ეფექტიანობის აუდიტის ანგარიში

სახელმწიფო აუდიტის სამსახური

სახელმწიფო აუდიტის სამსახური

„ვამტკიცებ“

ეფექტიანობის აუდიტის დეპარტამენტის უფროსი

გიორგი კაპანაძე

13 მარტი 2023 წელი

№ 7/36

ეგზ. №1

საჯარო სექტორში დისტანციური მუშაობისათვის
ეფექტიანი და უსაფრთხო გარემოს უზრუნველყოფა

სარჩევი

ტერმინთა განმარტებები

ბიზნესის უწყვეტობის დაგეგმვა / კატასტროფიდან აღდგენის დაგეგმვა (BCP/ DRP)	ბიზნესის უწყვეტობის დაგეგმვა – პროცესი, რომლის ფარგლებშიც ორგანიზაცია გეგმავს და ამოწმებს ბიზნესპროცესის შეფერხებისას აღდგენით აქტივობებს. აღნიშნული მოიცავს არასასურველი პირობების (კატასტროფის) შემთხვევაში ორგანიზაციის მიერ გადასადგმელ ნაბიჯებს ფუნქციონირების გასაგრძელებლად. DRP-ის ფარგლებში განისაზღვრება ინციდენტის შემდეგ IT ინფრასტრუქტურის აღდგენის სამუშაოები. აღნიშნული ბიზნესის უწყვეტობის დაგეგმვის ნაწილია და კონცენტრირებულია IT ინფრასტრუქტურაზე.
დიჯიტალიზაცია	ინფორმაციისა და სერვისების გაციფრულება ბიზნესპროცესების გაუმჯობესების მიზნით.
დისტანციური მუშაობის პრაქტიკა	თანამშრომელთა ქცევის შეთანხმებული ნორმები, პოლიტიკა და თანმდევი უსაფრთხოების ზომები, რომლებიც უნდა იქნეს უზრუნველყოფილი ორგანიზაციის ოფისს გარეთ მუშაობის პირობებში.
ვირტუალური კერძო ქსელი (VPN)	ინტერნეტით კერძო ქსელის შესაქმნელად გამოყენებული ტექნოლოგია, რომელიც უზრუნველყოფს დაშიფრული, უსაფრთხო გზით შიდა ინტრანეტის რესურსების გაზიარებას დისტანციურ მომხმარებლებთან და ორგანიზაციის სხვა ოფისებთან.
ინფორმაციული უსაფრთხოება	ინფორმაციის კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის უზრუნველყოფა.
ინფორმაციული უსაფრთხოების ინციდენტი	არასასურველი ან მოულოდნელი ინფორმაციული უსაფრთხოების შემთხვევა ან შემთხვევების სერია, რომელსაც აქვს ბიზნესოპერაციების კომპრომეტირების და ინფორმაციული უსაფრთხოებისთვის საფრთხის შექმნის მნიშვნელოვანი შესაძლებლობა.

ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები	კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ შესასრულებელი მინიმალური აქტივობები ინფორმაციული უსაფრთხოების მართვის სისტემის შესაქმნელად.
საბოლოო მომხმარებელი	პირი/თანამშრომელი, რომელიც თავის საქმიანობაში იყენებს ინფორმაციულ სისტემას.
RACI	პასუხისმგებლობების განაწილების მატრიცა/მოდელი. მატრიცის შემადგენელი კომპონენტებია: პასუხისმგებელი (Responsible), ანგარიშვალდებული (Accountable), მრჩეველი (Consulted), ინფორმირებული (Informed) პირი/უწყება.
IT მმართველობა	სისტემა, რომლის მეშვეობითაც იმართება და კონტროლდება ორგანიზაციის ინფორმაციული ტექნოლოგიებისა და სისტემების გარემო. აღნიშნული უზრუნველყოფს IT ოპერაციების ორგანიზაციის მიზნების შესაბამისად მართვას.

შემაჯამებელი მიმოხილვა და რეკომენდაციები

საჯარო სექტორის გაციფრულების პირობებში ორგანიზაციების ინფორმაციულ ტექნოლოგიებზე დამოკიდებულება სწრაფი ტემპით იზრდება. აღნიშნული განაპირობებს ორგანიზაციებში ქმედითი და ეფექტიანი IT მმართველობის არსებობის აუცილებლობას, რაც მიიღწევა მაღალი და საშუალო რგოლის მენეჯმენტის კოორდინირებული ქმედებებით. კერძოდ, სტრატეგიულ და საოპერაციო დონეებზე IT პროცესებთან მიმართებით მიღებული გადაწყვეტილებები ხელს უნდა უწყობდეს ორგანიზაციას ძირითადი მიზნის მიღწევასა (ბიზნესპროცესის ეფექტიანად წარმართვა) და ინფორმაციული უსაფრთხოების უზრუნველყოფაში. შესაბამისად, წინასწარგანსაზღვრული სტრატეგია, პოლიტიკა, პროცედურები და სამოქმედო გეგმების არსებობა, ქმედითი IT მმართველობის წინაპირობაა.

ეფექტიანი IT მმართველობის მნიშვნელობა განსაკუთრებით ცხადი გახდა COVID-19-ის პანდემიის დაწყების შემდგომ, როდესაც სოციალური დისტანცირების მოთხოვნის თანახმად, საჯარო ორგანიზაციები დისტანციურ სამუშაო რეჟიმზე გადავიდნენ. დისტანციური მუშაობის რეჟიმზე გადასვლა უწყებებისათვის ფორსმაჟორულ სიტუაციას ქმნიდა და ხელმძღვანელობის მხრიდან ეფექტიანი გადაწყვეტილებების მიღებასთან ერთად, აუცილებელი მატერიალურ – ტექნიკური რესურსის არსებობას მოითხოვდა. უკეთესი პრაქტიკის მიხედვით, ფორსმაჟორულ სიტუაციაში სამუშაოს შესრულების საერთო წესებისა და სტანდარტული პირობების არსებობა ორგანიზაციას ხელს უწყობს ოპტიმალური გადაწყვეტილებების მიღებაში.

სახელმწიფო აუდიტის სამსახურმა შეისწავლა დისტანციურ სამუშაო რეჟიმზე გადასვლის მიზნით მიღებული მმართველობითი გადაწყვეტილებები და მათი განხორციელების ეფექტიანობა პანდემიის პერიოდში. აუდიტი მოიცავს 2019-2021 წლებს.

აუდიტის ობიექტებია:

- საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;
- საქართველოს გარემოს დაცვისა და სოფლის მეურნეობის სამინისტრო;
- სსიპ – საჯარო რეესტრის ეროვნული სააგენტო.

ზოგადად, შესწავლილ უწყებებში IT მმართველობის არსებული პრაქტიკა საჭიროებს გაუმჯობესებას. ფორმალიზებული პროცედურების არარსებობისა და კომუნიკაციის ნაკლებობის პირობებში, ორგანიზაციები მოკლებულნი არიან ინფორმირებული და ეფექტიანი გადაწყვეტილებების მიღების შესაძლებლობას. აღნიშნული ნაკლოვანება, თავის მხრივ, აისახება ორგანიზაციაში რესურსების არასათანადო განაწილებასა და კონტროლის გარემოს სისუსტეებზე.

აუდიტის ძირითადი მიგნებებია:

- აუდიტის ობიექტებს არ შეუმუშავებიათ ბიზნესის უწყვეტობისა და კატასტროფიდან აღდგენის გეგმები, რომლებიც დაეხმარებოდა მათ პანდემიაზე დროულ რეაგირებაში. ამასთანავე, არ იყო შემუშავებული დისტანციური მუშაობის პოლიტიკა, ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესაბამისად. კერძოდ, დისტანციური მუშაობისათვის, უწყებებს უნდა შეემუშავებინათ პოლიტიკა, რომელიც განსაზღვრავდა დისტანციურ მუშაობასთან დაკავშირებულ პირობებსა და შეზღუდვებს. აღნიშნული პოლიტიკა აუდიტის ობიექტებს

ხელს შეუწყობდა დისტანციურ რეჟიმზე გადასვლისას აქტივების უკეთ გამოყენებასა და ინფორმაციული უსაფრთხოების პრინციპების დაცვაში. ამ მხრივ გამონაკლისი იყო საჯარო რეესტრის ეროვნული სააგენტო, რომელსაც შემუშავებული ჰქონდა დისტანციური წვდომის/მუშაობის პოლიტიკა, თუმცა დოკუმენტი არ იყო ფორმალიზებული/დამტკიცებული. აღნიშნულ საკითხთან მიმართებით, უწყებებმა სახელმძღვანელო მითითებები თანამშრომლებს სხვადასხვა ფორმით მიაწოდეს (ელექტრონული ფოსტა, ინტრანეტი);

- დისტანციურ სამუშაო რეჟიმზე გადასვლის პროცესში აუდიტის ობიექტების თანამშრომელთა დიდი ნაწილი ვერ იქნა უზრუნველყოფილი შესაბამისი კომპიუტერული ტექნიკით.[1] შედეგად, თანამშრომლებს დისტანციურად მუშაობისას მოუხდათ საკუთარი მოწყობილობების სამსახურებრივი მიზნებისათვის გამოყენება. ამასთანავე, ზოგიერთ შემთხვევაში[2] უწყებების მიერ კომპიუტერული ტექნიკის მიწოდების მიუხედავად, თანამშრომლების ნაწილი მაინც იყენებდა პირად მოწყობილობებს, სამსახურის მიერ მოწოდებული დაბალი წარმადობის ან/და მოძველებული მოწყობილობების გამო. აღნიშნული მიმართულებით საყურადღებოა შემდეგი გარემოებები:

    - შემოწმებული ორგანიზაციებიდან ეკონომიკისა და სოფლის მეურნეობის სამინისტროებს არ აქვთ აღრიცხული და კლასიფიცირებული ორგანიზაციის ფარგლებში არსებული ინფორმაციული აქტივები, ხოლო სსიპ – საჯარო რეესტრის ეროვნულ სააგენტოში მიმდინარეობს არსებულ ბიზნესპროცესებთან მიმართებით აქტივების გამოვლენა და შესაბამისი რეესტრის წარმოება.
    - თანამშრომლის მიერ პირადი კომპიუტერული მოწყობილობების გამოყენებისას არ განხორციელებულა ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესაბამისი აქტივობები.[3]

შესაბამისად, აუდიტის ობიექტები მოკლებულნი იყვნენ შესაძლებლობას, შეეფასებინათ მათ საკუთრებაში არსებული აქტივები კრიტიკულობის მიხედვით და მიეღოთ ოპტიმალური გადაწყვეტილებები ტექნიკის გადანაწილებაზე ან/და უსაფრთხოების შესაბამისი დონის განსაზღვრასთან მიმართებით.

- დისტანციურად მუშაობის პირობებში უწყებების თანამშრომლებს დასჭირდათ სამსახურისაგან დამოუკიდებელი/გარე ქსელების გამოყენება, რომლებიც არ კონტროლდება აუდიტის ობიექტების IT სამსახურების მიერ და შესაბამისად, ნაკლებად არის დაცული. აღნიშნული პრობლემის გადაჭრის ერთ-ერთ საუკეთესო პრაქტიკად მიჩნეულია ვირტუალური კერძო ქსელის (VPN) გამოყენება. სამივე ობიექტმა უზრუნველყო თანამშრომელთა კომპიუტერების დაშიფრულ (VPN) ქსელში ჩართვა, თუმცა თანამშრომლები შესაბამის აპლიკაციას ძირითადად ააქტიურებდნენ სამსახურში არსებულ პირად კომპიუტერსა ან სასერვერო ინფრასტრუქტურაზე განთავსებულ ინფორმაციაზე წვდომის საჭიროების შემთხვევაში. აღნიშნულის გათვალისწინებით, თანამშრომლებს დაუცველ გარე ქსელთან შეუზღუდავი წვდომა ჰქონდათ, რაც ინფორმაციული უსაფრთხოების თვალსაზრისით მნიშვნელოვანი რისკების შემცველია.

---

[1] აღნიშნული გამოწვეული იყო იმ გარემოებით, რომ სამივე უწყებაში, თანამშრომელთა დიდი უმრავლესობა იყენებდა სტატიკურ კომპიუტერს.

[2] დეტალები: იხ. 27 გვ.

[3] მაგალითად, მოწყობილობების პირადი და სამსახურებრივი მიზნებით გამოყენების გამიჯვნა, თანამშრომელთა მიერ შესასრულებელი მოვალეობების განსაზღვრა.

რეკომენდაციები:

აუდიტის ობიექტებმა IT მმართველობის სისტემური გაუმჯობესების მიზნით, COVID-19-ის პანდემიის პერიოდში შეძენილი გამოცდილების გათვალისწინებით, უზრუნველყონ შემდეგი:

- IT სერვისების უწყვეტობის პროცესის გაუმჯობესების მიზნით:
    - შეიქმნას მმართველობითი სისტემა სათანადო უფლებამოსილების, კვალიფიკაციისა და კომპეტენციის მქონე პერსონალით, რომელიც პასუხისმგებელი იქნება სერვისების უწყვეტობის მართვის პროცესში შესაბამისი აქტივობების დაგეგმვაზე, განხორციელებასა და რეაგირებაზე;
    - გადაიდგას საწყისი ნაბიჯები სერვისის უწყვეტობის გეგმების შესამუშავებლად, რომლებიც ხელს შეუწყობს ორგანიზაციაში კრიტიკული ბიზნესპროცესების განგრძობად მუშაობას;
    - განხორციელდეს რეგულარულად (სულ მცირე – ყოველწლიურად) შეუსაბამობების ანალიზი (gap analysis) IT სერვისების უწყვეტობასთან მიმართებით, რათა განისაზღვროს ორგანიზაციის მიმდინარე და სასურველი მდგომარეობა.

