საქართველოს ტექნიკური უნივერსიტეტი

ხათუნა ქორთიაშვილი

რისკების მართვის სისტემა საჯარო სექტორის მაგალითზე პერსონალის მიღება-დაგეგმვის

წარმოდგენილია დოქტორის აკადემიური ხარისხის მოსაპოვებლად

სადოქტორო პროგრამა „ინფორმატიკა“

შიფრი 0401

საქართველოს ტექნიკური უნივერსიტეტი

თბილისი, 0175, საქართველო

2019 წელი

ინფორმატიკისა და მართვის სისტემების ფაკულტეტი

ჩვენ, ქვემორე ხელისმომწერნი ვადასტურებთ, რომ გავეცანით ხათუნა ქორთიაშვილის მიერ შესრულებულ სადოქტორო ნაშრომს დასახელებით: „პერსონალის მიღება–დაგეგმვის რისკების მართვის სისტემა საჯარო სექტორის მაგალითზე “ და ვაძლევთ რეკომენდაციას საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის სადისერტაციო საბჭოში მის განხილვას დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

_____

2019

ხელმძღვანელი: პროფ. გიორგი მაისურაძე

რეცენზენტები: _____

_____

საქართველოს ტექნიკური უნივერსიტეტი
2019

ავტორი: ხათუნა ქორთიაშვილი
დასახელება: პერსონალის მიღება–დაგეგმვის რისკების მართვის სისტემა საჯარო სექტორის მაგალითზე

სადოქტორო პროგრამა „ინფორმატიკა“

ხარისხი: დოქტორი
სხდომა ჩატარდა:

ავტორის ხელმოწერა

ვუძღვნი მამის ხსოვნას

რეზიუმე

სადისერტაციო ნაშრომში განხილულია კადრების შერჩევის საკითხები მსოფლიოში ჩამოყალიბებული მეთოდებისა და მიდგომების საშუალებით. კადრების ეფექტიანი შერჩევის საფუძველია მუშაკზე ობიექტური ინფორმაციის ფლობა.

დისერტაციის კვლევის საგანია ორგანიზაციაში პერსონალის შერჩევის სხვადასხვა მეთოდის გამოყენების შედეგების ანალიზი, მათ შორის ისეთი მეთოდის, როგორიცაა გასაუბრება. გამოკითხვის ობიექტია ადამიანები, რომლებიც გადიან შერჩევას ორგანიზაციაში წარმოქმნილი ვაკანსიის შესავსებად.

სადისერტაციო ნაშრომის ძირითადი მიზანია ახსნას, თუ რა მეთოდების გამოყენებითაა შესაძლებელი ორგანიზაციის წინაშე არსებული ამოცანების გადასაწყვეტად საჭირო პერსონალის ოპტიმალური კონტიგენტის შერჩევის პროცესის ორგანიზების, წარმართვისა და შემდგომი მონიტორინგის უზრუნველყოფა.

პერსონალის კომპლექსური შეფასება შეიძლება განხორიელდეს პიროვნების შესახებ არსებული სხვადასხვა მონაცემის გამოკვლევის საფუძველზე, ობიექტური საკადრო მონაცემების, საქმიანი და მორალური თვისებების, ცხოვრებისეული გამოცდილების, პროფესიული ცოდნისა და უნარების, ჯანმრთელობისა და შრომისუნარიანობის, სამუშაო კარიერისა და სხვა ასპექტების გათვალისწინებით. კონკრეტული ელემენტების გამოყენებით აიგება სამუშაო ადგილებისა და თანამშრომლთა კრებსითი მოდელი, რომლის გამოყენება შემდგომში შესაძლებელია არამარტო საკადრო კომიისიის მუშაობის, არამედ პერსონალის მართვის სხვა პროცესებშიც.

სადისერტაციო ნაშრომში განხილულია პერსონალის შერჩევის მეთოდიკა. კერძოდ აღწერილია, თუ როგორ ეხმარება სოციალური ქსელები კომპანიებსა და კადრების სამსახურებს ვაკანტური ადგილების ან არსებულ კანდიდატებზე დამატებითი ინფორმაციის მოძიებაში.

