწარმოებს ინფორმაციული სისტემების მონიტორინგს, რაც საშუალებას მისცემდა მას დროულად გამოეცლინა ზემოაღნიშნული ნაკლოვანებები და გადაედგა ნაბიჯები რისკების სამართავად.

რეკომენდაცია

სახელმწიფო პენსიის ადმინისტრირების ბიზნესპროცესის გაუმჯობესების მიზნით, სააგენტომ, მის მფლობელობაში არსებული სისტემებისა და გამოცდილების გათვალისწინებით:

- შეიმუშაოს პენსიის ადმინისტრირების სისტემის განვითარების გეგმა, რომელიც უნდა ითვალისწინებდეს პენსიის ადმინისტრირების სისტემის ცენტრალიზებული მართვის შესაძლებლობას და თავსებადობას სოციალური უზრუნველყოფის სფეროს სხვა სისტემებთან;
- პენსიის ადმინისტრირების ბიზნესპროცესის პროდუქტიულობისა და საიმედოობის გაზრდის მიზნით, უზრუნველყოს პენსიის ადმინისტრირების ინფორმაციული სისტემის ავტომატიზაცია, რაც პირველ რიგში გულისხმობს სათავო ოფისსა და ტერიტორიულ ერთეულებს შორის მონაცემთა ავტომატურ მიმოცვლას. ასევე უზრუნველყოს პენსიის ადმინისტრირების ეტაპების ავტომატიზაცია, რაც გულისხმობს მანუალურად (ხელით) ჩატარებული პროცედურების შემცირებას.



3.2 ინფორმაციული უსაფრთხოება

სახელმწიფო პენსიის ადმინისტრირების ინფორმაციული სისტემა მოიცავს ბენეფიციარების შესახებ პერსონალურ ინფორმაციას და უზრუნველყოფს სოციალური სფეროს ერთ-ერთი მნიშვნელოვანი კომპონენტის ადმინისტრირებას. სისტემა ემსახურება ქვეყნის მასშტაბით არსებულ ყველა რეგიონს და მსხვილ დასახლებას, რაც საბოლოო ჯამში უზრუნველყოფს ქვეყნის ყველა უფლებამოსილ პირზე (დაახლოებით, 760 ათასი პირი) სახელმწიფო პენსიის გაცემას.

შესაბამისად, სისტემის მნიშვნელობის გათვალისწინებით, უზრუნველყოფილი უნდა იქნეს სახელმწიფო პენსიის ადმინისტრირების სისტემის ინფორმაციული უსაფრთხოება. აღნიშნული გულისხმობს სისტემაში არსებული მონაცემების კონფიდენციალობის უზრუნველყოფას, მონაცემების მთლიანობის დაცვასა და სისტემის ხელმისაწვდომობას (უწყვეტ ფუნქციონირებას). ასევე, მონაცემების სენსიტიურობის გათვალისწინებით, მნიშვნელოვანია დაცულ იქნეს კანონმდებლობით განსაზღვრული პერსონალურ მონაცემთა დამუშავების პრინციპები.

შემდეგ ქვეთავებში წარმოდგენილია სააგენტოში პერსონალურ მონაცემთა დაცვისა და ინფორმაციული უსაფრთხოების შესახებ საქართველოს კანონმდებლობით განსაზღვრული მოთხოვნების შესრულების მდგომარეობა.

საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“ ინფორმაციულ უსაფრთხოებას განმარტავს, როგორც საქმიანობას, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას. სააგენტო განსაზღვრულია როგორც კრიტიკული ინფორმაციული სისტემის სუბიექტი¹⁹ და შესაბამისად, ვალდებულია უზრუნველყოს ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესრულება. სააგენტოს, როგორც კრიტიკული ინფორმაციული სისტემის სუბიექტს, ევალება²⁰ ინფორმაციული უსაფრთხოების მართვის სისტემის (შემდგომ – იუმს) შექმნა და დანერგვა.

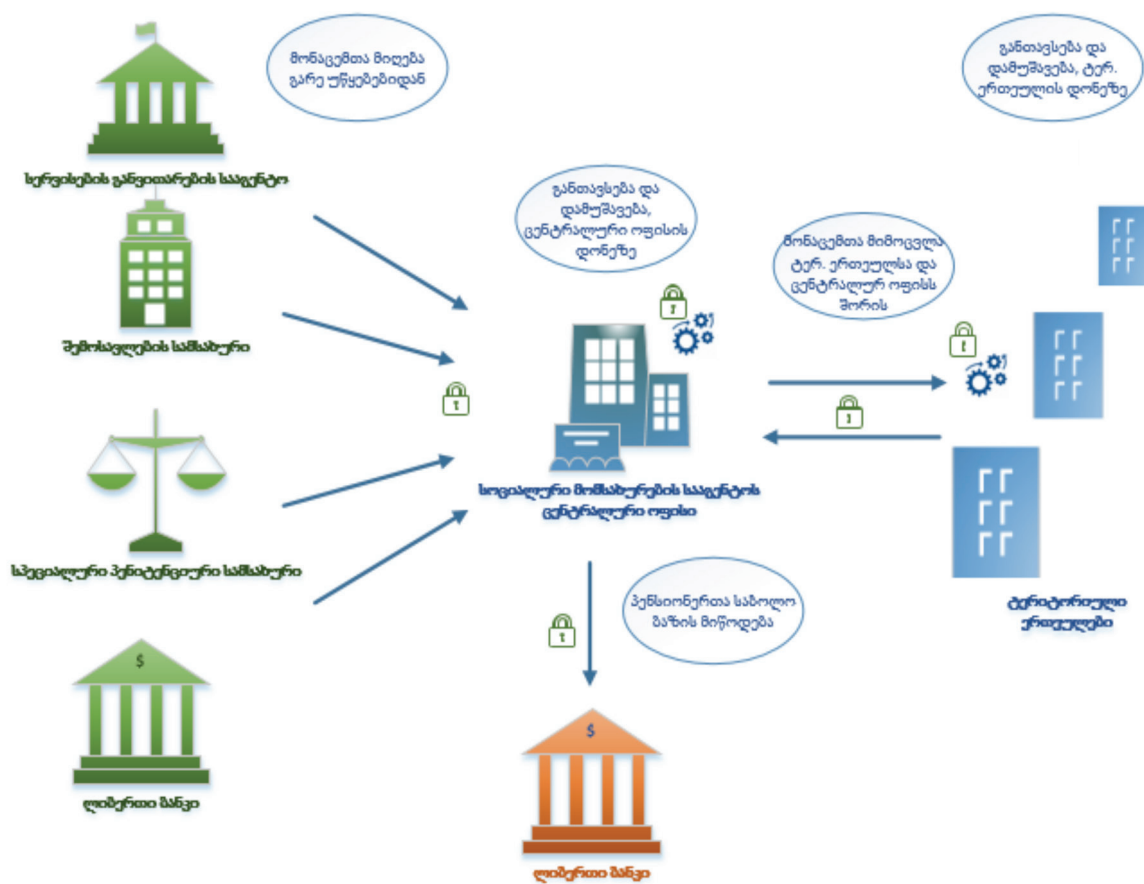
იუმს-ის ფარგლებში სააგენტომ უნდა შეიმუშაოს ინფორმაციული უსაფრთხოების პოლიტიკა და დანერგოს კონტროლის მექანიზმები ინფორმაციის კონფიდენციალურობის, ხელმისაწვდომობისა და მთლიანობის უზრუნველსაყოფად. ამასთანავე, სააგენტო ვალდებულია განსაზღვროს ინფორმაციული უსაფრთხოების მართვის განხორციელებაზე პასუხისმგებელი პირი ან პირები,²¹ განსაზღვროს უსაფრთხოების პოლიტიკების გავრცელების სფერო და შეიმუშაოს ინფორმაციული უსაფრთხოების კონტროლები.