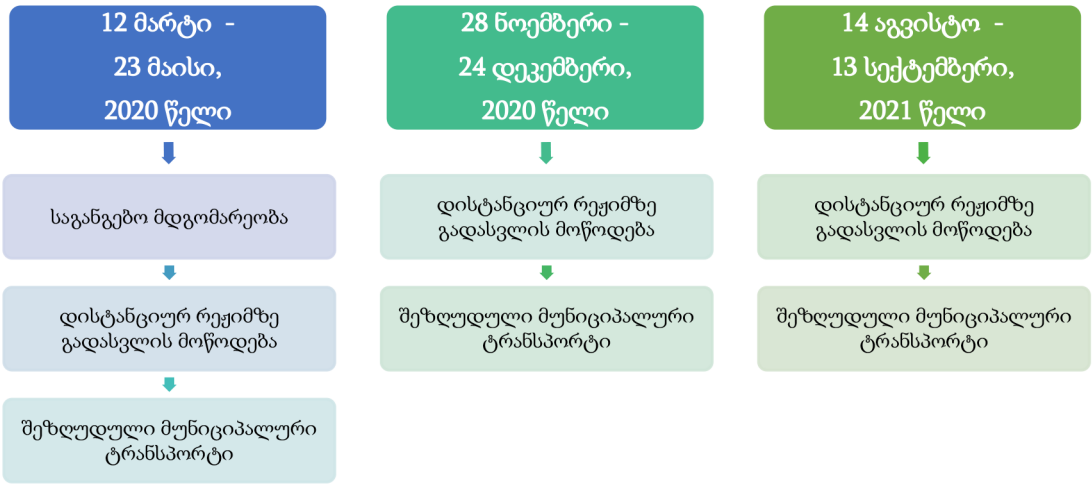
- ინფორმაციული უსაფრთხოების რისკების დასაზღვევად შემუშავდეს პოლიტიკა/პროცედურა, რომლის საშუალებითაც უზრუნველყოფილი იქნება ოპერაციული სისტემებისა და პროგრამული უზრუნველყოფების დროული ლიცენზირება/განახლება.

1. შესავალი

1.1 აუდიტის მოტივაცია

მსოფლიოში 2020 წელს დაწყებულმა COVID 19-ის პანდემიამ რადიკალური ცვლილებები გამოიწვია საჯარო და კერძო სექტორის მუშაობის პრაქტიკაში. საქართველოს სახელმწიფო უწყებებში დასაქმებული 290,700 საჯარო მოხელიდან,[4] თანამშრომლების უმეტესი ნაწილი გადაყვანილ იქნა დისტანციურ სამუშაო რეჟიმზე. პანდემიის პირობებში გადაადგილების შემზღუდველი სამთავრობო რეგულაციები წარმოდგენილია გრაფიკზე.

გრაფიკი №1. პანდემიის პირობებში სამთავრობო რეგულაციები, რომელთა ფარგლებშიც საჯარო უწყებების მიერ გამოყენებული იყო დისტანციური მუშაობის პრაქტიკა[5]



დისტანციური მუშაობის პრაქტიკის გამოყენება ორგანიზაციების მხრიდან მოითხოვდა მზაობას სხვადასხვა მიმართულებით – პანდემიის პირობებში უწყებები აღმოჩდნენ ისეთი პრობლემების წინაშე, როგორებიცაა:

- სერვისების უწყვეტობის უზრუნველყოფა;
- შესაბამისი პროცედურების არსებობა;
- ტექნიკური მხარდაჭერა;
- მოწყობილობების ხელმისაწვდომობა და უსაფრთხოების ზომები.

პანდემიის პირობებში რესურსების ხელმისაწვდომობა, როგორც ერთ-ერთი მნიშვნელოვანი შეზღუდვა, ხაზგასმულია გაერთიანებული ერების ორგანიზაციის განვითარების პროგრამისა და სსიპ – საჯარო სამსახურის ბიუროს მიერ ჩატარებულ კვლევაში,[6] რომლის მიხედვით,

[4] სსიპ – საქართველოს სტატისტიკის ეროვნული სამსახური, 2020 წლის მონაცემები.

[5] წყარო: საქართველოს მთავრობის ოფიციალური ვებგვერდი: www.gov.ge

[6] დისტანციურად მუშაობა: საჯარო სექტორში დასაქმებულთა განწყობების ანალიზი, UNDP, სსიპ – საჯარო სამსახურის ბიურო, 2020 წელი. კვლევის ფარგლებში შეფასდა საქართველოში საჯარო სექტორში დისტანციური სამუშაო პრაქტიკის გავლენა, უპირატესობები და ხარვეზები.

ერთ-ერთ მთავარ გამოწვევად სახლში მობილურ ტექნოლოგიებზე წვდომა და ტექნიკურ საკითხებთან დაკავშირებული პრობლემები დასახელდა. აღნიშნული გულისხმობს საოფისე პირობებთან შედარებით ფუნქციურად სუსტ და დაუცველ ინფორმაციულ მოწყობილობებსა და მაღალსიჩქარიან ინტერნეტთან ხელმისაწვდომობის ნაკლებობას, ასევე სათანადო სამუშაო სივრცის არარსებობასა და სხვა მსგავს პრობლემებს.

ასევე მნიშვნელოვანია ორგანიზაციების მიერ ინფორმაციული უსაფრთხოების უზრუნველსაყოფად გატარებული ღონისძიებები. დისტანციური მუშაობის პრაქტიკის გამართული ფუნქციონირება მსოფლიო მასშტაბის გამოწვევად ითვლება. არაერთი კვლევა აჩვენებს,[7] რომ პანდემიის პირობებში კიბერშეტევების რაოდენობა მსოფლიოში მნიშვნელოვნად გაიზარდა. აღნიშნული გარემოების ერთ-ერთი გამომწვევი მიზეზი დისტანციურად მუშაობის პრაქტიკის აქტიური გამოყენებაა, კერძოდ:

- გაიზარდა სხვადასხვა ვიდეო და სატელეკომუნიკაციო სისტემის გამოყენება;
- დაუცველი ქსელიდან სამსახურებრივ კონფიდენციალურ ან/და სენსიტიურ ინფორმაციაზე წვდომის აუცილებლობა;
- პირადი მოწყობილობებით სამსახურებრივი ინფორმაციის დამუშავება და სხვ.

შესაბამისად, საბოლოო მომხმარებელი უფრო მოწყვლადი გახდა კიბერინციდენტებისადმი. მსგავსი რისკების დასაზღვევად, უკეთესი პრაქტიკის[8] მიხედვით მნიშვნელოვანია გადაიხედოს არსებული უსაფრთხოების სისტემები და პროცესები, განხორციელდეს შესაბამისი ცვლილებები, უზრუნველყოფილ იქნეს აღნიშნული ცვლილებების კომუნიკაცია და შემდგომ მათი მონიტორინგი.

ჩამოთვლილი პრობლემები განსაკუთრებით აქტუალურია იმის გათვალისწინებით, რომ საჯარო სექტორში ინფორმაციული ტექნოლოგიების მართვის პროცესები გამოირჩევა სისტემური ნაკლოვანებებით, რომლებიც დასტურდება სახელმწიფო აუდიტის სამსახურის მიერ ჩატარებული რიგი აუდიტებით.[9] აღნიშნულ აუდიტის ანგარიშებში გამოიკვეთა IT მმართველობისა და ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვის პროცესებთან დაკავშირებული ნაკლოვანებები.

1.2 აუდიტის მიზანი და კითხვები

აუდიტის მიზანია აუდიტის ობიექტების მზაობის შეფასება თანამშრომლებისთვის სათანადო დისტანციური სამუშაო პირობების ორგანიზების მხრივ (საჯარო სერვისების უწყვეტობის უზრუნველსაყოფად).

აუდიტის ფარგლებში შესწავლილ იქნა არსებული რესურსების, პოლიტიკებისა და პროცედურების პირობებში, რამდენად იყო უზრუნველყოფილი სახელმწიფო ორგანიზაციების მიერ სამუშაო პროცესის სტაბილურ რეჟიმში გაგრძელება, ინფორმაციული უსაფრთხოების პრინციპების დაცვა და თანამშრომელთა უმრავლესობის დისტანციურ სამუშაო რეჟიმზე გადაყვანა.

---

[7] კიბერდანაშაულის ფარული ხარჯები (The Hidden Costs of Cybercrime), McAfee, 2020.

[8] COBIT 2019 სახელმძღვანელო დოკუმენტი.

[9] სახელმწიფო ვალის მართვის ინფორმაციული სისტემების შემდგომი რეაგირების ეფექტიანობის აუდიტი, სახელმწიფო პენსიის ადმინისტრირების ინფორმაციული სისტემების ეფექტიანობის აუდიტის ანგარიში, საჯარო სექტორში IT პროექტების მართვის ეფექტიანობის ანგარიში.

აღნიშნული მიზნის მისაღწევად აუდიტმა უპასუხა შემდეგ კითხვებს:

1. რამდენად არსებობდა ფორმალური პროცედურები (წინასწარგანსაზღვრული პრაქტიკა) პანდემიით გამოწვეული კრიზისის ეფექტიანი მართვისა და დისტანციური მუშაობის უზრუნველსაყოფად?
2. დისტანციურად მუშაობის პირობებში, რამდენად იყო უზრუნველყოფილი ორგანიზაციაში მხარდამჭერი სერვისების უწყვეტი მიწოდება თანამშრომლებისათვის და ინფორმაციული უსაფრთხოება?

1.3 შეფასების კრიტერიუმები

აუდიტის კრიტერიუმად გამოყენებულ იქნა საერთაშორისოდ აღიარებული ჩარჩო დოკუმენტი (framework) COBIT 2019, რომლის მიხედვით შეფასდა დისტანციურად მუშაობის პირობებში ბიზნესპროცესის ადმინისტრირებისა და უსაფრთხოების უზრუნველყოფის საკითხები და IT მმართველობის არსებული პრაქტიკა.

აუდიტის ფარგლებში COBIT სახელმძღვანელო დოკუმენტიდან გამოყენებულ იქნა ქვემოთ მოცემული პროცესები:

კრიტიკული აქტივების მართვა (BAI09.02) – ორგანიზაციას უნდა ჰქონდეს იდენტიფიცირებული და აღწერილი/კლასიფიცირებული თავის მფლობელობაში არსებული კრიტიკული აქტივები (რომლებიც შეიძლება იყოს ტექნიკური მოწყობილობა, პროგრამული უზრუნველყოფა, ინფორმაცია, მონაცემები, ადამიანები და სხვ.). კრიტიკული აქტივების ეფექტიანი მართვა დისტანციური მუშაობის თანდაყოლილ რისკებს მნიშვნელოვნად ამცირებს. კერძოდ, სახლიდან მუშაობის შემთხვევაში თანამშრომლებს ესაჭიროებათ სამსახურის აქტივებზე (მაგალითად, კომპიუტერულ მოწყობილობებზე, დასამუშავებელ კლასიფიცირებულ/სენსიტიურ/კრიტიკულ ინფორმაციაზე) დისტანციური გარემოდან წვდომა. შესაბამისად, აღნიშნული აქტივების კლასიფიცირება და კრიტიკულობის დადგენა მნიშვნელოვანია შესაფერისი კონტროლის მექანიზმების განსასაზღვრად.

გარდა ამისა, დისტანციური მუშაობის რეჟიმისთვის არსებითი მნიშვნელობის ფაქტორია ორგანიზაციის მიერ საკმარისი რაოდენობის ტექნიკური მოწყობილობების მობილიზება და სწორად გადანაწილება, რათა უზრუნველყოფილ იქნეს თანამშრომლების მიერ საკუთარი მოწყობილობების გამოყენების მინიმუმამდე შემცირება. ინფორმაციული აქტივების იდენტიფიცირება და კლასიფიკაცია აღნიშნული პროცესის მთავარ წინაპირობას წარმოადგენს.

ქსელის უსაფრთხოების მართვა (DSS05.02) – ქსელის უსაფრთხოების მიზანია:

- მხოლოდ ავტორიზებული მოწყობილობების წვდომის უზრუნველყოფა სამსახურებრივ ინფორმაციასა და ქსელზე;
- ქსელის ფილტრაციის უზრუნველყოფა შესაბამისი პროგრამული თუ აპარატურული უზრუნველყოფებით (მაგალითად, firewall-ები, შეღწევადობის აღმოჩენისა (IDS) და პრევენციის (IPS) სისტემები და სხვ.);
- ქსელში ინფორმაციის მიმოცვლისას მისი კლასიფიკატორის შესაბამისად დაშიფვრა.

ამასთანავე, მნიშვნელოვანია თანამშრომელთა მაღალი ცნობიერება უსაფრთხოების პრინციპების დაცვასთან მიმართებით.

საბოლოო მომხმარებლების უსაფრთხოება (DSS05.03) – საბოლოო მომხმარებლების უსაფრთხოება მოიცავს მოწყობილობების (როგორიცაა, სტატიკური კომპიუტერები, ლეპტოპები, მობილური მოწყობილობები) უზრუნველყოფას ანტივირუსული პროგრამებით, ასევე ელექტრონული კომუნიკაციის საშუალებების ფილტრაციას და მათ რეგულარულ მონიტორინგს. საბოლოო მომხმარებლის დაცვის მექანიზმია ასევე განახლებების და მომხმარებელთა ცენტრალიზებული მართვა.

გარდა აღნიშნულისა, სერვისების უწყვეტობისა და დისტანციურ რეჟიმზე გადასვლის პირობებში ინფორმაციული უსაფრთხოების მართვის პრაქტიკის შესაბამისობის დადგენის უზრუნველსაყოფად გამოყენებულ იქნა შემდეგი მარეგულირებელი დოკუმენტები:

- საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“;
- „პირველი და მეორე კატეგორიის ინფორმაციული სისტემის სუბიექტებისათვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“.[10]

1.4 აუდიტის მასშტაბი და მეთოდოლოგია

აუდიტის პერიოდი მოიცავს 2019-2021 წლებს. აუდიტის ობიექტებად განისაზღვრა შემდეგი საჯარო უწყებები:

- საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;
- საქართველოს გარემოს დაცვისა და სოფლის მეურნეობის სამინისტრო;
- სსიპ – საჯარო რეესტრის ეროვნული სააგენტო.