დისერტაციის პირველ თავში განხილულია საინფორმაციო სისტემებში ცვლილებების მენეჯმენტსა და ინფორმაციულ უსაფრთხიებასთან დაკავშირებული საკითხები. ორგანიზაციაში ცვლილებებზე რეაქცია, მართვის ყველა დონეს ეხება, თუმცა მას აქვს განსხვავებული ხასიათი და განსხვავებული შედეგები.

დისერტაციის მეორე თავში განხილულია ინფორმაციული რისკების მართვის თანამედროვე სისტემები, აუდიტის როლი რისკების ეფექტურად მართვის პროცესში, მომხმარებლის რესურსთან არასანქცირებული შეღწევის კონტროლის მექანიზმები- დაშვების მოდული (მატრიცა). მოცემულია ვირუსებთან ბრძოლის თანამედროვე მეთოდების ანალიზი წამყვანი კომპანია Symantec- ის უსაფრთხოების სოფტის მაგალითზე და რისკების მართვით ორგანიზაციის უსაფრთხო ფუნქციონირების ანალიზის
პროგრამული კომპლექსების აღწერა.

დისერტაციის მესამე თავში გაანალიზებულია რისკმენეჯმენტის თანამედროვე მეთოდები, მათ შორის ინფორმაციული რისკების ანალიზისა და კონტროლის პროგრამული კომპლექს CRAMM–ის ძლიერი და სუსტი მხარეები, ინფორმაციული რისკების მართვისა და კანონმდებლობის მოთხოვნების უზრუნველყოფის ინფორმაციული ტექნოლოგია Compliance - ის ინფრასტრუქტურა და სტრატეგიული დაგეგმვისა და რისკმენეჯმენტის პროცესების ინტეგრაციის საკითხები.

დისერტაციის მეოთხე თავში წარმოდგენილია რეკომენდაციები საჯარო სექტორში პერსონალის შერჩევა-მიღების მეთოდების და ინსტრუქციების დანერგვისა და შემდგომი მონიტორინგის საკითხები.

სადისერტაციო ნაშრომში ჩატარებული კვლევებისა და ანალიზის საფუძველზე გაკეთებულია დასკვნები და წარმოდგენილია კონკრეტული რეკომენდაციები ორგანიზაციაში პერსონალის მიღება-დაგეგმვისა და რისკების მართვის საკითხებში.

Abstract

Dissertation work discusses the selection of personnel through the methods and approaches developed in the world. Effective selection of staff is the objective information on the worker.
The dissertation research is the analysis of the use of different methods of selection of personnel in the organization, including a method such as interview. The survey is the subject of a survey of individuals who are selected to fill the vacancy in the organization.

The main objective of the dissertation work is to explain what methods are used to organize, conduct and further monitor the selection process of optimal contingency of personnel to solve the tasks before the organization.
Complex assessment of the personnel may be based on the examination of various data about personality, objective personnel data, business and moral qualities, life experiences, professional knowledge and skills, health and workability, working career and other aspects. Using concrete elements is a compilation model of workplaces and employees that can be used not only in the work of the staff of the staff but also in other personnel management processes.
The Dissertation Thesis is reviewed by the selection of personnel. Specifically describes how social networks help companies and staff to find more information on vacant seats or existing candidates.
The first chapter of the dissertation deals with issues related to change management and information security in information systems. The reaction to changes in the organization concerns all levels of management, but it has a different character and different results.
The second chapter of the dissertation deals with modern systems of information risk management, the role of audit in the efficient management of risks, control mechanisms for unauthorized access to the user's resource- module (access to the module). Analysis of the modern methods of fighting viruses is given by the leading company Symantec's safety system and the risk management of the organization's safe functioning analysis
Description of software complexes
The third chapter of the thesis analyzes riskmenejmentis modern methods, including information risk analysis and control of complex software CRAMM-'s strengths and weaknesses, and information risk management requirements of providing Information Technology Compliance - the infrastructure and the strategic planning process and riskmenejmentis s integration issues.
The fourth chapter of the dissertation presents the recommendations on the implementation and implementation of the methods and instructions for selection and adoption of personnel in the public sector.
Conclusions have been made based on the research and analysis conducted in the dissertation work and concrete recommendations are presented in the organization in planning and risk management.