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

20 საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“, ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები.

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

სქემა N6. სახელმწიფო პენსიის ადმინისტრირების პროცესი - მონაცემთა ნაკადები



დიაგრამაზე მოცემულ სახელმწიფო პენსიის ადმინისტრირების პროცესში, სააგენტო ვალდებულია უზრუნველყოს:

- სახელმწიფო პენსიის ადმინისტრირების სისტემის უწყვეტი ფუნქციონირება,²² რაც გულისხმობს სისტემის შეუფერხებელ ფუნქციონირებას;
- გარე წყაროებიდან (სსიპ - სერვისების განვითარების სააგენტო, სსიპ - შემოსავლების სამსახური, სპეციალური პენიტენციური სამსახური, სს „ლიბერთი ბანკი“) მიღებული და რაიონულ ოფისებთან გაცვლილი ინფორმაციის კონფიდენციალურობა და მთლიანობა, რაც გულისხმობს ინფორმაციის დაცვას უნებართვო მოდიფიკაციისაგან (მესამე მხარის მიერ) და უნებართვო გამჟღავნებას არაავტორიზებული პირების მიერ;
- სათავო ოფისსა და რაიონულ ოფისებში არსებული მონაცემების კონფიდენციალურობის, მთლიანობისა და პრიატულობის დაცვა, რაც გულისხმობს მონაცემებზე არასანქცირებული წვდომის შეზღუდვას, არაავტორიზებული ცვლილებების პრევენციას და პერსონალური მონაცემების დამუშავების პრინციპების დაცვას.

აუდიტის ფარგლებში შესწავლილ იქნა სააგენტოს ინფორმაციული უსაფრთხოების კონტროლები და პერსონალური მონაცემების დამუშავების პრაქტიკა. აღნიშნულისათვის, აუდიტორული პროცედურები ჩატარდა როგორც სათავო ოფისში, ასევე შერჩეულ რაიონულ ოფისებში.

²² საერთაშორისო პრაქტიკის თანახმად, არ არის აუცილებელი, რომ სისტემა ფუნქციონირებდეს უწყვეტად, ²⁴ საათის განმავლობაში. შესაძლებელია, სისტემას ჰქონდეს წყვეტა, მაგრამ ამან გავლენა არ უნდა მოახდინოს ბიზნესპროცესზე.

არსებული მდგომარეობით, სააგენტოს არ აქვს შესრულებული ინფორმაციული უსაფრთხოების შესახებ არსებული საკანონმდებლო მოთხოვნები, რაც პირველ რიგში გულისხმობს ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) შექმნას და შესაბამისი კონტროლების დანერგვას.

ცხრილი N2. ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები

მოთხოვნები	შესრულების მაჩვენებელი
ორგანიზაციაში ინფორმაციული უსაფრთხოების აუცილებლობის გაცნობიერება და ხელმძღვანელობის მხრიდან მხარდაჭერა	☒
ინფორმაციული უსაფრთხოების მენეჯერი	☒
ორგანიზაციული მოწყობა (ინფორმაციული უსაფრთხოების საბჭო)	☒
გავრცელების სფერო	☒
იუმს-ის პოლიტიკა	☒
აქტივების მართვა	☒
რისკების მართვა	☒
კონტროლის ეფექტიანობის გაზომვის მექანიზმები	☒
იუმს-ის აუდიტი	☒
ინფორმაციული უსაფრთხოების ინციდენტების მართვის პროცედურები	☒

აუდიტისას შესწავლილ იქნა აღნიშნული საკანონმდებლო მოთხოვნების პრაქტიკული იმპლემენტაცია (გადათარგმნა ბიზნესპროცესების შესაბამისად) და შეფასდა შესაბამისი კონტროლების ეფექტიანობა.

3.2.1 სისტემის ხელმისაწვდომობა

ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების თანახმად,²³ სააგენტო ვალდებულია უზრუნველყოს სახელმწიფო პენსიის ადმინისტრირების სისტემის ხელმისაწვდომობა (უწყვეტობა). აღნიშნული მოთხოვნა გულისხმობს ბიზნესის წყვეტის წინააღმდეგ და ბიზნესის კრიტიკული პროცესების დასაცავად მიმართული ქმედებების (კონტროლების) დანერგვას, რომელიც ინფორმაციული სისტემის მნიშვნელოვანი შეფერხების ან სტიქიური უბედურების შემთხვევაში უზრუნველყოფს ბიზნესპროცესის დროულ აღდგენას. სააგენტომ უნდა შეაფასოს უწყვეტობასთან დაკავშირებული რისკები, რის საფუძველზეც უნდა განხორციელდეს უწყვეტობის გეგმებისა და კატასტროფიდან აღდგენის გეგმების შემუშავება (disaster recovery plan). აუცილებელია აღნიშნული გეგმები იყოს განახლებული და პერიოდულად ხორციელდებოდეს მათი ტესტირება საჭიროების შემთხვევაში პროცესებისა და სისტემის აღდგენის მიზნით.

23 მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის N2 ბრძანება „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“, ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები, დანართი „ა“. 14. ბიზნესის უწყვეტობის მართვა.

როგორც უკვე აღინიშნა, სახელმწიფო პენსიის ადმინისტრირების სისტემა დეცენტრალიზებულია (ინდივიდუალურად ინსტალირებულია ყველა კომპიუტერზე) და მას იყენებს ქვეყნის მასშტაბით არსებული 69 რაიონული ოფისი. აღნიშნულის გათვალისწინებით, იმ შემთხვევაში, თუკი მოხდება რისკების რეალიზება (პროგრამის ტექნიკური გაუმართაობა, ოპერაციულ სისტემასა და სისტემურ განახლებებთან თავსებადობის პრობლემა), სააგენტო ვერ გამოიყენებს მწარმოებლის ტექნიკურ დახმარებას და მოუწევს საკუთარი ძალებით აღადგინოს სისტემის ფუნქციონირება.

სააგენტოს არ აქვს შეფასებული სისტემის უწყვეტ ფუნქციონირებასთან დაკავშირებული რისკები და ამასთანავე, არ აქვს დანერგილი ამ რისკების მაკომპენსირებელი მექანიზმები. კერძოდ, იუმს-ის დანერგვის ფარგლებში, სააგენტოს არ შეუფასებია პენსიის ადმინისტრირების სისტემასთან დაკავშირებული მონაცვლადობები და სისტემის ფუნქციონირების წყვეტის საფრთხე, რის საფუძველზეც უნდა დაენერგა შესაბამისი კონტროლები. სისტემასთან დაკავშირებული ტექნიკური ხარვეზის რეალიზების (რომლის მოხდენის ალბათობა დაბალია) შემთხვევაში, სააგენტოს მოუწევს შემჭიდროებულ ვადებსა და საგანგებო რეჟიმში ინციდენტზე რეაგირება, რაც გულისხმობს:

- ინციდენტის წყაროს დადგენას (რამ გამოიწვია ინციდენტი);
- გავრცელების არეალის დადგენას (რამდენ სამუშაო სადგურზე ან რაიონულ ოფისზე გავრცელდა ხარვეზი);
- ტექნიკური ხარვეზის გადაჭრის გზის მოძიებას (როგორ შეიძლება ხარვეზის აღმოფხვრა);
- ტექნიკური ხარვეზის გასწორებას (ხარვეზის აღმოფხვრა).