აუდიტის ფარგლებში შესწავლილ იქნა შერჩეული უწყებების სერვისების უწყვეტობის უზრუნველსაყოფად არსებული პოლიტიკა, პროცედურები და ღონისძიებები (პანდემიამდე მოქმედი), აგრეთვე აქტივობები, რომლებიც პანდემიის დაწყების შემდგომ გატარდა ორგანიზაციის ძირითადი ბიზნესპროცესის უწყვეტობისა და თანამშრომელთა დისტანციურად უსაფრთხოდ მუშაობის უზრუნველსაყოფად.

აუდიტის ძირითად კითხვებზე პასუხის გასაცემად შემუშავდა აუდიტორული პროცედურები, რომელთა მიხედვით შეფასდა აუდიტის ობიექტების მიერ დისტანციური სამუშაო რეჟიმის მართვის პრაქტიკა:

1. რამდენად არსებობდა ფორმალური პროცედურები (წინასწარგანსაზღვრული პრაქტიკა) პანდემიით გამოწვეული კრიზისის ეფექტიანი მართვისა და დისტანციური მუშაობის უზრუნველსაყოფად?

- მოცემული კითხვის ფარგლებში შეფასდა, რამდენად არსებობდა სერვისების უწყვეტობისა და კატასტროფიდან აღდგენის გეგმები (BCP/DRP) და აღნიშნული გეგმების პრაქტიკაში დანერგვის მდგომარეობა. აუდიტის პროცესში იქნა მოთხოვნილი და განხილული შესაბამისი დოკუმენტაცია. ფორმალური დოკუმენტაციის არსებობის შემთხვევაში ინტერვიუებისა და ადგილზე შესასრულებელი სამუშაოების მეშვეობით, შეფასდა პოლიტიკისა და პროცედურების რეალურ გარემოში დანერგვის მდგომარეობა;

[10] საქართველოს სახელმწიფო უსაფრთხოების სამსახურის, სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს უფროსის 2021 წლის 21 დეკემბრის №35 ბრძანება

- შესაბამისი ინფორმაციის მოთხოვნის გზით, შეფასდა დისტანციური მუშაობის პოლიტიკის არსებობა. პანდემიით გამოწვეული რისკების მინიმიზაციისა და ბიზნესპროცესების უწყვეტობის უზრუნველყოფის მიზნით, ასევე შესწავლილ იქნა ინფორმაციული უსაფრთხოების მიმართულებით თანამშრომელთა ცნობიერების ამაღლებისათვის გატარებული ღონისძიებები, მათთვის გაგზავნილი მითითებები, ჩატარებული ტრენინგები და სხვ. აღნიშნული მიმართულებით, ფორმალური პოლიტიკის არარსებობის პირობებში, შეფასდა ორგანიზაციის მიერ (უკეთესი პრაქტიკის მიხედვით) დისტანციური მუშაობისათვის საჭირო მოთხოვნების პრაქტიკაში შესრულების საკითხები;
- აუდიტის ჯგუფმა ინტერვიუებისა და მოთხოვნილი დოკუმენტაციის საფუძველზე შეისწავლა ზემოაღნიშნული ფორმალური პოლიტიკების შემუშავების მიმდინარე მდგომარეობა.

2. დისტანციურად მუშაობის პირობებში, რამდენად იქნა უზრუნველყოფილი ორგანიზაციაში მხარდამჭერი სერვისების უწყვეტი მიწოდება თანამშრომლებისათვის და ინფორმაციული უსაფრთხოება?

- თანამშრომელთა სათანადო რესურსებით უზრუნველყოფის შესაფასებლად, აუდიტის ჯგუფმა ორგანიზაციებიდან გამოითხოვა ინფორმაციული აქტივების რეესტრი. ამასთანავე, ინფორმაციის კლასიფიცირების დასადასტურებლად შეისწავლა კლასიფიკაციის არსებული პრაქტიკა და საკითხი კლასიფიკაციის ამსახველი დოკუმენტაციის არსებობის შესახებ;
  თანამშრომელთა მხარდამჭერი სერვისებით უზრუნველყოფის შესწავლისათვის აუდიტის ობიექტებში თანამშრომლებთან გაიგზავნა კმაყოფილების კითხვარი (სსიპ – საჯარო რეესტრის ეროვნული სააგენტო – 219 თანამშრომელი, ეკონომიკისა და მდგრადი განვითარების სამინისტრო – 76 თანამშრომელი, გარემოს დაცვისა და სოფლის მეურნეობის სამინისტრო – 138 თანამშრომელი). ამასთანავე, მხარდამჭერი სერვისების ადმინისტრირებისათვის გამოყენებული ინფორმაციული სისტემის მიერ გენერირებული ანგარიშების საფუძველზე მოხდა ტექნიკური ხარვეზების სიხშირის იდენტიფიცირება და მათი აღმოფხვრის დროულობის განსაზღვრა;
- საჯარო მოხელეების მიერ პირადი საკუთრების კომპიუტერული მოწყობილობის გამოყენების შემთხვევებში, შეფასდა ამ მოწყობილობებზე სამსახურის ინფორმაციული უსაფრთხოების პოლიტიკის/მოთხოვნების გავრცელების ხარისხი; ასევე: რამდენად უზრუნველყო ინფორმაციული ტექნოლოგიების დეპარტამენტმა თანამშრომლებისათვის მათი გამოყენების ინსტრუქციების მიწოდება. აღნიშნული ანალიზისათვის შედგა თითო შეხვედრა ინფორმაციული ტექნოლოგიების დეპარტამენტებთან და შესაბამისი საკითხები იქნა გათვალისწინებული თანამშრომელთა კმაყოფილების კითხვარის ფარგლებშიც;
- საბოლოო მომხმარებლების კომპიუტერების უსაფრთხოების შეფასებისათვის შესწავლილ იქნა თანამშრომლების კომპიუტერებზე[11] ოპერაციული სისტემების და აპლიკაციების მონიტორინგისა და განახლების არსებული პრაქტიკა. უზრუნველყოფილ იქნა შერჩეული თანამშრომლების კომპიუტერების სკანირება, ვირუსებისა და მავნე კოდისაგან დაცვისათვის არსებული მოწყობილობების ანალიზი;
- იდენტიფიცირდა ორგანიზაციის შიდა ქსელში ჩართული მოწყობილობები და ჩატარდა პოლიტიკების ანალიზი; ადგილზე შესასრულებელი სამუშაოების ფარგლებში შეფასდა მომხმარებელთა ცენტრალიზებული მართვის პრაქტიკა. კერძოდ, ორგანიზაციის ერთიან შიდა ქსელში გავრცელებული სხავადასხვა პოლიტიკა; ქსელის ფილტრაციისათვის გამოყენებული პროგრამული და აპარატურული უზრუნველყოფები და მათი მართვის პრაქტიკა; ასევე შეფასდა ვირტუალური კერძო ქსელის არსებობა, შესაბამისი ხელშეკრულება და VPN-ის გამოყენების პრაქტიკა.

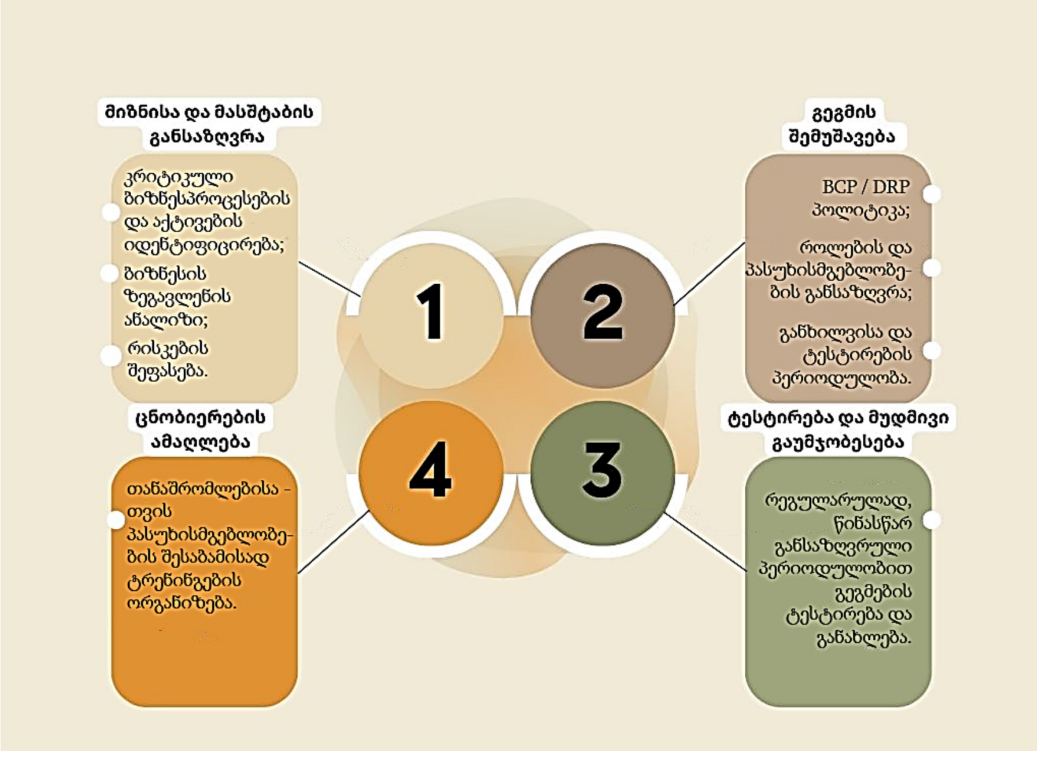
[11] აუდიტორული პროცედურის ფარგლებში შეფასდა თითოეულ აუდიტის ობიექტზე 5-5 კომპიუტერი.

2. ზოგადი ინფორმაცია

საჯარო სექტორის მიერ საზოგადოებისათვის მიწოდებული რიგი სერვისების წყვეტამ შესაძლოა არსებითი უარყოფითი გავლენა იქონიოს მოსახლეობის სოციალურ და ეკონომიკურ კეთილდღეობაზე.[12] სერვისების შეფერხების გამომწვევ მიზეზებს შეიძლება წარმოადგენდეს ბუნებრივი კატასტროფები, პანდემია, კიბერთავდასხმა და სხვ.

სერვისების უწყვეტობის მართვა გულისხმობს ორგანიზაციის საოპერაციო საქმიანობის უწყვეტობის შენარჩუნებას შემცირებული ან შეზღუდული ინფრასტრუქტურული და მატერიალური შესაძლებლობების გამოყენებით. აღნიშნული შედგება ქვემოთ მოცემულ დიაგრამაზე წარმოდგენილი ძირითადი კომპონენტებისგან.

დიაგრამა №1. ბიზნესუწყვეტობის მართვის სისტემის შემადგენელი კომპონენტები[13]



ბიზნესუწყვეტობის პროცესის მართვისა და დაგეგმვისათვის, კარგ პრაქტიკად[14] მიჩნეულია ორგანიზაციების მიერ ბიზნესუწყვეტობის გეგმის (BCP) შემუშავება, რომლის ფარგლებშიც უწყება გეგმავს და გამოცდის/ტესტავს აღდგენის ღონისძიებებს. კერძოდ, ამ გეგმაში ჩამოყალიბებულია, როგორ უნდა მოიქცეს ორგანიზაცია ინციდენტების შემთხვევაში, განსაზღვრულია შესაბამისი პასუხისმგებელი ერთეულები და თავდაპირველი/საწყისი ბიზნესმდგომარეობის აღდგენის საშუალებები.

[12] ჯანდაცვის, სოციალური, თავდაცვისა და საერთო დანიშნულების სახელმწიფო სერვისები, როგორიცაა, მაგალითად, სახელმწიფო გასაცემლების ადმინისტრირება, სოციალური დახმარებები, სამოქალაქო რეესტრის სერვისები და სხვ.

[13] COBIT 2019 სახელმძღვანელო დოკუმენტი.

[14] COBIT 2019 სახელმძღვანელო დოკუმენტი.

ბიზნესუწყვეტობის გეგმა ეხება ორგანიზაციის ზოგად ფუნქციებს, ხოლო უშუალოდ IT რესურსების მართვისათვის, მსგავს სიტუაციაში გამოიყენება კატასტროფიდან აღდგენის გეგმა (DRP). DRP წარმოადგენს პროცესს, სადაც ორგანიზაცია გეგმავს და გამოცდის/ტესტავს, როგორ უნდა აღადგინოს კატასტროფის შემდეგ ინფორმაციული ტექნოლოგიების ინფრასტრუქტურა.

საჯარო სერვისების მიწოდების უწყვეტობისათვის ერთ-ერთი მნიშვნელოვანი რგოლი საჯარო სექტორის თანამშრომლები არიან, რომელთა საქმიანობის შედეგად იქმნება სერვისი მოსახლეობისათვის. პანდემიის პირობებში აღნიშნული თანამშრომლებისათვის შესაბამისი სამუშაო გარემოს უზრუნველყოფა საჯარო სერვისების უწყვეტად მიწოდებისათვის მნიშვნელოვან წინაპირობად იქცა. სურათზე წარმოდგენილია უკეთესი პრაქტიკის შესაბამისად ეფექტიანი დისტანციური სამუშაო გარემოს უზრუნველყოფისათვის საჭირო საკითხები.