შინაარსი

ნახაზების ნუსხა

გამოყენებული აბრევიატურა

IT – ინფორმაციული ტექნოლოგიები

სს – საინფორმაციო სისტემა

იუ – ინფორმაციული უსაფრთხოება

მდმ – მოთხოვნების დამუშავების მონიტორი

იუუს – ინფორმაციული უსაფრთხოების უზრუნველყოფის სისტემა

აის – ავტომატიზებული ინფორმაციული სისტემა

პკ – პერსონალური კომპიუტერი

ოპს – ოპერაციული სისტემა

პუ – პროგრამული უზრუნველყოფა

ასს – ავტომატიზებული საინფორმაციო სისტემა

შესავალი

თანამედროვე ეპოქაში ინფორმაცია ერთერთი ყველაზე ძვირადღირებული და მოთხოვნადი რესურსია. აუარებელი საინფორმაციო ნაკადების მართვა და ანალიზი კი ელექტრონული საინფორმაციო სისტემების გარეშე შეუძლებელია.

ინტერნეტქსელის გაჩენამ მსოფლიოში თამაშის ახალი წესები დაამკვიდრა, ყველაფერი რასაც ვაკეთებთ, თანდათან უფრო და უფრო დამოკიდებული ხდება ინტერნეტზე.

XXI საუკუნეში, არ არსებობს საქმიანობა, სადაც მინიმალური დოზით მაინც არ გამოიყენება ინფორმაციის გაცვლისა, თუ შეგროვების ელექტრონული მეთოდები. ელექტრონული ფოსტა, ელექტრონული საცავები რამდენიმე წლის წინ იშვიათობას წარმოადგენდა, დღეს კი, ორგანიზაციისა თუ ცალკეული ინდივიდის მათ გარეშე შეუფერხებელი ფუნქციონირება შეუძლებელია.

დღეისათვის, საინფორმაციო ტექნოლოგიების განვითარება განსაკუთრებული დაჩქარებული ტემპებით მიმდინარეობს. ერთი, რომელიმე სფეროს პროგრესი თავისთავად მოითხოვს და ამავდროულად ასტიმულირებს მომიჯნავე ტექნოლოგიების წინსვლას. ამის მაგალითად შეგვიძლია განვიხილოთ ქსელური ინფრასტრუქტურის მნიშვნელოვანი წინსვლა-წარმადობის ზრდა, რომელიც მსხვილი ფაილსერვერების შექმნამ დააჩქარა. საჭირო გახდა დიდი მოცულობის საინფორმაციო ნაკადების გატარება, რაც ახალი მიდგომების გარეშე წარმოუდგენელი იქნებოდა.

საინფორმაციო ნაკადების ელექტრონულ სივრცეში გადანაცვლებასთან ერთად იზრდება ხელმისაწვდომობა. შესაბამისად მატულობს ინფორმაციაზე არაავტორიზებული წვდომის საფრთხე. გამოთვლილია, რომ მსოფლიოს მაშტაბით მხოლოდ ელექტრონული კომერცია წელიწადში 8 ტრილიონ დოლარს აღწევს. შესაბამისად ინფორმაციის ხელმისაწდომობის ზრდასთან ერთად XXI საუკუნის ინფორმაციული სისტემები დადგა ახალი გამოწვევის წინაშე – ერთის მხრივ მაქსიმალურად წვდომადი სისტემები უნდა გახდეს მაქსიმალურად დაცული. აღნიშნული საკითხი მრავალი სირთულესთანაა დაკავშირებული და ფიზიკურის გარდა ვირტუალურ დაცვასაც აერთიანებს. ამისათვის იქმნება შიფრაციის ახალი მექანიზმები, მუშავდება ავტორიზაციის განსხვავებული მეთოდები, თუმცა დაცვის მექანიზმების განვითარების პარალელურად იზრდება კიბერდანაშაული, საიდანაც მიღებული ზარალის ოდენობა წლიდან წლამდე იზრდება. ახალი გამოწვევები მსოფლიოს აიძულებს მნიშვნელოვნად დახვეწოს ინფორმაციული სისტემების მართვის მიდგომები. თანამედროვე ეპოქაში, არა მხოლოდ კერძო ბიზნესის, არამედ სახელმწიფო დონეზე ხდება უსაფრთხოების პოლიტიკის შემუშავება და

განვითარება. ეროვნული უსაფრთხოება უკვე თავად გახდა დამოკიდებული ელექტრონულ რესურსებზე, რამაც სამთავრობო და საკანონმდებლო დონეზესახელმწიფოს გააქტიურება გამოიწვია. როგორც წესი, ინფორმაციული უსაფრთხოების ეროვნული პოლიტიკა მოიცავს მხოლოდ სტრატეგიული მონაცემების სფეროს და არ იჭრება კერძო საწარმოთა კომპეტენციაში. კომპანიებს უკვე თავად უწევთ იზრუნოს საკუთარი ინფორმაციის დაცულობაზე.