სააგენტოს ინფორმაციული ტექნოლოგიების სპეციალისტების გამოცდილებისა და კვალიფიკაციის მიუხედავად, რომლებიც სისტემის მხარდაჭერას უზრუნველყოფენ, სისტემის გეოგრაფიული არეალის, მომხმარებლების რაოდენობისა და მატერიალურ-ტექნიკური ბაზის გათვალისწინებით, ზემოაღნიშნული პროცედურების დროულად ჩატარება შესაძლოა იყოს გამოწვევა. სახელმწიფო პენსია სოციალური სფეროს მნიშვნელოვანი კომპონენტია და შესაბამისად, მნიშვნელოვანია, რომ სააგენტომ გაითვალისწინოს არსებული რისკები და შეიმუშაოს შესაბამისი მოპყრობის გეგმა.

3.2.2 ინფორმაციის მიმოხვდის უსაფრთხოება

სახელმწიფო პენსიის ადმინისტრირების პროცესში სააგენტო იყენებს სხვადასხვა გარე უწყების მონაცემებს. წინამდებარე ცხრილში წარმოდგენილია დეტალური ინფორმაცია გარე უწყებებიდან მიღებული მონაცემების თაობაზე.



ცხრილი N3. გარე წყაროებიდან მიღებული მონაცემები

უწყება	ბაზა	მონაცემები	მონაცემების კატეგორია	მონაცემების მოცულობა
სერვისების განვითარების სააგენტო	მოქალაქეთა პირადი მონაცემები	- პირის სახელი, გვარი - პირადი ნომერი - ნასამართლეობის სტატუსი - მოქალაქეობის სტატუსი - მისამართი - დაბადების თარიღი	პერსონალური / განსაკუთრებული კატეგორიის	საქართველოს ყველა მოქალაქის შესახებ ინფორმაცია
შემოსავლების სამსახური	მოქალაქეთა შემოსავლები	- პირის სახელი, გვარი - პირადი ნომერი - დაბადების თარიღი - სამუშაო ადგილი / დამსაქმებელი - პირის შემოსავალი	პერსონალური	ყველა მოქალაქის დეკლარირებული შემოსავლის შესახებ ინფორმაცია ²⁴
სპეციალური პენიტენციური სამსახური	მოქალაქეთა პატიმრობის ან წინასწარი პატიმრობის შესახებ მონაცემები	- პირის სახელი, გვარი - პირადი ნომერი - დაბადების თარიღი - სასჯელის დასაწყისი - სასჯელის დასასრული - სასჯელის ტიპი - დანესებულება	პერსონალური / განსაკუთრებული კატეგორიის	ყველა პირის პატიმრობის ან წინასწარი პატიმრობის შესახებ ინფორმაცია
ლიბერთი ბანკი	ნ თვის განმავლობაში მოქალაქის საპენსიო ანგარიშზე უმოძრაობის შესახებ მონაცემები	- პირის სახელი, გვარი - პირადი ნომერი - შეჩერების მიზეზი	პერსონალური	ინფორმაცია იმ პენსიონერთა შესახებ, რომელთა საპენსიო ანგარიშზე არ განხორციელებულა ტრანზაქცია ნ თვის განმავლობაში ²⁵
სოციალური მომსახურების სააგენტო	„რესპუბლიკის ბაზა“ – მოქალაქეთა მიერ ნებისმიერი ტიპის სახელმწიფო გასაცემლის მიღების შესახებ მონაცემები	- პირის სახელი, გვარი - პირადი ნომერი - მისამართი - სახელმწიფო გასაცემლის დასახელება - სახელმწიფო გასაცემლის ოდენობა	პერსონალური / განსაკუთრებული კატეგორიის	საქართველოს ყველა მოქალაქის შესახებ ინფორმაცია, რომელიც იღებს ან იღებდა ნებისმიერი ტიპის სახელმწიფო გასაცემელს.

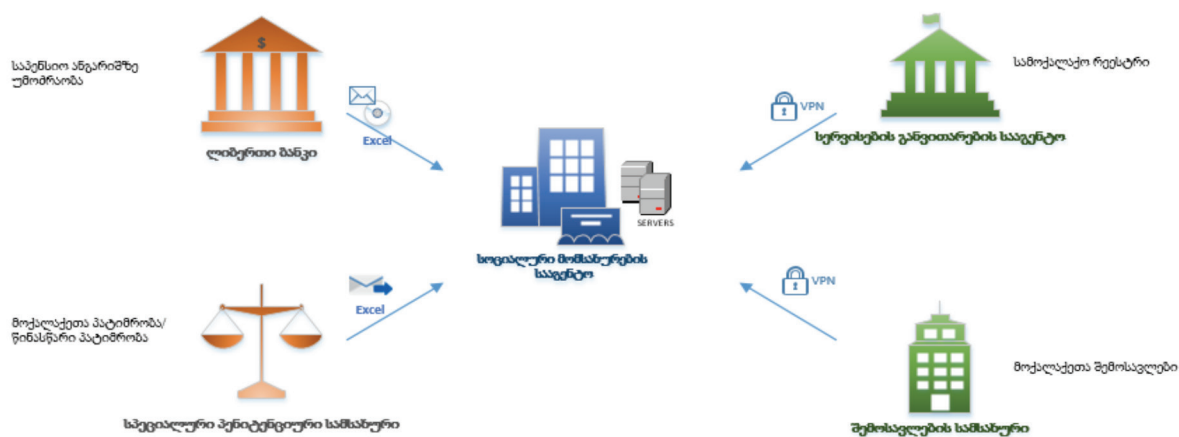
24 აღნიშნულ ბაზაში არ ფიქსირდებიან მხოლოდ იმ სამსახურის თანამშრომლები, რომლებიც საკუთარ სახელფასო განაკვეთებს კონფიდენციალურ სტატუსს ანიჭებენ.

25 გარდა ამისა, ბანკიდან იგზავნება შემდეგი ტიპის ინფორმაცია: მინდობილობა არ განახლებულა ერთი წლის განმავლობაში, პენსიის დეპოზიტზე გადატანიდან ერთი წლის განმავლობაში არ მიუმართავთ ბანკისთვის, უკან დასაბრუნებელი თანხების სტატუსის შესახებ ინფორმაცია.