სურათი №1. დისტანციური სამუშაო გარემოს ეფექტიანობისა და უსაფრთხოებისათვის მნიშვნელოვანი საკითხები

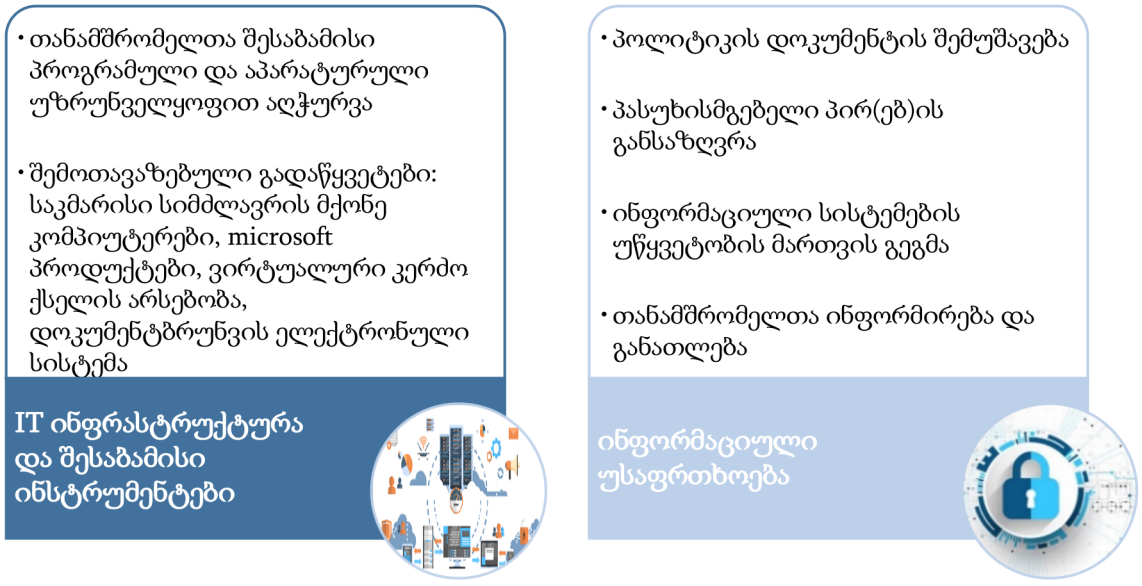
დისტანციური მუშაობის სახელმძღვანელოების[15] მიხედვით, პროდუქტიული სამუშაო გარემოს უზრუნველყოფისთვის მნიშვნელოვანია:

- დისტანციური მუშაობის პრინციპები;
- სამართლებრივი რეგულირება;
- IT ინსტრუმენტები და ოპტიმალური გადაწყვეტილებები;
- ინფორმაციული უსაფრთხოება;
- დისტანციური სამუშაო პროცესის ორგანიზება;
- დისტანციური შეხვედრების ორგანიზება და სხვ.

აღნიშნული დოკუმენტი ინფორმაციული ტექნოლოგიებისა და უსაფრთხოების მიმართულებით მოიცავს №2 დიაგრამაზე წარმოდგენილ კომპონენტებს.

[15] Toolkit on Teleworking in Public Administration, ევროსაბჭო, 2020 – ევროპის რიგი ქვეყნებისა და საერთაშორისო ორგანიზაციების მიერ შემუშავებული სახელმძღვანელო დოკუმენტი დისტანციურ მუშაობასთან მიმართებით; 2021 Guide to Telework and Remote Work in the Federal Government, United States Office Of Personnel Management, 2021; ავსტრალიის კიბერუსაფრთხოების ცენტრის მიერ გამოიცა სახელმძღვანელო მითითებები საჯარო სექტორში დისტანციური მუშაობის პროცესების მართვისათვის და სხვ.

დიაგრამა №2. დისტანციური მუშაობის სახელმძღვანელოში ასახული კომპონენტები



დისტანციური მუშაობის პრაქტიკის მიმართულებით მნიშვნელოვანი საკითხები, ასევე გაწერილია ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების ფარგლებში. საკანონმდებლო დონეზე განსაზღვრულია სერვისების უწყვეტობისა და დისტანციურად მუშაობის მინიმალური პრინციპები.[16] კერძოდ, ორგანიზაციებს კანონით მოეთხოვებათ, არსებობდეს სამოქმედო გეგმები, რომლებიც უზრუნველყოფს ოპერაციების შენარჩუნებას ან აღდგენას, ასევე ინფორმაციის ხელმისაწვდომობას (სათანადო დონეზე და მისაღებ დროში, ბიზნესპროცესის წყვეტის ან გაჩერების შემდეგ) და განსაზღვრავს აუცილებელ კონტროლს სამსახურს გარეთ მუშაობის პირობებში.

[16] ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები.

3. აუდიტის მიგნებები

3.1 IT მმართველობის მიმართულებით არსებული ნაკლოვანებები

საჯარო სერვისებისა და ადმინისტრაციული პროცესების გაციფრულების პირობებში არსებითი მნიშვნელობა შეიძინა ეფექტიანი IT მმართველობის პრაქტიკის არსებობამ. IT მმართველობის პრაქტიკის შეფასების ერთ-ერთი წყაროა COBIT ჩარჩო დოკუმენტი, რომელიც განსაზღვრავს ზოგად მიმართულებებს ეფექტიანი მმართველობითი სტრუქტურის შესაქმნელად. დოკუმენტი მკაფიოდ მიჯნავს უმაღლესი და საშუალო რგოლის მენეჯმენტის მიერ განსახორციელებელ აქტივობებს.

უმაღლესი რგოლის მენეჯმენტი უზრუნველყოფს[17] ორგანიზაციის მისიის, მიზნებისა და სტრატეგიული ხედვების განსაზღვრასა და მათი აღსრულების მონიტორინგს, ხოლო საშუალო რგოლის მენეჯმენტი განსაზღვრული მიმართულებების შესაბამისად გეგმავს, განავითარებს, წარმართავს და მონიტორინგს უწევს არსებულ პროცესებსა და IT სერვისებს. ამასთანავე, ორგანიზაციის ეფექტიანი ფუნქციონირებისათვის მნიშვნელოვანია აღნიშნულ რგოლებს შორის კომუნიკაცია, რომელიც წარმოდგენილია ქვემოთ მოცემულ სურათზე.

სურათი №2. პასუხისმგებლობების განაწილება RACI მატრიცის მიხედვით

A	უმაღლესი რგოლის მმართველობა (საბჭო)	CIO	საშუალო რგოლის მენეჯმენტი	IT მენეჯერი	მონიტორინგი/IT აუდიტორი
მიმართულებების განსაზღვრა	A, R	R	C	C	C
მართვისათვის შესაბამისი რესურსის უზრუნველყოფა	A	R	R	C	I
მიმართულებების განსაზღვრისა და მონიტორინგის განხორციელებისათვის შესაბამისი სტრუქტურისა და პროცესების შექმნა	A	C	I	I	I, R
შესაბამისი პროგრამების/სერვისების შექმნა და მართვა	A	R	C	C	I
ერთიანი მიდგომის ფარგლებში ბიზნეს და IT მიზნების დაკავშირება	A	R	C	C	C

R – პასუხისმგებელი (Responsible)
A – ანგარიშვალდებული (Accountable)
C – მრჩეველი (Consulted)
I – ინფორმირებული (Informed)

[17] COBIT 2019 Framework Governance and Management Objectives.

ეფექტიანი მმართველობითი პროცესების არსებობის საჭიროებას დამატებითი მნიშვნელობა შესძინა COVID-19-ის პანდემიამ. კერძოდ, ორგანიზაციაში ფორსმაჟორულ პირობებში რესურსების ეფექტიანი და პროდუქტიული მართვისათვის მნიშვნელოვან წინაპირობად ითვლება მაღალი ხარისხის IT მმართველობის არსებობა. მმართველობითი სისტემის შექმნა COBIT 2019-ის მიხედვით, მოიცავს ცხრილში წარმოდგენილ შემდეგ კომპონენტებს:

ცხრილი №1. IT მმართველობის შემადგენელი კომპონენტები

IT მმართველობის შემადგენელი კომპონენტები	პროცესების განსაზღვრა
	ქმედითი ორგანიზაციული სტრუქტურის ჩამოყალიბება
	შესაბამისი პოლიტიკის, პრინციპებისა და სახელმძღვანელო დოკუმენტების შექმნა ყოველდღიური აქტივობების ეფექტიანი მართვისათვის
	ინფორმაციის მართვის ეფექტიანი პოლიტიკის განსაზღვრა
	ეთიკისა და შესაბამისი ორგანიზაციული კულტურის უზრუნველყოფა
	ადამიანური რესურსებისა და შესაბამისი კომპეტენციების უზრუნველყოფა
	სერვისების, ინფრასტრუქტურისა და შესაბამისი აპლიკაციების უზრუნველყოფა/მხარდაჭერა

აუდიტის ფარგლებში შეფასდა შერჩეულ უწყებებში IT მმართველობის მიმართულებით არსებული პროცედურები და პრაქტიკები. გამოიკვეთა ნაკლოვანებები, რომლებიც დეტალურად განხილულია ქვემოთ წარმოდგენილ ქვეთავებში.

3.1.1 უწყვეტობა/კატასტროფიდან აღდგენის გეგმები

ეფექტიანი IT მმართველობის პრაქტიკა[18] გულისხმობს აქტივებისა და რისკების რეგულარულ იდენტიფიცირებას, მათ შეფასებას, შესაბამისი გეგმების არსებობას და კატასტროფისა თუ კონკრეტული რისკის რეალიზების შემთხვევაში, გეგმის მიხედვით მოქმედებას. ასეთი მიდგომა უზრუნველყოფს ნაკლები დროითი და ფინანსური რესურსის დანახარჯით კოორდინირებული ქმედებების შესაძლებლობას, არსებული IT ინვესტიციების პროდუქტიულ გადანაწილებასა და სიტუაციის ადეკვატური მართვის შესაძლებლობას. აღნიშნული პრაქტიკის ეფექტიანობას განაპირობებს ქმედითი IT მმართველობითი ორგანო, რომელიც შესაძლოა დაკომპლექტებული იყოს საშუალო რგოლის მენეჯერებით (საკვანძო, დარგობრივი ან მიმართულებების ხელმძღვანელი პირებით) და ინფორმაციული უსაფრთხოების მენეჯერით.

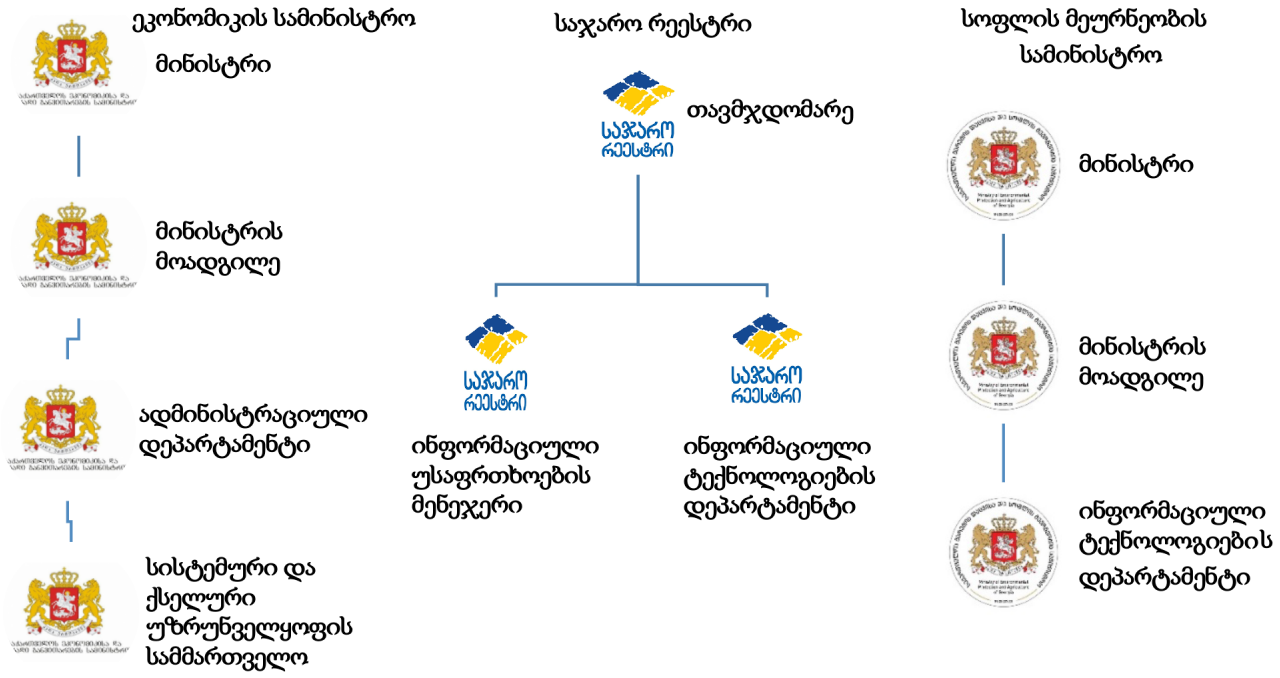
მათი კომუნიკაცია და ურთიერთშეთანხმებული კოორდინაცია ხელს უწყობს ინფორმირებული გადაწყვეტილებების მიღებას ისეთ საკითხებთან მიმართებით, როგორებიცაა:

- ორგანიზაციის სტრატეგიული ხედვისა და მიმართულების განსაზღვრა ინფორმაციული აქტივების ეფექტიან და მიზნობრივ გამოყენებასთან მიმართებით;
- შესაბამისობის უზრუნველყოფა კანონებთან, რეგულაციებსა და პოლიტიკებთან;
- არსებული და პოტენციური რისკების მართვა IT პროცესებსა და ინფორმაციულ აქტივებთან მიმართებით.

[18] COBIT 2019, ბიზნესის მდგრადობის უზრუნველყოფა (DSS04.02).

არსებული მდგომარეობით აუდიტის ობიექტების სტრუქტურა და ინფორმაციული ტექნოლოგიების დეპარტამენტების/სამმართველოების გადანაწილება წარმოდგენილია დიაგრამაზე.

დიაგრამა №3. აუდიტის ობიექტების სტრუქტურა



აუდიტორული პროცედურების შედეგად შეფასდა უწყებებში არსებული IT მმართველობითი სტრუქტურა და პრაქტიკა. კერძოდ, აუდიტის ჯგუფმა შეისწავლა გადაწყვეტილებების მიღებისა და თანმდევი პროცესები – საჭიროებებისა და რისკებთან მიმართებით (შეფასდა, ბიზნესუწყვეტობის პროცესი, ინფორმაციული აქტივების საჭიროებებისა და რისკების ანალიზის პრაქტიკა). შესწავლის შედეგად გამოჩნდა, რომ უწყებებში უკეთესი პრაქტიკის[19] შესაბამისი რიგი კომპონენტები IT მმართველობისათვის უზრუნველყოფილი არ არის. კერძოდ, ორგანიზაციებში არსებული მმართველობითი/ორგანიზაციული სტრუქტურა სათანადოდ ვერ უზრუნველყოფს შესაბამისი/საჭირო პროცედურების დანერგვის ინიციირებას და მართვას. მმართველობითი პროცესები არ არის სტრუქტურირებული და ფორმალიზებული, კომუნიკაციის ნაკლებობის პირობებში არ ხორციელდება საჭიროებების პერიოდული იდენტიფიცირება და მმართველი რგოლის მიერ შესაბამისი მიმართულებების განსაზღვრა.