ქსელური ინფრასტრუქტურის განვითარებამ, მნიშვნელოვნად შეცვალა მენეჯმენტის და ზოგადად ორგანიზაციების მუშაობის სტილი. გაზრდილი ტრაფიკის გატარების შესაძლებლობამ გააიოლა მოშორებული ოფისების კავშირი. თანამშრომლებს გაუჩნდათ შესაძლებლობა, სახლიდან გაუსვლელად ჩართულიყვნენ სამსახურებრივ ქსელში და შეესრულებინათ დაკისრებული სამუშაო (VPN-ის მეშვეობით). ასევე, კომპანიის წინაშე აღარ იდგა საკუთარი Data Center-ის ოფისშივე ქონის აუცულებლობა, მონაცემების გადატანა ერთი წერტილიდან მეორემდე პრობლემას აღარ წარმოადგენდა. აღნიშნულმა მოვლენამ ასევე დააჩქარა „აუთსორსინგის“ განვითარება ქართული საინფორმაციო სისტემების ბაზარზე - გაჩნდნენ კომპანიები, რომლებიც უშუალოდ IT მომსახურებაზე იყვნენ დასპეციალიზებული. ამ ფაქტმა ბიზნესს სისტემების საექსპულატაციო ხარჯების შემცირების საშუალება მისცა.

საინფორმაციო ნაკადების ზრდასთან ერთად რთულდება საინფორმაციო სისტემების მართვა. საჭირო ხდება ხარჯების ოპტიმიზაცია, შრომის ეფექტურობის ამაღლება და დროის მენეჯმენტის ხარისხის ზრდა. გლობალიზაციის ზრდა ასევე თავის მოთხოვნებს უყენებს სისტემებსაც, აქტუალური ხდება მობილურობა - მომხმარებლებს სურთ წვდომის უზრუნველყოფა მსოფლიოს ნებისმიერი წერტილიდან. სისტემის გახსნილობა და უსაფრთხოება მაქსიმალურად უნდა იყოს დაბალანსებული. გამომდინარე. აქედან, დგება ახალი გამოწვევები, რომლებიც საინფორმაციო სისტემების მენეჯერებს კრეატიული აზროვნებისკენ უბიძგებს.

დღევანდელ რეალობაში ორგანიზაციაში კადრების შერჩევისა და ვაკანსიების შევსების პროცესების ორგანიზებისა და მართვის საკითხები, ინფორმაციულ ტექნოლოგიებზე დაფუნებული მეთოდებისა და მიდგომების მეშვეობით ხორციელდება.

სადისერტაციო ნაშრომის ძირითადი მიზანია პერსონალის მიღება-დაგეგმვის ამოცანების გადაწყვეტისას, შეიმუშაოს რისკების მართვის ისეთი სისტემა, რომელიც სხვა მნიშვნელოვან ფაქტორებთან ერთად, გაითვალისწინებს პროცესის ინფორმაციულ უსაფრთხოებას.

დისერტაციის ფარგლებში ფართოდ არის გაშუქებული მუშაკზე ობიექტური და დაცული ინფორმაციის მოპოვების, გადამუშავებისა და შენახვის საკითხები, რაც ძალზედ აქტუალური და მნიშვნელოვანი საკითხებია, როგორც კადრების ოპტიმალური შერჩევის, ასევე მისი ეფექტიანი მართვის პროცესში.

დისერტაციის კვლევის ძირითადი საგანია ორგანიზაციაში პერსონალის მიღება-დაგეგმვის პროცესში გასაუბრება- გამოკითხვის მეთოდის გამოყენების შედეგების ანალიზი.

დისერტაციის კვლევის ძირითადი ობიექტია საჯარო სექტორში მოხელეთა დასაქმებასთან დაკავშირებული საკითხები.