სააგენტო ვალდებულია უზრუნველყოს გარე წყაროებიდან მიღებული და გაცვლილი ინფორმაციის მთლიანობა და კონფიდენციალობა, რაც გულისხმობს ინფორმაციის დაცვას უნებართვო მოდიფიკაციისგან (მესამე მხარის მიერ) და უნებართვო გამჟღავნებას არაავტორიზებული პირების მიერ. აღნიშნული მიზნის მისაღწევად არსებობს 2 გზა:²⁶ ა) მონაცემების შემცველი ფაილის დაშიფვრა ძლიერი კრიპტოგრაფიული ალგორითმით; ბ) მონაცემების გაცვლა დაცული საკომუნიკაციო არხის საშუალებით. პირველი მეთოდი უზრუნველყოფს, რომ იმ შემთხვევაში, თუ არაავტორიზებული პირი მოიპოვებს ფაილზე წვდომას, ის ვერ შეძლებს მონაცემების წაკითხვას და მათ მოდიფიცირებას სააგენტოსგან შეუმჩნევლად. შესაბამისად, ეს მეთოდი უზრუნველყოფს მონაცემების კონფიდენციალობის, მთლიანობისა (მონაცემების სისრულე და სიზუსტე) და ავთენტურობის (წარმომავლობის) დადასტურებას. მეორე მეთოდი უზრუნველყოფს, რომ მესამე მხარემ ვერ შეძლოს წვდომა მოიპოვოს მონაცემების შემცველ ფაილზე მისი ტრანსპორტირებისას და ვერ შეძლოს ამ მონაცემების წაკითხვა ან შეცვლა. რაც უფრო მეტად სენსიტიურია ინფორმაცია, მით უფრო მეტად მნიშვნელოვანია, გამოყენებული უსაფრთხოების კონტროლები იყოს უფრო მეტად საიმედო (უფრო ძლიერი დაშიფვრის ალგორითმი, უფრო მეტად დაცული საკომუნიკაციო არხი და ა.შ.).

პენსიის ადმინისტრირების პროცესში სააგენტო იყენებს არაერთგვაროვან მიდგომას გარე წყაროებიდან მონაცემების მიღებისა და გადამონმებისთვის (ვალიდაციისთვის). კერძოდ, სააგენტო იყენებს დაცულ საკომუნიკაციო არხს (ვირტუალურ კერძო ქსელს – VPN-ს) – სსიპ – სერვისების განვითარების სააგენტოსთან და სსიპ – შემოსავლების სამსახურთან, ხოლო სპეციალურ პენიტენციურ სამსახურთან და სს „ლიბერთი ბანკთან“ მონაცემების გაცვლა ხორციელდება ლაზერული დისკის (CD) და ელექტრონული დოკუმენტბრუნვის სისტემის (სისტემა – დეს) საშუალებით.

სქემა N 7. გარე უწყებებთან მონაცემთა მიმოცვლა



ლაზერული დისკისა და ელექტრონული დოკუმენტბრუნვის გამოყენების შემთხვევაში, მონაცემების გაცვლა საფრთხის შემცველია. კერძოდ, სააგენტო და გარე უწყებები,²⁷ აღნიშნულ მონაცემებს ცვლიან დაუცველი საკომუნიკაციო არხის საშუალებით და ამასთანავე, მონაცემების შემცველი ფაილებისთვის არ გამოიყენება დამატებითი დაცვის კონტროლები (მაგალითად, შიფრაცია – კონფიდენციალობის დასაცავად, ჰეშირება – მთლიანობის დასაცავად). შესაბამისად, მოქალაქეებისა და საპენსიო სისტემის ბენეფიციარების შესახებ მონაცემები, მათ შორის, პერსონალური და განსაკუთრებული კატეგორიის პერსონალური მონაცემები, საფრთხეების მიმართ სათანადო ხარისხით დაცული არ არის.

26 შესაძლებელია ორივე მეთოდის ერთდროულად გამოყენებაც.

27სს „ლიბერთი ბანკი“ და სპეციალური პენიტენციური სამსახური



3.2.3 ღამუშავებუი ინფორმაციის უსაფრთხოება

სააგენტო ვალდებულია უზრუნველყოს სათავო ოფისისა და რაიონულ ოფისებში არსებული მონაცემების კონფიდენციალობის, მთლიანობისა და პერსონალური მონაცემების დამუშავების პრინციპების დაცვა, რაც გულისხმობს მონაცემებზე არასანქცირებული წვდომის შეზღუდვას, არავტორიზებული ცვლილებების პრევენციას და პერსონალური მონაცემების იმგვარ დამუშავებას, როგორიც აუცილებელი და საკმარისია ბიზნესპროცესით. აღნიშნული მიზნის მისაღწევად, სააგენტო ვალდებულია:

- უზრუნველყოს იმ სამუშაო სადგურების (კომპიუტერების, საბოლოო მომხმარებლების) უსაფრთხოება, სადაც მუშავდება მონაცემები;
- განსაზღვროს მონაცემებზე დაშვების მქონე პირები და გააკონტროლოს ამ მონაცემების გამოყენება მხოლოდ სამსახურებრივი მოვალეობის შესასრულებლად;

მომდევნო ქვეთავებში განხილულია ზემოაღნიშნულ საკითხებთან დაკავშირებული მიგნებები.

სამუშაო სადგურების უსაფრთხოება

პენსიის ადმინისტრირების უდიდესი ნაწილს ახორციელებენ ტერიტორიული ერთეულები. როგორც უკვე აღინიშნა, სამუშაო პროცესში რაიონული ოფისები იყენებენ პერსონალურ და განსაკუთრებული კატეგორიის მონაცემებს. სისტემის დეცენტრალიზებული არქიტექტურიდან გამომდინარე, ზემოთ მითითებული მონაცემების შემცველი ბაზები ცენტრალური ოფისის გარდა განთავსებულია ყველა ტერიტორიულ ერთეულში, საბოლოო მომხმარებლის სამუშაო სადგურებში (მომხმარებლები, რომლებიც ჩართულნი არიან პენსიის ადმინისტრირების პროცესში). შესაბამისად, აღნიშნული სენსიტიური მონაცემების შემცველი ბაზების უსაფრთხოებისთვის კრიტიკულად მნიშვნელოვანია, რომ საბოლოო მომხმარებელთა სამუშაო სადგურები იყოს დაცული. ამასთანავე, აუცილებელია, რომ ყველა სამუშაო სადგური უზრუნველყოფდეს არსებული მონაცემების არასანქცირებული მოპოვებისა და მოდიფიკაციის პრევენციას. არსებული მოწყობიდან გამომდინარე, სისტემა იმდენად დაცულია, რამდენადაც მისი ყველაზე სუსტი რგოლი.

ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები და საერთაშორისო საუკეთესო პრაქტიკა ითვალისწინებს მრავალ უსაფრთხოების კონტროლს სამუშაო სადგურების დაცვისათვის. **თუმცა, სააგენტოს მატერიალურ-ტექნიკური ბაზისა და ზოგადი კონტექსტის გათვალისწინებით, აუდიტის ჯგუფმა შეფასების კრიტერიუმად განსაზღვრა შემდეგი მინიმალური მოთხოვნები, რომლებიც სააგენტოში უნდა იყოს უზრუნველყოფილი:**

- **სამუშაო სადგურების ცენტრალიზებული მართვა** – სააგენტოს უნდა გააჩნდეს, ცენტრალიზებული, აქტიური კონტროლის საშუალება ყველა სამუშაო სადგურზე. აღნიშნული შესაძლებელია განხორციელდეს Active Directory-ის საშუალებით. სააგენტოს უნდა შეეძლოს დაანესოს ცენტრალიზებული წესები ყველა მომხმარებლისთვის. მაგალითად, პაროლის სირთულე, ახალი პროგრამის ინსტალაციის და წაშლის უფლება და სხვ. ასევე აუცილებელია მუდმივად ხდებოდეს ოპერაციული სისტემის განახლება და უსაფრთხოების განახლებების დაყენება (security patches);
- **მავნე კოდისგან დაცვა** – სააგენტოს სამუშაო სადგურებზე უნდა არსებობდეს მავნე კოდისგან დაცვის ადეკვატური პროგრამული უზრუნველყოფა (მაგალითად, ანტივირუსი), რომელიც მუდმივად განახლებულია და რომლის გამოყენებითაც პერიოდულად ხდება სისტემის



სკანირება მავნე კოდის (მაგალითად, ვირუსი, ე.წ. „ტროას ცხენი“, ჭია, ჯაშუშური პროგრამა და სხვ.) აღმოსაჩენად;

- **შეზღუდული წვდომა ვებრესურსებზე** – სააგენტომ უნდა უზრუნველყოს საბოლოო მომხმარებლების წვდომა ვებრესურსებზე, რაც გულისხმობს არასასურველი და ცუდი რეპუტაციის (საიტები, რომელიც პოტენციურად შეიცავს მავნე კონტენტს) მქონე ვებგვერდების დაბლოკვას. ასევე მნიშვნელოვანია, გაკონტროლდეს ან სრულად დაიბლოკოს მონაცემების გაცვლის საშუალებები (ფაილების გაცვლის სერვისები), არასასურველი რეპუტაციის მქონე მეილსერვისები და საძიებო სისტემები.

ყოველივე ზემოთქმულის გათვალისწინებით, დაიგეგმა აუდიტორული პროცედურები და შეფასდა საბოლოო მომხმარებლების კომპიუტერების დაცულობა. პროცედურების ჩასატარებლად პირველ ეტაპზე (2017 წელს) შეფასდა – 6, ხოლო მეორე ეტაპზე (2019 წელს) – 3 რაიონული ოფისი. შემოწმდა სამუშაო სადგურებზე არსებული ოპერაციული სისტემა და სისტემური განახლებები, ანტივირუსი და მისი გამოყენების პრაქტიკა, ასევე ვებრესურსების ფილტრაცია. გარდა ზემოაღნიშნულისა, შეფასდა, იყვნენ თუ არა სამუშაო სადგურები დომენის²⁸ წევრები. აუდიტორული პროცედურების შედეგად გამოვლენილი გარემოებები წარმოდგენილია ქვემოთ მოცემულ ცხრილში.

ცხრილი N4. სააგენტოს ტერიტორიულ ერთეულებში განხორციელებული პროცედურების შედეგად გამოვლენილი ნაკლოვანებები

კონტროლი	2017	2019	შეფასება
ცენტრალიზებული მართვა	X	✓	2017 წელს რაიონული ოფისის წარმომადგენლების მართვა არ ხორციელდებოდა ცენტრალიზებული ფორმით. შესაბამისად, არ კონტროლდებოდა შერჩეული კრიტერიუმის არცერთი კომპონენტი. 2018 წელს, სამინისტრომ და სააგენტომ დაიწყეს რაიონულ ოფისებში არსებული მომხმარებლების ეტაპობრივი გადაყვანა ცენტრალურ დომენში. შესაბამისად, დომენში არსებული მომხმარებლების ცენტრალიზებულად გაკონტროლება ტექნიკურად შესაძლებელი გახდა. თუმცა, გადამოწმების შედეგად დადგინდა, რომ: • შერჩეული სამუშაო სადგურებიდან ყველა მომხმარებელს ჰქონდა ლოკალური ადმინისტრატორის უფლება.²⁹ • კომპიუტერებზე შექმნილი იყო ლოკალური მომხმარებლები (accounts), რომლებიც აქტიურია. ნებისმიერი, ვისთვისაც ცნობილია ამ მომხმარებლების პაროლი, შეუძლია შევიდეს სისტემაში და ამ მომხმარებლისთვის მინიჭებული უფლებებით განახორციელოს ქმედებები. • არ ხორციელდება სისტემების მუდმივი განახლება. აუდიტის მიმდინარეობისას, დომენში ჩართული იყო არსებული 1500 საბოლოო მომხმარებელიდან, დაახლოებით, 400 მათგანი. შესაბამისად, მომხმარებლების დიდ ნაწილზე საერთოდ არ ვრცელდება დომენის პოლიტიკები (მაგალითად, პაროლების პოლიტიკა) და არ ხორციელდება მათი ცენტრალიზებული მართვა.

28 Microsoft-ის ოპერაციული სისტემის მომხმარებლების ცენტრალიზებული მართვის სისტემა.

29 აღნიშნული როლი, საშუალებას იძლევა მომხმარებლის ოპერაციულ სისტემაზე, როგორც პროგრამული უზრუნველყოფების დაყენება/წაშლის/რედაქტირების, ასევე ოპერაციულ სისტემაში, კონფიგურაციის ცვლილებების ასახვის შესაძლებლობას.



მავნე კოდის- გან დაცვა	X	✓	2017 წელს რაიონული ოფისის საბოლოო მომხმარებლების სამუშაო სადგურებზე არ გამოიყენებოდა მავნე კოდისგან დაცვის საშუალებები. 2019 წელს, შერჩეულ სამუშაო სადგურებზე გამოიყენებოდა ანტივირუსის პროგრამული უზრუნველყოფა. ანტივირუსის კლიენტების პარამეტრების შემოწმებისას დადგინდა, რომ • კომპიუტერებზე სისტემის სრული სკანირება ან საერთოდ არ იყო ჩატარებული, ან განხორციელებული იყო რამდენიმე თვით ადრე. • ზოგიერთ შემთხვევაში არ იყო განახლებული ანტივირუსის პროგრამული უზრუნველყოფა.
ვებრესურსების კონტროლი	✓	✓	2017 და 2019 წელსაც, სააგენტო იყენებდა ვებრესურსების კონტროლის საშუალებას (Proxy Server).³⁰ აღნიშნული სერვისის გამოყენების მიუხედავად, რაიონული ოფისის საბოლოო მომხმარებლებს წვდომა აქვთ შემდეგი კატეგორიების ვებგვერდებზე: • აზარტული საიტები (leader-bet.com; crystalbet.ge); • სოციალური ქსელები (facebook.com, twitter.com); • საფოსტო ყუთები (mail.ru, yandex.ru); • ფაილების მიმოცვლის სერვისები (dropbox.com, wetransfer.com, google.drive.com).