უკეთესი პრაქტიკის შესაბამისად, ორგანიზაციაში ბიზნესუწყვეტობისა და კატასტროფიდან აღდგენის პროცესების შემუშავებასა და დანერგვაზე პასუხისმგებელი პირი, როგორც წესი, არის ინფორმაციული უსაფრთხოების მენეჯერი (მნიშვნელოვანია აღნიშნულ პროცესებში მაღალი რგოლის მენეჯმენტის ჩართულობა). როგორც №3 დიაგრამაზეა წარმოდგენილი, ინფორმაციული უსაფრთხოების მენეჯერის პოზიცია მხოლოდ საჯარო რეესტრის ეროვნული სააგენტოს ორგანიზაციულ სტრუქტურაშია გათვალისწინებული.

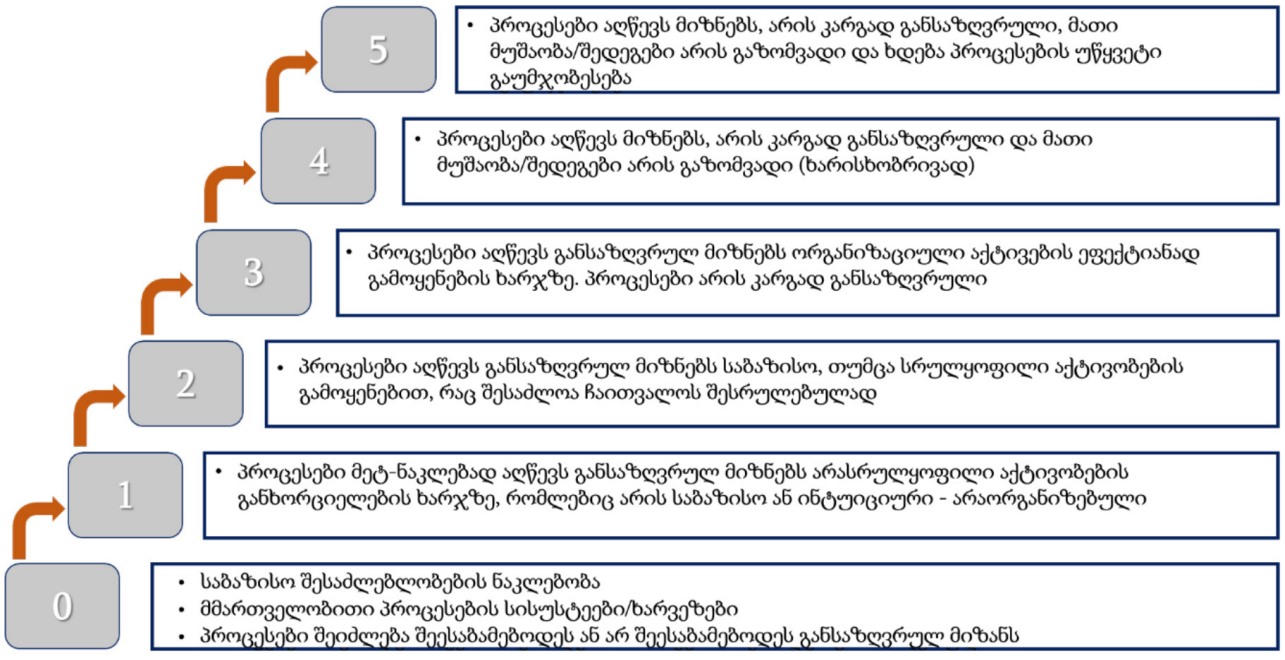
აღნიშნულის საფუძველზე, აუდიტის 3 ობიექტიდან მხოლოდ საჯარო რეესტრის ეროვნულ სააგენტოს ჰქონდა დაწყებული მუშაობა სერვისების უწყვეტობის პროცესების შემუშავებასა

[19] იხ. ცხრილი №1. IT მმართველობის შემადგენელი კომპონენტები.

და გამართვაზე – სამუშაოები მოიცავდა საწყის ეტაპზე ბიზნესის ზეგავლენის ანალიზის შემუშავებას. სამინისტროებში ამ მიმართულებით ნაბიჯები ჯერ არ გადადგმულა.

ქვემოთ მოყვანილ დიაგრამაზე წარმოდგენილია COBIT 19 სახელმძღვანელო ჩარჩო დოკუმენტით განსაზღვრული შესაძლებლობების სიმწიფის მოდელი,[20] რომლის მიხედვით ფასდება ორგანიზაციების მიმდინარე მდგომარეობა IT მმართველობასა და შესაბამის პროცესებთან მიმართებით.

დიაგრამა №4. შესაძლებლობების სიმწიფის მოდელი



კერძოდ, აღნიშნული მოდელის მიხედვით შესაძლებელია შეფასდეს, უწყებებს რამდენად გამართული და სრულყოფილი პროცესები აქვთ IT მმართველობასთან მიმართებით, რა პროცესები საჭიროებს გაუმჯობესებას და რა ნაბიჯები უნდა გადაიდგას სასურველი შედეგების მისაღწევად.[21]

აუდიტის ფარგლებში შეფასებული პროცესების მიხედვით შესწავლილი უწყებები შესაძლებლობების სიმწიფის მოდელის მიხედვით პირველ და მე-2 საფეხურებს შორის არიან.[22] კერძოდ, საჯარო რეესტრის ეროვნულ სააგენტოში ბიზნესუწყვეტობის, აქტივებისა[23] და რისკების მართვის მიმართულებით რიგი ღონისძიებები გატარებულია, თუმცა არასრულყოფილია, ხოლო ეკონომიკისა და სოფლის მეურნეობის სამინისტროები ამ მიმართულებებით ქმედითი ნაბიჯების გადადგმას საჭიროებენ.

---

[20] Capability Maturity Model Integration (CMMI)-COBIT 2019 Framework Governance and Management Objectives.

[21] საუკეთესო პრაქტიკის მიხედვით, ქმედითი IT მმართველობის პირობებში, ორგანიზაციები, სულ მცირე, მე-3 საფეხურის მოთხოვნებს უნდა აკმაყოფილებდნენ.

[22] აღნიშნული შეფასება გაკეთდა რამდენიმე პროცესთან მიმართებით: ბიზნესუწყვეტობის მართვა, აქტივების მართვა, რისკების მართვა.

[23] აღნიშნული საკითხი დეტალურად განხილულია ქვეთავში: 3.1.4 თანამშრომელთა უზრუნველყოფა საჭირო რესურსებითა და მხარდამჭერი სერვისებით.

შედეგად, შესწავლილ უწყებებში IT მმართველობის პრაქტიკაში შეიმჩნევა ნაკლოვანებები და ვერ უზრუნველყოფს:

- მმართველობისათვის საჭირო ფორმალური პროცედურებისა და პოლიტიკის შემუშავებას, რათა შეიქმნას/დაგროვდეს ინსტიტუციური ცოდნა;
- ფორსმაჟორულ სიტუაციაში ორგანიზაციის მხრიდან დროული და ინფორმირებული გადაწყვეტილებების მიღების შესაძლებლობას.

შესაბამისად, გამოვლინდა ფორსმაჟორული სიტუაციებისადმი ტექნიკური მზაობის დაბალი მაჩვენებელი, რომელიც რეალიზდა წინამდებარე ანგარიშში წარმოდგენილ საკითხებში (იხ. ქვეთავი 3.1 – IT მმართველობის მიმართულებით არსებული ნაკლოვანებების გავლენა).

3.1.2 დისტანციური მუშაობის პოლიტიკა

დისტანციური მუშაობის პოლიტიკა და პროცედურები უზრუნველყოფს, სამსახურის ფიზიკური გარემოს გარეთ, საჯარო მოხელის მიერ სამსახურებრივი მოწყობილობით სამუშაოს შესრულებისას, გარკვეული საერთო წესებისა და სტანდარტული პირობების დაცვას.

ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების თანახმად, ორგანიზაციებმა დისტანციური მუშაობისათვის უნდა შეიმუშაონ პოლიტიკა, რომელიც განსაზღვრავს დისტანციურ მუშაობასთან დაკავშირებულ შეზღუდვებსა და პირობებს. კერძოდ, ასეთის არსებობის შემთხვევაში, მხედველობაში უნდა იქნეს მიღებული შემდეგი საკითხები:

- პირად საკუთრებაში არსებული კომპიუტერების შეზღუდვები;
- დისტანციური მუშაობის ადგილის გარემო პირობების მოთხოვნების იდენტიფიცირება და თანამშრომლებთან აღნიშნულის შესახებ კომუნიკაცია;
- დისტანციური მუშაობის ადგილების ფიზიკური უსაფრთხოება, შენობის და ლოკალური გარემოს უსაფრთხოების მხედველობაში მიღებით;
- სახლის ქსელების გამოყენება და უსადენო კავშირგაბმულობის ქსელების (wireless) კონფიგურირების შეზღუდვები ან მოთხოვნები;
- ორგანიზაციის შიდა სისტემებზე დისტანციური წვდომა, ინფორმაციის სენსიტიურობა, რომელზე წვდომაც და რომლის გადაცემაც ხორციელდება საკომუნიკაციო ხაზებით და მთლიანად სისტემის სენსიტიურობა;
- ვირტუალური ე.წ. „დესკტოპ წვდომის“ უზრუნველყოფა;
- მავნე კოდებისგან დაცვა.

მნიშვნელოვანია აღნიშნული პოლიტიკის მექანიზმების და უსაფრთხოების მოთხოვნების შესახებ თანამშრომლებთან კომუნიკაცია, რათა მათ იცოდნენ, როგორ უნდა უზრუნველყონ დისტანციური სამუშაო გარემოდან სამსახურებრივი ინფორმაციის დაცვა.

აუდიტის ობიექტების მიერ არ ყოფილა შემუშავებული დისტანციური მუშაობის პოლიტიკა და შესაბამისი პროცედურები. აღნიშნული მიმართულებით გამონაკლისი იყო საჯარო რეესტრის ეროვნული სააგენტო, რომელსაც შემუშავებული ჰქონდა დისტანციური წვდომის/მუშაობის პოლიტიკა, თუმცა აღნიშნული დოკუმენტის საოპერაციო გარემოში არ დამტკიცებულა.

აღსანიშნავია, რომ დისტანციური მუშაობის პოლიტიკის არქონის მიუხედავად,[24] აუდიტის ობიექტების ინფორმაციული ტექნოლოგიების დეპარტამენტებმა/სამმართველოებმა უზრუნველყვეს სამუშაოს განხორციელებისათვის საჭირო მინიმალური სახელმძღვანელო მითითებების მიწოდება სხვადასხვა საშუალებებით (მაგალითად, ელექტრონული ფოსტა, ინტრანეტი). აუდიტის ფარგლებში შეფასდა ორგანიზაციების მიერ გატარებული ღონისძიებები მინიმალურ მოთხოვნებთან მიმართებით. შედეგები წარმოდგენილია ქვემოთ მოყვანილ ცხრილში:

ცხრილი №2. უწყებების ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებთან შესაბამისობის მდგომარეობა[25]

მინიმალური მოთხოვნები	სსიპ - საჯარო რეესტრის ეროვნული სააგენტო	საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო	საქართველოს გარემოს დაცვისა და სოფლის მეურნეობის სამინისტრო
ვირტუალური ე.წ. „დესკტოპ წვდომის“ უზრუნველყოფა;			
მავნე კოდებისგან დაცვა;			
ორგანიზაციის შიდა სისტემებზე დისტანციური წვდომა, ინფორმაციის სენსიტიურობა, რომელზე წვდომაც და რომლის გადაცემაც ხორციელდება საკომუნიკაციო ხაზებით და მთლიანად სისტემის სენსიტიურობა;			
პირად საკუთრებაში არსებული კომპიუტერების შეზღუდვები;			
დისტანციური მუშაობის ადგილის გარემო პირობების მოთხოვნების იდენტიფიცირება და კომუნიკაცია;			
დისტანციური მუშაობის ადგილების ფიზიკური უსაფრთხოება, ზოგადად, შენობის და ლოკალური გარემოს უსაფრთხოების მხედველობაში მიღებით;			
სახლის ქსელების გამოყენება და უსადენო კავშირგაბმულობის ქსელების (wireless) კონფიგურირების შეზღუდვები ან მოთხოვნები.			

შესრულებულია
ნაწილობრივ შესრულებულია
შეუსრულებელია

უწყვეტობის პროცესების მართვისათვის COBIT ჩარჩო დოკუმენტის მიხედვით, შემდგომ პერიოდში მსგავსი რისკების რეალიზებისას ორგანიზაციების მზაობისთვის მნიშვნელოვანია:

- შესაბამისი პროცესების გადახედვა წარსული გამოცდილების გათვალისწინებით;
- არსებული ნაკლოვანებების იდენტიფიცირება და შემდგომში მათი გამოსწორებისათვის მკაფიოდ განსაზღვრული და გაწერილი სამოქმედო გეგმის შემუშავება.[26]

[24] იგულისხმება სამინისტროები.

[25] ნაწილობრივ შესრულებულია-უწყებები ვერ უზრუნველყოფდნენ თანაშრომელთა პირადი მოხმარების ტექნიკის მართვას.

[26] ბიზნესის მდგრადობის (resilience) უზრუნველყოფა (DSS04.02), COBIT 2019.