ნაშრომში განხილულია საჯარო სექტორში პერსონალის შერჩევის, ვაკანსიების შევსების, თანამშრომელთა დასჯისა და განთავისუფლების, წახალისებისა და პრემირების, კონკურსების ორგანიზებისა და მართვის საკანონმდებლო დოკუმენტები, მითითებები და სხვა ნორმატიული აქტები.

ნებისმიერი ორგანიზაცია, განსაკუთრებით კი სახელმწიფო დაწესებულება, სამუშაო პროცესების საწარმოებლად, საჭიროებს საკუთარი აქტივების, მათ შორის ადამიანური რესურსების მოცემთა ბაზების არსებობას, რომლის ეფექტიანი მართვისთვის აუცილებელია, რომ ის იყოს რეალური, მარტივად სამართავი, ადვილად განახლებადი, შეიძლებოდეს მისი უწყვეტი და კომპლექსური კონტროლი და უზრუნველყოფილი იყოს მისი ინფორმაციული უსაფრთხოება.

სადისერტაციო ნაშრომში, პერსონალის ანკეტირების მონაცემთა ბაზების შექმნის, ინფორმაციული უსაფრთხოების უზრუნველყოფისა და რისკების მართვის სისტემების ფორმირებისთვის გამოყენებულია პროგრამული ენა ექსელი, რომელიც შედარებით მარტივი და , ადვილად აღქმადი საშუალებაა, თუმცა მისი შესაძლებლობები სრულიად საკმარისია დისერტაციის ფარგლებში დასახული ამოცანების ეფექტიანი გადაწყვეტისთვის.

დისერტაციაში პერსონალის შერჩევისთვის განხილულია სამი ძირითადი ხერხი:

- პირველი ხერხით, ორგანიზაციის კონკრეტული ნიშანთვისებებისა და ქვედანაყოფების ფუნქციონალობის გათვალისწინებით, წამოქმნილი პრობლემებისა და ამოცანების გადასაწყეტად, შიდა კონტიგენტიდან შეირჩევიან ის თანამშრომლები, რომლებსაც შეუძლიათ არსებული პრობლემების ეფექტიანი გადაწყვეტა. ამ შემთხვევაში, ვაკანსიების შევსება, ხორციელდება თვისობრივი მეთოდების გამოყენებით, ხელმძღვანელის ან კადრების სამსახურის წარმომადგენლის მიერ, პირადი შეფასებით თანამშრომლის საქმიანი და პროფესიული თვისებების საფუძველზე. აღნიშნული მეთოდის ნაკლოვანება არის ის, რომ ამ შემთხვევში, გარკვეულწილად, იზღუდება თანამშრომლის კარიერული განვითარება, ვინაიდან მას მოუწევს შემოიფარგლოს რაიმე კონკრეტული სამუშაო პოზიციით მკაფიო პერსპექტივის გარეშე.
- მეორე ხერხით, შერჩევა წარმოებს პროფესიული მომზადების მიხედვით, თანამშრომლის სამუშაო გამოცდილებისა და თვისებების გათვალისწინებით. ამ მეთოდის ნაკლოვანება არის ის, რომ ვაკანსიის გამოცდილი თანამშრომლით შევსების შემდეგ, იკარგება ადგილი შეიძლება უფრო ნიჭიერი და შრომისმოყვარე, მაგრამ ნაკლებად გამოცდილი პერსონალისთვის.
- მესამე ხერხის გამოყენებისას ხდება პირველი და მეორე მეთოდის გაერთიანება, რომლის დროსაც, მაღალკვალიფიციური და გამოცდილი კადრებისთვის ადგილის შერჩევა ხორციელდება არსებული ფუნქციების განაწილების ცვლილებების საშუალებით, ხოლო დარჩენილი ვაკანსიის შევსება ხდება სამუშაო ადგილების ნორმატიული მოთხოვნების გათვალისწინებით.

პერსონალის შერჩევის ყოველ აღნიშნულ შემთხვევაში, სწორი შერჩევის საფუძველს წარმოადგენს მუშაკზე და სამუშაო ადგილზე ობიექტური ინფორმაციის ფლობა. ამ შემთხვევაში, გააზრებულად მოხდება მათი შესაბამისობის ანალიზი. პერსონალის კომპლექსური შეფასება უნდა განხორიელდეს პიროვნების შესახებ არსებული სხვადასხვა მონაცემის გამოკვლევის გათვალისწინებით კერძოდ:

- ობიექტური საკადრო მონაცემები
- საქმიანი და მორალური თვისებები

- ცხოვრებისეული გამოცდილება
- პროფესიული ცოდნა და უნარების
- ჯანმრთელობა
- შრომისუნარიანობა
- სამუშაო კარიერა და სხვ.