არ არის დანერგილი
დანერგილია, ნაწილობრივ
დანერგილია, სრულად

აუდიტორული პროცედურები ცხადყოფს, რომ საბოლოო მომხმარებელთა უსაფრთხოების მართულებით სააგენტომ ნაწილობრივ გააუმჯობესა მდგომარეობა. დაწყებულია საბოლოო მომხმარებლების დომენში განვევრიანების პროცესი (1500 სამუშაო სადგურიდან³¹ დაახლოებით, 400-მდე უკვე განვევრიანებულია) და საბოლოო მომხმარებლებში ინერგება მავნე კოდისგან დაცვის საშუალებები. თუმცა, მიუხედავად ცვლილებებისა, საბოლოო მომხმარებლების დაცვის კონტროლები არაეფექტიანია, კერძოდ:

- არ არის ცნობილი სამუშაო სადგურების ზუსტი რაოდენობა, რომელიც უნდა ჩაერთოს დომენში;
- არასათანადოდ დაკონფიგურებული ოპერაციული სისტემა მომხმარებელს საშუალებას აძლევს დააყენოს ახალი პროგრამული უზრუნველყოფა, რომელიც შესაძლოა საფრთხეს შეიცავდეს;
- არასათანადო პაროლების პოლიტიკიდან გამომდინარე (მომხმარებლების დიდ ნაწილზე საერთოდ არ ვრცელდება პოლიტიკა), შესაძლებელია საბოლოო მომხმარებლების პაროლების მოპოვება და სისტემაში შეღწევა;
- არასათანადოდ დაკონფიგურებული პროქსი სერვერის გამო, სააგენტოს თანამშრომლების (სისტემის საბოლოო მომხმარებლების) დაცვა არ ხორციელდება ინტერნეტსაფრთხეებისგან. შესაბამისად, საჭიროების შემთხვევაში, სააგენტო ვერ შეძლებს უზრუნველყოს სისტემაში არსებული სენსიტიური მონაცემების არასანქცირებული გავრცელების პრევენცია;
- შერჩეული ანტივირუსის პროგრამული უზრუნველყოფა ზოგიერთ შემთხვევაში არ არის განახლებული, რის გამოც მისი შედეგიანობა შედარებით დაბალია.

30 შუალედური სერვერი, რომელიც უზრუნველყოფს მომხმარებლების დაშვებას წინასწარ განსაზღვრულ ვებრესურსებზე.

31 აღნიშნული წარმოადგენს მიახლოებით მაჩვენებელს.



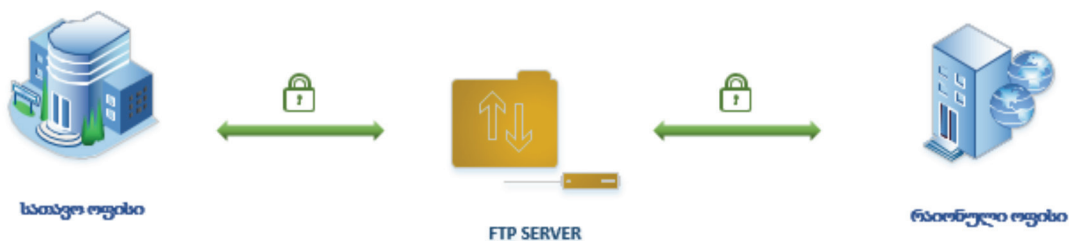
მონაცემებზე დაშვების კონტროლი

მონაცემებზე დაშვების კონტროლი ხორციელდება წვდომის კონტროლების საშუალებით. ინფორმაციის სენსიტიურობისა და მომხმარებლის (თანამშრომლის) სამსახურებრივი მოვალეობის გათვალისწინებით, სააგენტომ უნდა განსაზღვროს ინფორმაციაზე დაშვების წესები. ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესაბამისად, დაშვების განსაზღვრისას გათვალისწინებული უნდა იქნეს მინიმალური პრივილეგიებისა³² და ცოდნის საჭიროების³³ პრინციპები. აღნიშნული პრინციპები უზრუნველყოფს, რომ მომხმარებელს დაშვება ჰქონდეს მხოლოდ იმ ინფორმაციაზე, რომელიც აუცილებელი და საკმარისია სამსახურებრივი მოვალეობის შესასრულებლად.

აუდიტისას შესწავლილ იქნა სააგენტოს რაიონულ ოფისებში თანამშრომლებისთვის ხელმისაწვდომი ინფორმაცია და შეფასდა დაშვების კონტროლები. არსებული მოწყობით, რაიონული ოფისის წარმომადგენლებს დაშვება აქვთ სახელმწიფო პენსიის ადმინისტრირების სისტემაზე („პენსია 2005“) და ფაილების გაცვლის სერვერზე (FTP Server) არსებულ მონაცემებზე. აუდიტისას გაანალიზდა პენსიის ადმინისტრირების სისტემაზე წვდომის პრაქტიკა და მონაცემებზე დაშვების საჭიროება.

როგორც აუდიტორული პროცედურებით დადგინდა, სისტემა „პენსია 2005“ არ საჭიროებს მომხმარებლის სახელის შეყვანას და სისტემაში შესვლა ხდება მხოლოდ პაროლით, კერძოდ, სისტემის ადმინისტრატორი განსაზღვრავს სისტემის პაროლებს თითოეული რაიონული ოფისისათვის, რომელსაც იყენებს ამ ოფისის ყველა მომხმარებელი. მაგალითად, ერთსა და იმავე პაროლს შესაძლოა იყენებდეს რაიონული ოფისის რამდენიმე თანამშრომელი.

სქემა N8. მონაცემთა გაცვლა სათავო ოფისსა და რაიონულ ოფისს შორის



ფაილების გაცვლის სერვერის შესწავლისას გამოვლინდა, რომ რაიონული ოფისის წარმომადგენლები მათ მიერ დამუშავებულ მონაცემთა ბაზებს (მაგალითად, მიმდინარე თვის უფლებამოსილი ბენეფიციარების რეესტრი) ათავსებენ ამ სერვერზე. ასევე სათავო ოფისი იყენებს FTP სერვერს რაიონული ოფისებისთვის მონაცემთა ბაზების მისაწოდებლად. პენსიის ადმინისტრირების სისტემის მსგავსად, ფაილურ სერვერზე წვდომისათვის რაიონულ ოფისებს მინიჭებული აქვთ მომხმარებლის ანგარიში და პაროლი, რომელიც საერთოა ოფისის ყველა მომხმარებლისთვის. ასევე: აუდიტორული პროცედურებით გამოვლინდა, რომ სააგენტო უზრუნველყოფს ზემოაღნიშნულ სერვერზე განთავსებულ ინფორმაციაზე წვდომის ლოგირებას, თუმცა არ ახორციელებს ამ ჩანაწერების ანალიზს, რაც საშუალებას მისცემდა სააგენტოს, საჭიროების შემთხვევაში მიეკვლია განხორციელებული ოპერაციებისთვის.

32 Least Privilege Approach

33 Need-to-know

მეორე მხრივ, აუდიტისას შესწავლილ იქნა, თუ რა ინფორმაციაზე აქვთ დაშვება რაიონული ოფისის წარმომადგენლებს და რამდენად საჭიროა ეს მათი სამსახურებრივი მიზნებისთვის. წინამდებარე ცხრილში წარმოდგენილია აღნიშნული შესწავლის შედეგები.