აღსანიშნავია, რომ პანდემიის დაწყების შემდგომ, დისტანციურ სამუშაო რეჟიმზე გადასვლის პროცესი ორგანიზაციებისათვის მნიშვნელოვანი გამოცდილებაა, რომლის გაანალიზებისა და გათვალისწინების შემთხვევაში უწყებებს რიგი პროცედურების გაუმჯობესების პოტენციალი აქვთ.

3.1.3 IT მმართველობის ნაკლოვანებების გავლენა

დიაგრამაზე წარმოდგენილია ის ძირითადი წინაპირობები, რომლებიც ხელს უწყობს დისტანციური მუშაობის კარგ პრაქტიკას.

დიაგრამა №5 დისტანციური მუშაობის ეფექტიანი პრაქტიკის წინაპირობები[27]

აღნიშნული მიმართულებებით არსებული ნაკლოვანებები დეტალურად წარმოდგენილია ქვემოთ მოცემულ ქვეთავებში.

3.1.4 თანამშრომელთა უზრუნველყოფა საჭირო რესურსებითა და მხარდამჭერი სერვისებით

დისტანციური მუშაობის პრაქტიკის ეფექტიანობისათვის მნიშვნელოვანი წინაპირობა არის თანამშრომელთა შესაბამისი კომპიუტერული მოწყობილობებითა და ინსტრუმენტებით უზრუნველყოფა, ასევე მნიშვნელოვანია საჯარო სერვისების უწყვეტობისათვის კრიტიკული ბიზნესპროცესებისა და თანამშრომლების განსაზღვრა.

[27] დისტანციური მუშაობის სახელმძღვანელო, სსიპ – საჯარო სამსახურის ბიურო.

პრიორიტეტულობის/კრიტიკულობის განსაზღვრისათვის საჭიროა შესაბამისი აქტივების იდენტიფიცირება და კლასიფიცირება. ინფორმაციული უსაფრთხოების საკანონმდებლო მოთხოვნების შესაბამისად, აქტივებს მიეკუთვნება როგორც ფიზიკური ინფრასტრუქტურა, მონაცემები და ინფორმაცია, პროგრამული უზრუნველყოფები და ინფორმაციული სისტემები, ასევე ადამიანური რესურსები, რომლებიც ღირებულია ორგანიზაციისათვის.[28] მნიშვნელოვანია, ყოველ ინფორმაციულ აქტივს მიენიჭოს კრიტიკულობის შესაბამისი კლასი,[29] რომლის მიხედვით უზრუნველყოფილი იქნება შესაბამისი კონტროლის მექანიზმების დანერგვა.

ხარისხიანი ინფორმაცია აქტივების შესახებ, ორგანიზაციას შესაძლებლობას მისცემს ფორსმაჟორულ პირობებში განახორციელოს კრიტიკულად მნიშვნელოვანი კადრებისათვის საჭირო რესურსების დროულად მობილიზება, მიიღოს ინფორმირებული გადაწყვეტილებები და გაატაროს სათანადო უსაფრთხოების ზომები.

აუდიტის ფარგლებში შეფასდა ობიექტების მიერ აქტივების მართვასთან მიმართებით განხორციელებული აქტივობები როგორც პანდემიამდე, ასევე მისი დაწყების შემდგომ პერიოდში. შესწავლის შედეგად გამოჩნდა, რომ სამინისტროებს არ აქვთ აღრიცხული და კლასიფიცირებული ორგანიზაციის ფარგლებში არსებული ინფორმაციული აქტივები და შესაბამისად, არც შესაბამისი ფორმალური პროცედურები და დოკუმენტაციაა შემუშავებული. საჯარო რეესტრის ეროვნულ სააგენტოში მიმდინარეობს არსებულ ბიზნესპროცესებთან მიმართებით აქტივების გამოვლენა და შესაბამისი რეესტრის წარმოება.

IT მმართველობის შესაბამისი პროცედურებისა და პოლიტიკის მექანიზმების არარსებობამ, თავის მხრივ, განაპირობა რიგი ნაკლოვანებები, როგორიცაა, სამსახურის კუთვნილი კომპიუტერული ტექნიკის თანამშრომლებისთვის ოპტიმალური გადანაწილების საკითხი. პირადი საკუთრების კომპიუტერული მოწყობილობის გამოყენება არ წარმოადგენს მნიშვნელოვან ხარვეზს, თუ აღნიშნული განხორციელებულია შესაბამისი პროცედურების დაცვით (დეტალურად განხილულია ქვეთავში: 3.1.5 პირადი მოწყობილობების გამოყენება). ამასთანავე, იმის გათვალისწინებით, რომ აუდიტის ობიექტებში არ იყო გამოყოფილი კრიტიკული სერვისები და კრიტიკული პოზიციები, რთულია არსებული კომპიუტერული მოწყობილობების პრიორიტეტულობის/კრიტიკულობის მიხედვით გადანაწილების შეფასება.

მხარდამჭერი სერვისების კუთხით მნიშვნელოვანია აღინიშნოს, რომ უწყებებმა შეძლეს შესაბამისი ტექნიკური პერსონალის მობილიზება და თანამშრომელთა სათანადო მხარდაჭერა. უწყებებში,[30] რომელთაც დანერგილი ჰქონდათ მხარდამჭერი IT ჯგუფისათვის შესაბამისი პროგრამული უზრუნველყოფები,[31] შეფასდა აღნიშნული სისტემის მიერ გენერირებული მონაცემები წლების მიხედვით.[32]

---

[28] „ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის“. კანონი „ინფორმაციული უსაფრთხოების შესახებ“, მუხლი 2, „კ“ ქვეპუნქტი.

[29] კონფიდენციალური ან შინასამსახურებრივი გამოყენების. კანონი „ინფორმაციული უსაფრთხოების შესახებ“, მუხლი 5, პუნქტი 1.

[30] საქართველოს გარემოს დაცვისა და სოფლის მეურნეობის სამინისტრო და სსიპ – საჯარო რეესტრის ეროვნული სააგენტო.

[31] თანამშრომელი მუშაობის პროცესში წარმოქმნილი ტექნიკური ხასიათის პრობლემის თუ მოვლენის შესახებ აფიქსირებს აღნიშნული მიზნით შემუშავებულ/შეძენილ პროგრამულ გადაწყვეტაში.

[32] იმის გათვალისწინებით, რომ აღნიშნული პროგრამების გამოყენება არ არის სავალდებულო და არის შემთხვევები, როცა თანამშრომლები მაინც სატელეფონო ზარის საშუალებით ახორციელებენ ხარვეზებზე კომუნიკაციას, რეალური მდგომარეობა შესაძლოა მცირედით განსხვავდებოდეს პროგრამაში ასახული მდგომარეობისაგან.

ცხრილი №3. წლების მანძილზე მომხმარებელთა მიერ იდენტიფიცირებული ტექნიკური პრობლემები

გარემოს დაცვისა და სოფლის მეურნეობის სამინისტრო	2019		2020		2021	
კატეგორია	რაოდ.	საშ. მოგვარების დრო (სთ.)	რაოდ.	საშ. მოგვარების დრო (სთ.)	რაოდ.	საშ. მოგვარების დრო (სთ.)
ინტრანეტის პრობლემა	5	5	5	216	16	57
პროგრამების დაყენება	132	25	76	95	387	12
რესურსებთან წვდომა	72	48	60	159	53	31
საოფისე პროგრამები	61	20	20	232	28	41
ტექნიკური პრობლემა	346	56	125	92	162	21
სხვა	1452	57	935	296	1532	59
საჯარო რეესტრის ეროვნული სააგენტო	2019		2020		2021	
კატეგორია	რაოდ.	საშ. მოგვარების დრო (სთ.)	რაოდ.	საშ. მოგვარების დრო (სთ.)	რაოდ.	საშ. მოგვარების დრო (სთ.)
პროგრამული	49599	41	43191	20	39844	8
სამომხმარებლო პროგრამები	165	316	161	138	266	253
ტექნიკური პრობლემა	9031	50	7861	55	9344	17

როგორც ცხრილიდან ჩანს, სოფლის მეურნეობის სამინისტროში, 2020 წელს დისტანციურ სამუშაო რეჟიმზე გადასვლის პირობებში დაფიქსირებული ტექნიკური პრობლემების რაოდენობა შემცირდა, თუმცა მათი აღმოფხვრის დრო მნიშვნელოვნად გაზრდილია, რაც შესაძლოა განპირობებული იყოს ახალ სამუშაო პირობებთან ადაპტაციის პროცესით (თუმცა აღნიშნულის რეგულირება უზრუნველყოფილ იქნა 2021 წლისთვის), ხოლო საჯარო რეესტრის ეროვნული სააგენტოს შემთხვევაში, წლების მიხედვით პრობლემების რაოდენობაში არსებითი ცვლილებები არ შეიმჩნევა, ხოლო პრობლემების აღმოფხვრის საშუალო დრო – 2021 წელს გაუმჯობესებულია.

გარდა ტექნიკური ანგარიშების ანალიზისა, აუდიტის ფარგლებში შეფასდა თანამშრომლების კმაყოფილება მიღებული მხარდამჭერი სერვისებით.[33] აღნიშნულთან მიმართებით აუდიტის ობიექტების თანამშრომლების მიერ ძირითად გამოწვევად დასახელდა – სამუშაო პროგრამებზე წვდომის სირთულე და მონაცემების დამუშავების გახანგრძლივებული დრო. თუმცა აღსანიშნავია, რომ გამოკითხულ თანამშრომელთა უმრავლესობამ დადებითად შეაფასა IT დამხმარე ჯგუფის საქმიანობა.

3.1.5 პირადი მოწყობილობების გამოყენება

თანამშრომლების მიერ პირად საკუთრებაში მყოფი კომპიუტერების გამოყენების შემთხვევაში, ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნებით განსაზღვრულია ორგანიზაციის მიერ გასატარებელი კონკრეტული აქტივობები. კერძოდ, მნიშვნელოვანია, რომ ორგანიზაციამ, სულ მცირე, უზრუნველყოს:

- მოწყობილობების პირადი და სამსახურებრივი მიზნებით გამოყენების გამიჯვნა, რათა თავიდან იქნეს აცილებული ორგანიზაციისთვის მნიშვნელოვანი ინფორმაციის გამჟღავნება/დაკარგვა/არასათანადო დამუშავება;[34]
- სამსახურებრივ ინფორმაციაზე წვდომის შესაძლებლობა მხოლოდ მას შემდეგ, რაც მომხმარებლები ხელს მოაწერენ შესაბამის ხელშეკრულებას, რომელიც განსაზღვრავს მათ მოვალეობებს (კომპიუტერის ფიზიკური დაცვა, პროგრამული განახლებები).

იმ ორგანიზაციის თანამშრომლებს, რომელთაც არ აღმოაჩნდათ საკმარისი კომპიუტერული მოწყობილობები, მოუხდათ პირად საკუთრებაში არსებული კომპიუტერების გამოყენება სამსახურებრივი მიზნებისათვის. აუდიტის ჯგუფმა ჩაატარა თანამშრომელთა ელექტრონული გამოკითხვა,[35] რომლის შესწავლის ერთ-ერთი საკვანძო საკითხი იყო შესაბამისი მატერიალურ-ტექნიკური ბაზის არსებობა. კერძოდ, აუდიტის ფარგლებში შერჩეულ სამივე უწყებაში თანამშრომლებს გაეგზავნათ კითხვარები დისტანციური სამუშაო რეჟიმის პირობებში კომპიუტერული ტექნიკის მოხმარებასთან დაკავშირებულ საკითხებზე. შედეგები წარმოდგენილია ქვემოთ მოცემულ დიაგრამაზე:

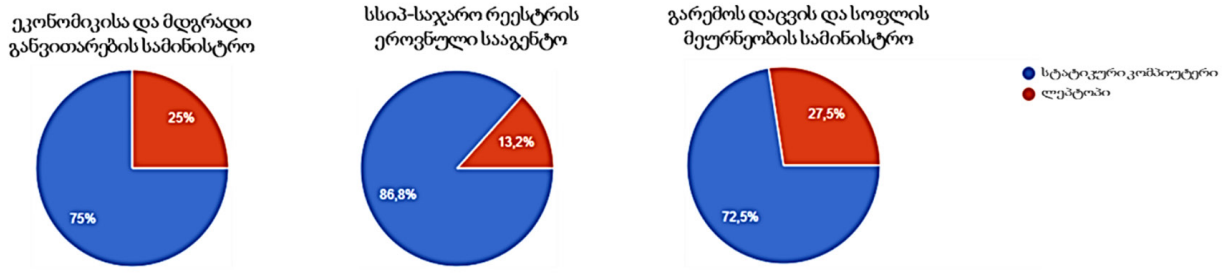
[33] აღნიშნული კვლევის ფარგლებში გათვალისწინებული იყვნენ ის თანამშრომლები, რომლებიც ძირითადად იმყოფებოდნენ მუშაობის დისტანციურ რეჟიმზე და არ იყვნენ ინფორმაციული ტექნოლოგიების დეპარტამენტში დასაქმებული: საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტროში 167 თანამშრომლიდან გამოიკითხა 76; საქართველოს გარემოს დაცვისა და სოფლის მეურნეობის სამინისტროში 209 თანამშრომლიდან – 138; სსიპ – საჯარო რეესტრის ეროვნული სააგენტოში 453 თანამშრომლიდან – 219.

[34] როგორიც შესაძლოა იყოს სხვადასხვა გარემო/მომხმარებელი პირადი და სამსახურებრივი მიზნებისათვის.