ამ კონკრეტული ელემენტების გამოყენებით აიგება სამუშაო ადგილებისა და თანამშრომლების კრებსითი მოდელი, რომელიც შემდგომში შესაძლებელია გამოყენებულ იქნას საკადრო კომიისიის მუშაობისა და პერსონალის მართვის შემდგომ პროცესებში. ვაკანტურ სამუშაო ადგილებზე შესაბამისი კანდიდატურის შერჩევის პროცესში აუცილებელია გათვალისწინებულ იქნას შრომით ბირჟაზე არსებული კადრების რეზერვის ნუსხა.

კადრების პროფესიონალური შერჩევა წარმოადგენს ერთ-ერთ ყველაზე მნიშვნელოვან პროცესს და შეიცავს შემდეგ ეტაპებს:

1. საკადრო კომისიის შექმნა;
2. სამუშაო ადგილების მიმართ მოთხოვნების ფორმირება;
3. მასობრივი ინფორმაციის საშუალებებში კონკურსის გამოცხადება
4. ;კანდიდატების ფსიქოლოგიური გამოკვლევა;
5. კანდატების გატაცებისა და მავნე ჩვევების ანალიზი;
6. კანდიდატების შეფასება რეიტინგის მიხედვით და სიის საბოლოო ფორმირება;
7. საკადრო კომისიის დასკვნა კანდიდატურის ვაკანტურ პოზიციაზე შერჩევასთან დაკავშირებით;

სადისერტაციო ნაშრომში განხილულია პერსონალის შერჩევის მეთოდიკა. კერძოდ აღწერილია, თუ როგორ ეხმარება სოციალური ქსელები კომპანიებსა და კადრების სამსახურებს ვაკანტური ადგილების ან არსებულ კანდიდატებზე დამატებითი ინფორმაციის მოძიებაში.

დაწესებულება მუდმივად უნდა ზრუნავდეს კადრების გეგმიური და არაგეგმიური დენადობით გამოწვეული დეფიციტის დასაფარად. აღნიშნული პრობლემების გადაწყვეტისათვის დაწესებულების ადამიანური რესურსების მართვის ქვედანაყოფი მუდმივად უნდა იყოს საქმის კურსში ქვეყნის შრომითი რესურსების ბაზარზე არსებული მდგომარეობის შესახებ. გარდა ამისა,

ახალგაზრდა კადრების მოზიდვის მიზნით, ქვედანაყოფის ერთ-ერთ თანამშრომელს მუდმივი კავშირი უნდა ჰქონდეს უმაღლეს სასწავლებლებთან, რომელიც შესაბამისი კვალიფიკაციის სპეციალისტებს ამზადებს. მას, აგრეთვე, უნდა ჰქონდეს ინფორმაცია დაწესებულებისათვის საჭირო სფეროში კვალიფიკაციის ამაღლების შესახებ. განსაკუთრებით ეს ეხება პირებს, რომლებმაც საზღვარგარეთ მიიღეს ცოდნა და გამოცდილება.

უკანასკნელ წლებში დამკვიდრდა უმაღლესი სასწავლებლის დამამთავრებელი კურსის სტუდენტებისა და კურსდამთავრებულთათვის სახელმწიფო დაწესებულებებში სასწავლო პრაქტიკისა და სტაჟირების მოწყობა. ესეც საჯარო სამსახურში ახალგაზრდა პერსპექტიული სპეციალისტების მოზიდვის ერთ-ერთ გზას წარმოადგენს. მიზანშეწონილია, დაწესებულებას ჰქონდეს ოფიციალური ხელშეკრულება შესაბამის უმაღლეს სასწავლებლებთან სტუდენტების სასწავლო პრაქტიკისა და სტაჟირების მოწყობის შესახებ.