ცხრილი N5. ტერიტორიული ერთეულების მიერ ვალიდაციის პროცესში გამოყენებული მონაცემთა ბაზები

მონაცემები	არსებული პრაქტიკა	უკეთესი პრაქტიკა (Need-to-know)
სერვისების განვითარების სააგენტოდან მიღებული მონაცემები	ყველა რაიონულ ოფისს წვდომა აქვს საქართველოს ყველა მოქალაქის პირადი მონაცემების შემცველ ერთიან და მუდმივად განახლებად ბაზასთან.	რაიონულ ოფისს წვდომა აქვს მხოლოდ იმ პირთა მონაცემებზე, რომლებიც ამ ტერიტორიული ერთეულის ბენეფიციარები არიან.
„რესპუბლიკის ბაზა“ – სახელმწიფო გასაცემლის მიმღები, ყველა მოქალაქის შესახებ მონაცემები	ყველა რაიონულ ოფისს აქვს წვდომა სახელმწიფო გასაცემლების მიმღებ პირთა ერთიან და მუდმივად განახლებად ბაზასთან.	ერთიანი ბაზის ყოველთვიურად გადაგზავნის აუცილებლობა არ არსებობს, ვინაიდან, იმავე ინფორმაციის მიღება (პირის გადამოწმება გასაცემლების რეესტრში) რაიონულ ოფისებს შეუძლიათ ვებსერვისის საშუალებით, რომელიც არ მოითხოვს მთლიანი ბაზის ლოკალურად არსებობას.
შემოსავლების სამსახურიდან მიღებული მონაცემები	ყველა რაიონულ ოფისს აქვს წვდომა მთელი ქვეყნის მასშტაბით საჯარო სამსახურში დასაქმებული პენსიონერების შესახებ ინფორმაციაზე.	რაიონულ ოფისებს წვდომა აქვთ მხოლოდ იმ პირთა მონაცემებზე, რომლებიც ამ ტერიტორიული ერთეულის ბენეფიციარები არიან.
სპეციალური პენიტენციური სამსახურიდან მიღებული მონაცემები	ყველა რაიონულ ოფისს აქვს წვდომა მთელი ქვეყნის მასშტაბით პენსიის მიმღები პირების პატიმრობის ან წინასწარი პატიმრობის შესახებ ინფორმაციაზე.	რაიონულ ოფისს წვდომა აქვს მხოლოდ იმ პირთა მონაცემებზე, რომლებიც ამ ტერიტორიული ერთეულის ბენეფიციარები არიან.
ბანკიდან მიღებული მონაცემები	ყველა რაიონულ ოფისს აქვს წვდომა მთელი ქვეყნის მასშტაბით პენსიის მიმღები იმ პირების შესახებ, რომელთა საბანკო ანგარიშზე ბოლო ექვსი თვის განმავლობაში არ განხორციელებულა ტრანზაქცია.	რაიონულ ოფისებს წვდომა აქვთ მონაცემებზე მხოლოდ იმ პირთა შესახებ, რომლებიც ამ ტერიტორიული ერთეულის ბენეფიციარები არიან.

მოცემულ ცხრილში წარმოდგენილი ინფორმაცია ცხადყოფს, რომ სააგენტო არ იყენებს ცოდნის საჭიროებაზე დაფუძნებულ მიდგომას და შედეგად, გარკვეულ შემთხვევებში, რაიონულ ოფისებს წვდომა აქვთ მთლიანი ქვეყნის მოქალაქეების შესახებ მონაცემებზე, რაც არაა საჭირო მათი სამსახურებრივი მოვალეობის შესასრულებლად. უკეთესი პრაქტიკის განხილვა ცხადყოფს, რომ პენსიის მართვის პროცესში გამოყენებული მონაცემების სენსიტიურობის გათვალისწინებით, სააგენტომ მაქსიმალურად უნდა შეზღუდოს არასაჭირო ინფორმაციაზე დაშვება ყველა რაიონული ოფისის მასშტაბით.

ასევე: სათანადო ხარისხით არ არის დაცული პერსონალური და განსაკუთრებული კატეგორიის მონაცემების შემცველი ბაზები მათი უნებართვო მოპოვებისა და გავრცელებისგან. არსებული არქიტექტურისა და მოწყობის გათვალისწინებით, რაიონულ ოფისებს წვდომა აქვთ უშუალოდ მონაცემთა ბაზების ფაილებზე (არა კონკრეტულად მონაცემზე, არამედ მონაცემთა ბაზაზე). როგორც უკვე აღინიშნა, სააგენტო ვერ უზრუნველყოფს FTP სერვერზე განთავსებულ

მონაცემთა ბაზებზე წვდომების ადეკვატურ³⁴ ლოგირებასა და მიკვლევადობას, რასაც ასევე ემატება დაუცველი სამუშაო სადგურები. შესაბამისად, ინფორმაციული უსაფრთხოების კონტროლების სისტემის გათვალისწინებით, სააგენტომ შესაძლოა ვერ უზრუნველყოს რაიონულ ოფისებში არსებული მონაცემთა ბაზების არასანქცირებული გავრცელების პრევენცია.

დასკვნა

ინფორმაციული უსაფრთხოების დანერგვისათვის უპირველესი ვალდებულებაა ორგანიზაციის ხელმძღვანელობის მიერ უსაფრთხოების მნიშვნელობის გაცნობიერება. ვალდებულებების შესრულება ხორციელდება არამარტო საკანონმდებლო მოთხოვნებთან შესაბამისობის უზრუნველსაყოფად, არამედ უპირველეს ყოვლისა, ორგანიზაციის მფლობელობაში არსებული ინფორმაციის დასაცავად. შემდგომ ეტაპზე კი, კანონით გათვალისწინებული სხვა მოთხოვნები მენეჯმენტის მხარდაჭერით უნდა შესრულდეს.

საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“ ძალაში 2013 წელს შევიდა, რაც სააგენტოს ავალდებულებს, დანერგოს ინფორმაციული უსაფრთხოების მართვის სისტემა, თუმცა აუდიტის მიმდინარეობისას, სააგენტოს არ ჰქონდა შესრულებული შესაბამისი კანონით გათვალისწინებული არცერთი მოთხოვნა.

აღნიშნულის გათვალისწინებით, აუდიტის პროცესში შეფასდა სააგენტოს მიერ პრაქტიკაში დანერგილი ინფორმაციული უსაფრთხოების კონტროლები. აუდიტის ჯგუფმა შეაფასა მინიმალური მოთხოვნები, რომლებიც აუცილებლად უნდა დააკმაყოფილოს სააგენტომ პენსიის ადმინისტრირების სისტემის უსაფრთხო ფუნქციონირებისათვის. შესწავლის შედეგად გამოვლინდა, რომ პენსიის ადმინისტრირების სისტემა („პენსია 2005“) დგას უწყვეტი ფუნქციონირების რისკის წინაშე, რომლის რეალიზების შემთხვევაში, სააგენტოს დასჭირდება არაპროპორციულად დიდი ძალისხმევა სისტემის ფუნქციონირების აღდგენისათვის. ასევე არსებობს რისკი, რომ სააგენტო საერთოდ ვერ შეძლებს სისტემის ფუნქციონირების აღდგენას.

მეორე მხრივ, პენსიის ადმინისტრირების სისტემის არქიტექტურისა და ტექნიკური მოწყობის გათვალისწინებით, მნიშვნელოვნად რთულდება მონაცემების უსაფრთხო დამუშავება. აღნიშნული მოიცავს ინფორმაციის დაცვას მისი გადაცემის, მისი შენახვისა და მისი დამუშავების ეტაპებზე. გარე წყაროებიდან ინფორმაციის მიღება ხდება არაერთგვაროვანი მიდგომით: სახელმწიფო სერვისების სააგენტოსთან და შემოსავლების სამსახურთან გამოიყენება დაცული საკომუნიკაციო არხი, ხოლო „ლიბერთი ბანკთან“ და სპეციალურ პენიტენციურ სამსახურთან მონაცემების გაცვლა ხდება დაუცველი საკომუნიკაციო არხების გამოყენებით.