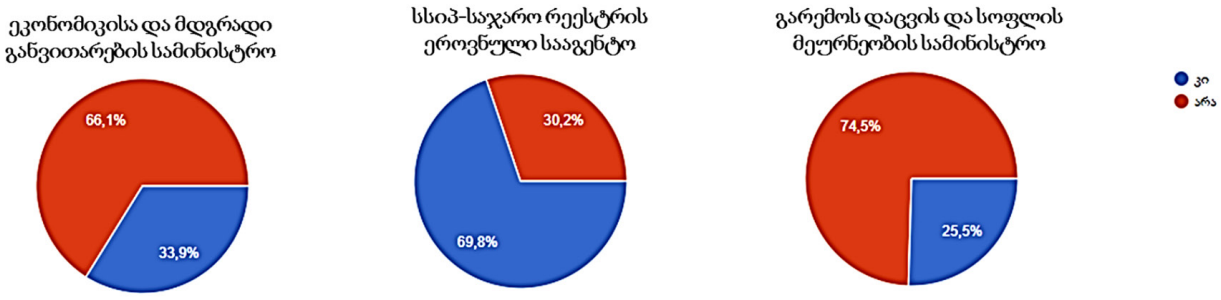
[35] კითხვარის ადრესატები შეირჩნენ თანამშრომლთა იმ წრიდან, რომლებიც ძირითადად დისტანციურად მუშაობდნენ. გამოკითხვის ელექტრონულ ფორმაზე პასუხი გასცა საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტროში 56 თანამშრომელმა; საქართველოს გარემოს დაცვის და სოფლის მეურნეობის სამინისტროში – 51-მა; სსიპ – საჯარო რეესტრის ეროვნულ სააგენტოში – 53-მა.

დიაგრამა №6 თანამშრომელთა გამოკითხვის შედეგები

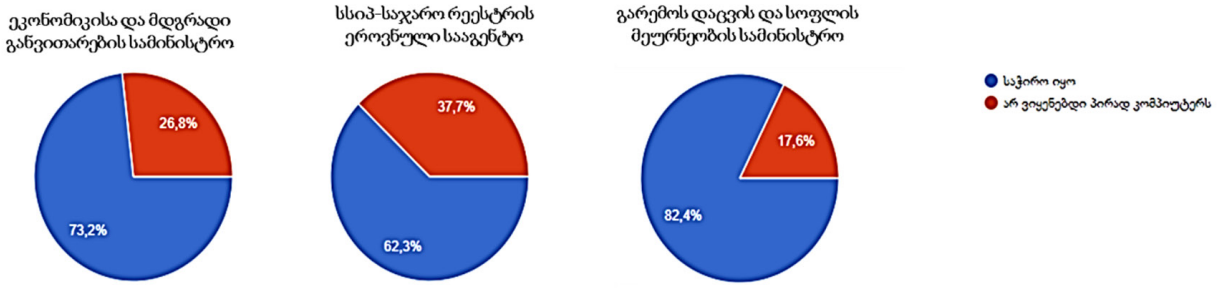
მუშაობის დისტანციურ რეჟიმზე გადასვლამდე რა ტიპის კომპიუტერულ მოწყობილობას იყენებდით?



იყო თუ არა მოწოდებული სამსახურის მიერ დისტანციური მუშაობისთვის საჭირო მოწყობილობები (ლეპტოპები)?



რამდენად შეგექმნათ სამსახურებრივი ამოცანების შესრულების პროცესში პირადი მოხმარების მოწყობილობების (კომპიუტერების) გამოყენების საჭიროება?



თანამშრომელთა გამოკითხვის შედეგები აჩვენებს, რომ ძირითად შემთხვევებში თანამშრომლები ლეპტოპებით (მობილური მოწყობილობებით) სრულად ვერ იყვნენ უზრუნველყოფილნი. აღნიშნული გამოწვეული იყო იმ გარემოებით, რომ სამივე უწყებაში თანამშრომელთა დიდი ნაწილი იყენებდა სტატიკურ კომპიუტერს. გამოკითხვის თანახმად, საჯარო რეესტრის თანამშრომლები შედარებით უკეთესად იყვნენ უზრუნველყოფილნი ლეპტოპებით.

ამასთანავე, ჩატარებულმა გამოკითხვამ აჩვენა, რომ უწყებების მიერ კომპიუტერული მოწყობილობების მიწოდების მიუხედავად, თანამშრომლებს მაინც უწევდათ პირადი საკუთრების კომპიუტერების/ტექნიკის გამოყენება დისტანციური მუშაობისთვის. კერძოდ, საჯარო რეესტრში მიუხედავად იმისა, რომ 69%-ს გადაეცა სამსახურის კუთვნილი ლეპტოპი, გამოკითხულების 62% ასახელებს, რომ უწევდათ პირად საკუთრებაში არსებული კომპიუტერების გამოყენება. ასევე, შედარებით მცირე, მაგრამ მსგავსი განსხვავებებია აღნიშნული ორი კომპონენტის პროცენტულ გადანაწილებაში ეკონომიკისა და სოფლის მეურნეობის სამინისტროებში. აღნიშნული განპირობებული იყო დაბალი წარმადობისა და/ან მოძველებული ტექნიკის მიწოდებით.

პირადი საკუთრების კომპიუტერების გამოყენების შემთხვევაში, აუდიტის ობიექტებს არ ჰქონდათ წინასწარ შემუშავებული გეგმა/პოლიტიკა, რომლის მიხედვით განსაზღვრული იქნებოდა ის მინიმალური აქტივობები, რაც ქსელის უსაფრთხოების უზრუნველსაყოფად იყო საჭირო. უწყებებმა საწყის ეტაპზე განახორციელეს მათი შემოწმება და ვირტუალური კერძო ქსელის (VPN) პროგრამული უზრუნველყოფის დაყენება, თუმცა შემდგომი ნაბიჯები, როგორებიცაა, თანამშრომლებისთვის აღნიშნული მოწყობილობების სამსახურებრივი მიზნებისათვის გამოყენების გამიჯვნა, მათთვის მინიმალური მოთხოვნების შესახებ კომუნიკაცია და მათი ვალდებულებების შემდგომი მონიტორინგი, ვერ იქნა უზრუნველყოფილი.

3.1.6 საბოლოო მომხმარებელთა უსაფრთხოება

დისტანციურად მუშაობის პოლიტიკისა და წინასწარ განსაზღვრული ქმედების ნორმების არ არსებობა, ორგანიზაციისათვის დაკავშირებულია რისკებთან. კერძოდ, აღნიშნულ პროცესთან მიმართებით გასათვალისწინებელი საკითხებია:

- სენსიტიური მონაცემების დაცვა;
- ქსელების დაცვა, რომლებთანაც დაკავშირებულია თანამშრომლების მოწყობილობები;
- პასუხისმგებლობა და ანგარიშვალდებულება მოწყობილობებსა და მათზე არსებულ ინფორმაციაზე;
- ორგანიზაციის მონაცემების წაშლა თანამშრომლების საკუთრებაში არსებული მოწყობილობებიდან სამუშაოს შეწყვეტის ან მოწყობილობის დაკარგვისას.

იმ მიზნით, რომ ორგანიზაციამ თავიდან აიცილოს დისტანციური მუშაობის პრაქტიკის თანმდევი რისკები, არსებობს რიგი მნიშვნელოვანი წინაპირობები:[36] კერძოდ, ორგანიზაციებს უნდა გააჩნდეთ შესაბამისი პროგრამული და აპარატურული უზრუნველყოფის შესაძლებლობები, რომლებსაც ექნებათ მწარმოებლის ლიცენზია და მხარდაჭერა. უსაფრთხოების აპარატურული და პროგრამული უზრუნველყოფების კონფიგურირება უზრუნველყოფილი უნდა იყოს ბიზნესმიზნებიდან გამომდინარე. მნიშვნელოვანია ინტერნეტრესურსსა და სამსახურის ინფორმაციაზე თანამშრომელთა დაცული/დაშიფრული გზით კავშირი.

[36] https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/telework-successfully-during-and-after-the-covid-19-pandemic

აუდიტის ფარგლებში შეფასდა თანამშრომელთა კომპიუტერები[37] და მათი დაცულობის დონეები. კერძოდ, სამივე უწყებაში[38] ჩატარდა კომპიუტერების სკანირება მავნე კოდებზე და შეფასდა უსაფრთხოების მიმართულებით არსებული მდგომარეობა. №4 ცხრილში წარმოდგენილია აუდიტის ფარგლებში ჩატარებული აქტივობები და შესაბამისი შედეგები:

ცხრილი №4. განხორციელებული აუდიტორული პროცედურების შედეგები[39]

აუდიტის ჯგუფის მიერ განხორციელებული ტესტირებები	შედეგი		
	სოფელი	ეკონომიკა	Napr
სისტემის მავნე კოდზე შემოწმება			
თანამშრომლების მიერ ადმინისტრატორის უფლებით სარგებლობა			
რამდენიმე მომხმარებლის (User) არსებობა ერთ მოწყობილობაზე			
სამსახურებრივი საქმიანობისთვის არასაჭირო და არასასურველი უცხოური ქვეყნის ინტერნეტ რესურსთან წვდომა			
ანტივირუსის რეგულარული განახლება და პერიოდული სკანირების კონფიგურაცია			

პრობლემა არ იდენტიფიცირდა

პრობლემა ნაწილობრივ იდენტიფიცირდა

პრობლემა იდენტიფიცირდა

სისტემის მავნე კოდზე შემოწმება – აუდიტის ჯგუფის მიერ მავნე კოდზე შემოწმდა თითოეული ობიექტის რამდენიმე შერჩეული კომპიუტერული მოწყობილობა. შემოწმებული უწყებებიდან მავნე კოდი აღმოჩნდა სსიპ – საჯარო რეესტრის ეროვნულ სააგენტოში, რაც გამოწვეული იყო არალიცენზირებული პროდუქტების გამოყენებით.

თანამშრომლების მიერ ადმინისტრატორის უფლებით სარგებლობა – ადმინისტრატორის როლი და შესაბამისი პრივილეგიები შეიძლება მიენიჭოს ნებისმიერ პროფილს (მომხმარებელს – User) ბიზნესპროცესის საჭიროებიდან გამომდინარე. აღნიშნული როლი საშუალებას იძლევა მომხმარებლის ოპერაციულ სისტემაზე, როგორც პროგრამული უზრუნველყოფების დაყენების/წაშლის/რედაქტირების, ასევე ოპერაციულ სისტემაში – კონფიგურაციის ცვლილებების ასახვის შესაძლებლობას. მნიშვნელოვანია, მსგავსი პრივილეგირებული მომხმარებლების რაოდენობა იყოს მაქსიმალურად შეზღუდული. ინფორმაციული უსაფრთხოების მიზნებიდან გამომდინარე აუცილებელია, მხოლოდ ინფორმაციული ტექნოლოგიების (IT) გუნდის კვალიფიციურ წარმომადგენლებს ჰქონდეთ მსგავსი ტიპის პრივილეგიები სისტემაში. შემოწმების შედეგად საჯარო რეესტრის ეროვნულ სააგენტოში აღმოჩნდა სისტემები, რომელთა მომხმარებლებსაც ჰქონდათ ადმინისტრატორის უფლება.[40]

---

[37] როგორც სამსახურის კუთვნილი ლეპტოპები, ასევე სტატიკური კომპიუტერები.

[38] საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტროში შემოწმდა 5 კომპიუტერი; საქართველოს გარემოს დაცვისა და სოფლის მეურნეობის სამინისტროში – 5; სსიპ – საჯარო რეესტრის ეროვნული სააგენტოში – 5.

[39] ფერების განსაზღვრა: მწვანე – დადებითი შედეგი, წითელი – უარყოფითი შედეგი, ნარინჯისფერი – ნაწილობრივ შესრულებული დადებითი შედეგი.

[40] აღნიშნული მომხმარებლები საჯარო რეესტრის საოპერაციო საქმიანობის პროცესში სარგებლობენ სხვადასხვა სპეციფიური არალიცენზირებული პროგრამებით და სამუშაო პროცესის წარმოებისთვის საჭიროებენ ადმინისტრატორის ნებართვას.

რამდენიმე მომხმარებლის არსებობა ერთ მოწყობილობაზე – ერთ კომპიუტერზე ფიქსირდება რამდენიმე მომხმარებელი (user). კრიტერიუმის თანახმად, ინფორმაციული ტექნოლოგიების სპეციალისტის მიერ უნდა ხდებოდეს არასაჭირო პროფილების წაშლა და მხოლოდ იმ პროფილის გააქტიურება, რომელიც ეკუთვნის კომპიუტერულ მოწყობილობაზე პასუხისმგებელ პირს (თანამშრომელს, რომელზეც გადაცემულია კონკრეტული მოწყობილობა). შემოწმების შედეგად აღმოჩნდა, რომ სამივე ობიექტის შემოწმებულ სისტემებში, თანამშრომლის მომხმარებლის გარდა, ფიქსირდება სხვა AD (Active Directory) ან/და ლოკალური მომხმარებელი (ხელით, მექანიკურად შექმნილი სისტემაში).

სამსახურებრივი საქმიანობისათვის არასაჭირო და არასასურველი უცხოური ქვეყნის ინტერნეტრესურსზე წვდომა – უნდა არსებობდეს პოლიტიკა თანამშრომელთა მიერ ინტერნეტრესურსებზე წვდომის რეგულირების მიზნით. როგორც წესი, ორგანიზაციის მიერ იბლოკება ზოგადი სახის არასასურველი ინტერნეტრესურსი. შემოწმებულ ორგანიზაციებში ინტერნეტრესურსზე წვდომის მოთხოვნის პოლიტიკა არ არსებობს. ზოგიერთ თანამშრომელს აქვს წვდომა სამსახურებრივი მიზნებისათვის შეუსაბამო და არასასურველი უცხოური ქვეყნის ინტერნეტრესურსზე. კერძოდ, სოფლის მეურნეობისა და ეკონომიკის სამინისტროებში ხელმისაწვდომია არასასურველი ქვეყნის ინტერნეტრესურსი, ხოლო საჯარო რეესტრის ეროვნულ სააგენტოში არსებობს თანამშრომელთა კატეგორია,[41] რომელთაც ინტერნეტ რესურსზე შეუზღუდავი წვდომა აქვთ (როგორც სამსახურებრივი საქმიანობისათვის არასაჭირო, ასევე არასასურველი უცხოური ქვეყნის ინტერნეტრესურსზე).

ანტივირუსის რეგულარული განახლება და პერიოდული სკანირების კონფიგურაცია – მავნე კოდისაგან საბოლოო მომხმარებელთა დაცვისათვის ერთ-ერთი მნიშვნელოვანი საკითხია ანტივირუსის გამოყენება. აღნიშნული საშუალებას იძლევა, რომ კომპიუტერული მოწყობილობები და ზოგადად მთლიანი IT გარემო, იყოს დაცული. აუცილებელია, რომ მიმდინარეობდეს ანტივირუსის რეგულარული განახლება და მონიტორინგი. გარდა აღნიშნულისა, მნიშვნელოვანია, ანტივირუსი იყოს კონფიგურირებული ორგანიზაციის ინტერესებიდან და მიზნებიდან გამომდინარე, ხდებოდეს გარკვეულ პერიოდში სისტემის მავნე კოდზე სრულად შემოწმება და რეალურ, მიმდინარე დროში მავნე კოდის აღმოჩენა. შემოწმების შედეგად აღმოჩნდა, რომ სამივე ობიექტის კომპიუტერულ მოწყობილობებში მიმდინარეობს რეალურ, მიმდინარე დროში (Real Time) სკანირება, თუმცა არაა განსაზღვრული ანტივირუსის მიერ სრული ავტომატური სკანირების პერიოდი, რაც უწყებებს მისცემდა სისტემის საფუძვლიანად შემოწმების საშუალებას. რაც შეეხება ანტივირუსის ლიცენზიების განახლებას, აუდიტის პერიოდში სოფლის მეურნეობისა და ეკონომიკის სამინისტროები განახლებული ანტივირუსით სარგებლობდნენ, ხოლო საჯარო რეესტრის ეროვნულ სააგენტოში ანტივირუსი დროულად არ განუახლებიათ.[42]

3.1.7 თანამშრომელთა მიერ სამსახურის რესურსებზე წვდომის მხრივ არსებული ნაკლოვანებები

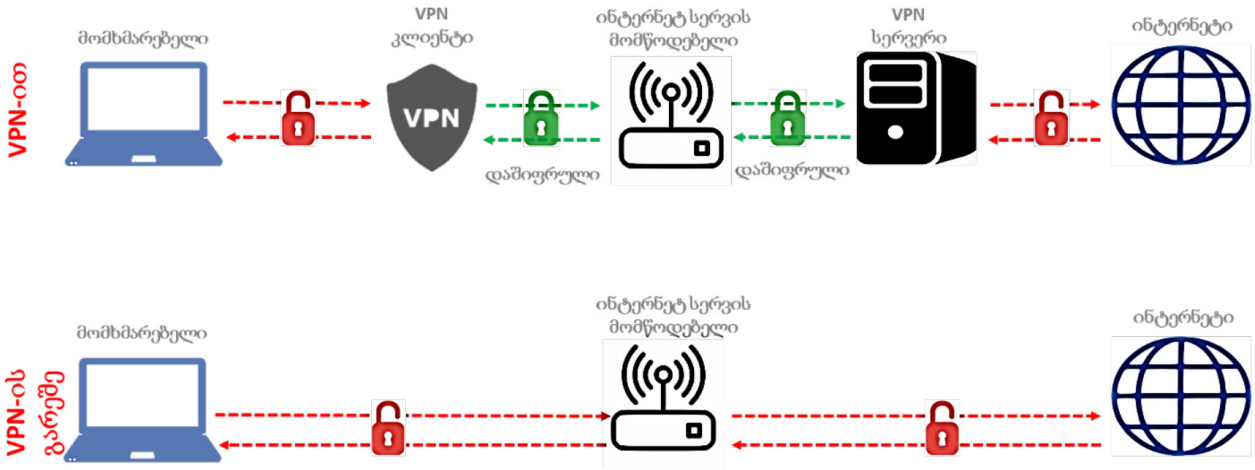
დისტანციური სამუშაო რეჟიმის არსებობასთან ერთად მნიშვნელოვანი გახდა გარე, დაუცველი ქსელიდან უსაფრთხოდ მუშაობის უზრუნველყოფა. პანდემიამდე აუდიტის ობიექტების თანამშრომლებს მუშაობა უწევდათ ადმინისტრაციულ შენობებში და მათი კომპიუტერები უკავშირდებოდა შიდა ორგანიზაციულ ქსელს, რომელიც უზრუნველყოფილია

[41] კონკრეტული ოპერატორები და სპეციალისტები

[42] 2018 წლის 24 დეკემბრის ხელშეკრულებით შეძენილი 3-წლიანი ლიცენზია განახლდა 2022 წლის ივლისში.

დაცვის შესაბამისი მექანიზმებით. დისტანციურად მუშაობის პირობებში კი საჭირო გახდა სამსახურისაგან დამოუკიდებელი/გარე ქსელების გამოყენება, რომლებიც არ კონტროლდება აუდიტის ობიექტის IT სამსახურების მიერ და არ არსებობს შესაბამისი დაცვის მექანიზმები.[43] ასეთ პირობებში უკეთეს პრაქტიკად მიჩნეულია ვირტუალური კერძო ქსელის (VPN) გამოყენება. VPN არის სერვისი, რომელიც მომხმარებელს საშუალებას აძლევს ინტერნეტთან წვდომა ჰქონდეს დაშიფრული გზით.

დიაგრამა №7. VPN სერვისის მუშაობის პრინციპი



აღნიშნული გულისხმობს, რომ ნებისმიერი ტიპის კავშირი ქსელთან არის დაშიფრული და ამ ინფორმაციაზე წვდომა არ აქვს გარე მხარეებს (მათ შორის, ინტერნეტსერვისის მომწოდებლებს). ორგანიზაციის მიერ VPN სერვისის გამოყენების პროცესში ყურადღება უნდა გამახვილდეს შემდეგ საკითხებზე:

- მმართველობა (პოლიტიკა, მომხმარებელთა ცნობიერება);
- გამოყენება და კონფიგურაცია;
- შესაბამისი ოპერაციები (პოლიტიკის აღსრულება, VPN-თან კავშირში არსებული ოპერაციების ცოდნა, მართვა და კონტროლი);
- მოვლა-შენახვა/განახლება და მონიტორინგი.

დისტანციური სამუშაო რეჟიმის პირობებში ორგანიზაციებს გარკვეულ შემთხვევებში მოუხდათ ან VPN-ის დაყენება და მისი გამოყენების დაწყება, ან უკვე არსებულის განახლება. აუდიტის ობიექტებში გამოვლინდა აღნიშნული სერვისის გამოყენებასთან დაკავშირებული ნაკლოვანებები, რომლებიც ასახულია ქვემოთ მოცემულ ცხრილში:

[43] მაგალითად, სახლში თანამშრომელთა მიერ გამოყენებული ინტერნეტკავშირისათვის არსებული ყველა მარშუტიზატორს (router) გააჩნია სტანდარტული მომხმარებელი და პაროლი. აღნიშნულის გამოყენებით მომხმარებელს საშუალება აქვს შეცვალოს საკუთარი ქსელის კონფიგურაცია: დააყენოს პაროლი, განსაზღვროს ქსელის შიფრაცია და სხვ. ხშირ შემთხვევაში სტანდარტული მომხმარებელი არ ცვლის მსგავს პარამეტრებს, რაც ზრდის აღნიშნულ ქსელში ინფორმაციის ხელმისაწვდომობას არასასურველი დაინტერესებული მხარეებისათვის.

ცხრილი №5. VPN სერვისის გამოყენებასთან არსებული ნაკლოვანებები

	ეკონომიკისა და მდგრადი განვითარების სამინისტრო	გარემოს დაცვისა და სოფლის მეურნეობის სამინისტრო	საჯარო რეესტრის ეროვნული სააგენტო
სამუშაო საათებში მუდმივი VPN კავშირი	არ იყო სრული სამუშაო საათების განმავლობაში მოთხოვნილი. VPN-ს იყენებდნენ მხოლოდ სამსახურის რესურსებზე წვდომისათვის	არ იყო სრული სამუშაო საათების განმავლობაში მოთხოვნილი. VPN-ს იყენებდნენ მხოლოდ სამსახურის რესურსებზე წვდომისათვის	არ იყო სრული სამუშაო საათების განმავლობაში მოთხოვნილი. VPN-ს იყენებდნენ მხოლოდ სამსახურის რესურსებზე წვდომისათვის
VPN გადაწყვეტის განახლება	განახლებულია	განახლებულია	არ არის განახლებული (იყენებს მწარმოებლის ძველ ვერსიას)
VPN გადაწყვეტის დროული დანერგვა	დროულად იქნა უზრუნველყოფილი	დროულად იქნა უზრუნველყოფილი	დროულად იქნა უზრუნველყოფილი
ინტერნეტრესურსებზე წვდომისას VPN კავშირის გამოყენება	არ მოითხოვება	არ მოითხოვება	არ მოითხოვება

ზემოაღნიშნულის გათვალისწინებით, აუდიტის ობიექტების მიერ VPN სერვისის გამოყენებისას ფიქსირდება ნაკლოვანებები. კერძოდ, სამსახურის საკუთრებაში არსებულ და თანამშრომლების პირად კომპიუტერზე უზრუნველყოფილ იქნა VPN აპლიკაციების დაყენება, თუმცა VPN აპლიკაციის გამოყენების გარეშე (რომელსაც მომხმარებელი რთავს სურვილის შემთხვევაში) მომხმარებელს შეუძლია ჰქონდეს შეუზღუდავი წვდომა გარე ქსელთან. კერძოდ, VPN კავშირის თანამშრომელი VPN სერვისს იყენებდა მხოლოდ სამსახურის შენობაში არსებულ მასზე განპიროვნებულ სტატიკურ კომპიუტერთან დასაკავშირებლად ან სამსახურის სასერვერო ინფრასტრუქტურაზე განთავსებულ ინფორმაციაზე წვდომისათვის.

ამასთანავე, როგორც ცხრილიდან ჩანს, ნაკლოვანებით მიმდინარეობს პროგრამული უზრუნველყოფის განახლების და შესყიდვის საკითხი.

შედეგად, აუდიტის ობიექტებში არსებული პრაქტიკა ვერ უზრუნველყოფს თანამშრომლების მიერ საქმიანობის განხორციელებისას მონაცემების უსაფრთხოების პრინციპების დაცვით გაცვლას, აღნიშნული კი ზრდის ინფორმაციაზე არასანქცირებული წვდომისა და ინფორმაციული უსაფრთხოების დარღვევის რისკებს.

3.1.8 დასკვნა და რეკომენდაციები

COVID-19 პანდემიამ დღის წესრიგში დააყენა აუდიტის ობიექტების მიერ სამუშაო პროცესების შემჭიდროებულ ვადებში დისტანციურ რეჟიმზე გადაყვანის პროცესი. აუდიტის ფარგლებში შესწავლილმა სახელმწიფო ორგანიზაციებმა რესურსების მობილიზებისა და ინდივიდუალური თანამშრომლების ძალისხმევის ხარჯზე შეძლეს აღნიშნულ გამოწვევასთან გამკლავება და უზრუნველყვეს სამუშაო პროცესის უწყვეტობა.

მიუხედავად ამისა, აღნიშნულმა პროცესმა ხაზი გაუსვა ინფორმაციული სისტემების მმართველობისადმი უკეთესი პრაქტიკით გათვალისწინებული სისტემური მიდგომის მნიშვნელობას.

კერძოდ, ორგანიზაციაში ბიზნესის უწყვეტობისა და კატასტროფისგან აღდგენის გეგმების არსებობა ხელს შეუწყობს სამომავლოდ ფორსმაჟორული შემთხვევების წარმოშობის პირობებში უფრო ეფექტიან და დროულ რეაგირებას წარმოქმნილ საჭიროებებზე, ინფორმაციული აქტივების იდენტიფიცირებისა და კლასიფიცირების გზით მათ ოპტიმალურ განაწილებას ორგანიზაციაში, კრიტიკულად მნიშვნელოვანი ფუნქციების შესანარჩუნებლად.

ასევე, ორგანიზაციული დონის პოლიტიკა/სახელმძღვანელო დოკუმენტები პროგრამების/ლიცენზიების განახლების პერიოდულობის, ინტერნეტ რესურსებზე დისტანციური წვდომისა და თანამშრომელთა პირადი ანგარიშების მართვის შესახებ ხელს შეუწყობს დისტანციურად მუშაობასთან ასოცირებული ინფორმაციული უსაფრთხოების რისკების შემცირებას.

შესაბამისად, აუდიტის ანგარიშში იდინტიფიცირებული ნაკლოვანებებიდან და მიგნებებიდან გამომდინარე, სახელმწიფო აუდიტის სამსახურმა გასცა შემდეგი რეკომენდაციები :

- IT სერვისების უწყვეტობის პროცესის გაუმჯობესების მიზნით:
  - შეიქმნას მმართველობითი სისტემა სათანადო უფლებამოსილების, კვალიფიკაციისა და კომპეტენციის მქონე პერსონალით, რომელიც პასუხისმგებელი იქნება სერვისების უწყვეტობის მართვის პროცესში შესაბამისი აქტივობების დაგეგმვაზე, განხორციელებასა და რეაგირებაზე;
  - გადაიდგას საწყისი ნაბიჯები სერვისის უწყვეტობის გეგმების შესამუშავებლად, რომლებიც ხელს შეუწყობს ორგანიზაციაში კრიტიკული ბიზნესპროცესების განგრძობად მუშაობას;
  - განხორციელდეს რეგულარულად (სულ მცირე – ყოველწლიურად) შეუსაბამობების ანალიზი (gap analysis) IT სერვისების უწყვეტობასთან მიმართებით, რათა განისაზღვროს ორგანიზაციის მიმდინარე და სასურველი მდგომარეობა.

- ინფორმაციული უსაფრთხოების რისკების დასაზღვევად შემუშავდეს პოლიტიკა/პროცედურა, რომლის საშუალებითაც უზრუნველყოფილი იქნება ოპერაციული სისტემებისა და პროგრამული უზრუნველყოფების დროული ლიცენზირება/განახლება.

აუდიტორი

გიორგი მოლაშვილი
ინფორმაციული ტექნოლოგიების უფროსი აუდიტორ-ასისტენტი

ხელმოწერა

სახელმწიფო აუდიტის სამსახური
ქ.თბილისი, 0144, წმ. ქეთევან დედოფლის გამზირი N96
+995 32 243 84 38
SAO.GE