სახელმწიფო პენსიის ადმინისტრირების ბიზნესპროცესის გათვალისწინებით, სააგენტოსთვის გამოწვევაა ქვეყნის მასშტაბით არსებულ 69 რაიონულ ოფისში არსებული სამუშაო სადგურ-

34 როგორც უკვე აღინიშნა, სისტემის რამდენიმე მომხმარებელი იყენებს სისტემის ერთსა და იმავე ანგარიშს და შესაბამისად, ლოგირების ჩანაწერები არ არის პერსონიფიცირებული (დაკავშირებული კონკრეტულ თანამშრომელთან). შესაბამისად, საჭიროების შემთხვევაში ვერ მოხდება გაიმიჯნოს, რომელმა თანამშრომელმა რა ოპერაცია განახორციელა.



ბის უსაფრთხოების დაცვა. ინფორმაცია, რომელიც ინახება და მუშავდება ამ სამუშაო სადგურებში (კომპიუტერებში) დაუცველია პოტენციური საფრთხეების მიმართ. კერძოდ, სააგენტოს არ აქვს დანერგილი შესაბამისი ქმედითი კონტროლის მექანიზმები, რომლებიც უზრუნველყოფდა სამუშაო სადგურების დაცვას მავნე კოდისგან, ინტერნეტსაფრთხეებისგან, მომხმარებლებისთვის მინიჭებული ტექნიკური პრივილეგიების ბოროტად გამოყენებისგან და სხვა გარე წყაროებიდან მომავალი საფრთხეებისგან.

ინფორმაციული უსაფრთხოების კონტროლებთან ერთად, მნიშვნელოვანი ყურადღება უნდა გამახვილდეს პერსონალური მონაცემების დამუშავების პრინციპებზეც. სააგენტო ყოველდღიურ საქმიანობაში ამუშავებს მოქალაქეთა პერსონალურ და განსაკუთრებული კატეგორიის მონაცემებს, რის გამოც ვალდებულია უზრუნველყოს ამ მონაცემების დამუშავება კანონმდებლობით დადგენილი პრინციპების შესაბამისად. თუმცა, სააგენტოს თანამშრომლებს დაშვება აქვთ საჭიროზე მეტი ადამიანის მონაცემებზე და ასევე ამ ინფორმაციის საჭიროზე მეტ ატრიბუტზე. აღნიშნულის პირობებში, სააგენტოს არ აქვს დანერგილი კონტროლები, რომლებიც უზრუნველყოფდა მონაცემებზე წვდომის ლოგირებასა და მიკვლევადობას. ასევე: სააგენტოს არ აქვს დანერგილი კონტროლები ინფორმაციის არასანქცირებული გავრცელების პრევენციისა და აღმოჩენისათვის.

ჩაკომპლექსია

სახელმწიფო პენსიის ადმინისტრაციის პროექტისა და დაკავშირებული სისტემის უწყვეტად ფუნქციონირებას მნიშვნელოვან გათვალისწინებით, სააგენტომ:

- შეაფასოს სისტემის უწყვეტ ფუნქციონირებასთან დაკავშირებული რისკები და შეიმუშაოს ამ რისკების მოპყრობის გეგმა;
- შეიმუშაოს ბიზნესუწყვეტობისა (BCP) და კატასტროფიდან აღდგენის გეგმები (DRP). უზრუნველყოს ამ გეგმების პერიოდული ტესტირება და განახლება.

საკანონმდებლო მოთხოვნების შესაბამისად, სააგენტომ უზრუნველყოს გარე წყაროებიდან მიღებული ინფორმაციის უსაფრთხოება, რაც გულისხმობს სპეციალური პენიტენციური სამსახურიდან მოწოდებული ინფორმაციის მიღებას დაცული საკომუნიკაციო არხის გამოყენებით.

სააგენტომ უზრუნველყოს საბოლოო მომხმარებელთა სამუშაო სადგურების მინიმალური უსაფრთხოება, რაც მოიცავს შემდეგ აქტივობებს:

- მაქსიმალურად სწრაფად უზრუნველყოს რაიონული ოფისის ყველა სამუშაო სადგურის ჩართვა დომენში;
- მაქსიმალურად სწრაფად შეიმუშაოს და გაავრცელოს დომენში ჩართული სამუშაო სადგურების მომხმარებლების ჯგუფური პოლიტიკები, რომლებიც, მინიმუმ, უნდა მოიცავდეს პაროლების პოლიტიკას, ანგარიშების პოლიტიკას, როლებისა და დაკავშირებული პრივილეგიების განსაზღვრას;
- დანერგოს მავნე კოდისგან დაცვის ქმედითი მექანიზმი (მაგალითად, მუდმივად განახლებადი ანტივირუსი) და უზრუნველყოს სისტემების პერიოდული სკანირება;
- განიხილოს საბოლოო მომხმარებლების საჭიროებები და დანერგოს მოქმედი კონტროლები ვებრესურსებზე წვდომისათვის. უზრუნველყოს წვდომის შეზღუდვა მავნე და არასასარგებლო რესურსებზე, ასევე შეზღუდოს წვდომა ფაილების გაცვლის სერვისებზე.



სახელმწიფო პენსიის ადმინისტრაციის პროცესში პანსონალიზირებული მონაცემების დამუშავების პრინციპების დასაყრდენი, სააგენტო:

- განსაზღვროს ინფორმაციაზე დაშვების წესები, მინიმალური პრივილეგიებისა³⁵ და ცოდნის საჭიროებაზე³⁶ დაფუძნებული პრინციპის გათვალისწინებით;
- შეიმუშაოს წვდომის კონტროლები ფაილების გაცვლის (FTP) სერვერისათვის, რომელიც უზრუნველყოფს მომხმარებლების იდენტიფიკაციისა და ავთენტიფიკაციის სათანადო პრაქტიკის ჩამოყალიბებას, ასევე განახორციელოს სისტემაზე წვდომის ლოგების ანალიზი.

35 Least Privilege Approach

36 Need-to-know



ბიბლიოგრაფია

ნორმატიული მასალა

საქართველოს კანონი „სახელმწიფო პენსიის შესახებ“, 2005 წელი;

საქართველოს კანონი „სოციალური დახმარების შესახებ“, 2006 წელი;

საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“, 2012 წელი;

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 2011 წელი;

მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის N2 ბრძანება „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“, 2013 წელი.

საერთაშორისო სტანდარტები და პუბლიკაციები

ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ შემუშავებული ჩარჩო დოკუმენტი (framework) COBIT 5;

ISO/IEC 27001:2013 ინფორმაციული უსაფრთხოების მართვის სისტემა – მოთხოვნები;

ინფორმაციული ტექნოლოგიების აუდიტის სახელმძღვანელო უმაღლესი აუდიტორული ორგანიზაციებისთვის.

აუდიტორთა ხელმოწერა:
სახელი, გვარი

ხელმოწერა

დავით შავგულიძე
ინფორმაციული ტექნოლოგიების
სამსახურის უფროსი

თამარ ივანიძე
ინფორმაციული ტექნოლოგიების
აუდიტორი