ვაკანტურ თანამდებობაზე თანამშრომლის მიღების დაგეგმვისას, ამ პროცესზე პასუხისმგებელი მენეჯერი უნდა დარწმუნდეს, რომ ვაკანტური თანამდებობის აღწერა, განსაკუთრებით საკვალიფიკაციო მოთხოვნები, ზუსტად შეესაბამება არსებულ მოთხოვნებს. საჭიროების შემთხვევაში თანამდებობის აღწერაში შეტანილი უნდა იქნეს სათანადო ცვლილებები. შემდეგ მენეჯერმა უნდა განიხილონ და გაესაუბრონ ყველა თანამშრომელს, ვისაც შესაძლებელია ჰქონდეს ამ თანამდებობის დაკავების სურვილი და, ამავე დროს, აკმაყოფილებს ვაკანტური თანამდებობის მიმართ წაყენებულ მოთხოვნებს, რადგან ზოგჯერ მიზანშეწონილია შიდა რესურსის გამოყენება. ეს განსაკუთრებით მნიშვნელოვანია იმ შემთხვევაში, როდესაც დაგეგმილია შტატების შემცირება.

არსებული კანონმდებლობის თანახმად საჯარო მოსამსახურეების სამსახურში მიღება ძირითადად კონკურსის შედეგად შერჩევის საფუძველზე ხდება. კონკურსს ატარებს დაწესებულების საკონკურსო-საატესტაციო კომისია. კონკურსის ჩატარების ზოგადი წესი და პირობები განსაზღვრულია „საჯარო სამსახურის შესახებ“ საქართველოს კანონის 29-36[4]-ე მუხლებით და საქართველოს პრეზიდენტის 2009 წლის 5 თებერვლის #46 ბრძანებულებით „საჯარო თანამდებობათა დასაკავებელი კონკურსის ჩატარების წესის

დამტკიცების შესახებ“ დამტკიცებულ წესით. საჯარო სამსახურის თითოეულ დაწესებულებას თავისი სპეციფიკის გათვალისწინებით დამტკიცებული უნდა ჰქონდეს საკონკურსო-საატესტაციო კომისიის დებულება და კონკურსისა და ატესტაციის ჩატარების პირობები. ამ დოკუმენტის შესაბამისად შესაძლებელია ცალკეული კონკურსის ჩატარების წინ დაწესებულების ხელმძღვანელის ბრძანებით ან საკონკურსო-საატესტაციო კომისიის გადაწყვეტილებით განისაზღვროს ამ კონკრეტულიკონკურსის მოწყობის პირობები, რომელიც, ბუნებრივია, არ უნდა ეწინააღმდეგებოდეს არც ერთ ზემოაღნიშნულ დოკუმენტს.

რაც შეეხება საკონკურსო-საატესტაციო კომისიას. „საჯარო სამსახურის შესახებ“ საქართველოს კანონის 36^2-ე მუხლის პირველი პუნქტის თანახმად, ადგილობრივი თვითმმართველობის ორგანოს გარდა, კომისიის თავმჯდომარეს ნიშნავს საჯარო სამსახურის ბიუროს უფროსი. იგივე მუხლის მე-2 პუნქტის თანახმად, თავმჯდომარედ, როგორც წესი, ინიშნება დაწესებულების ხელმძღვანელი ან მისი მოადგილე. იგივე კანონის 36^3-ე მუხლის პირველი პუნქტის თანახმად კომისიის წევრთა რაოდენობასა და შემადგენლობას განსაზღვრავს კომისიის თავმჯდომარე. კომისიის თავმჯდომარე და ხშირად წევრების ძირითადი ნაწილიც ორგანიზაციის ხელმძღვანელი მუშაკები არიან. ბუნებრივია, მათი დრო შეზღუდულია და თავის ძირითად საქმიანობასთან ერთად უჭირთ მაქსიმალურად ჩაერთონ კონკურსის მოწყობის პროცესში, რამაც შესაძლოა ნეგატიური გავლენა იქონიოს კონკურსის პროცესზე. ეს გარემოება გათვალისწინებული უნდა იყოს კომისიის შემადგენლობის შერჩევის დროს. რეკომენდებულია კომისია შედგებოდეს 5-7 წევრისგან და მის შემადგენლობაში აუცილებლად იყოს კონკურსის პირობებით გათვალისწინებული პროცედურების ჩატარების სპეციალისტი. კარგი იქნება, თუ იგი წინასწარ მოამზადებს კომისიის წევრებს კონკურსის მოწყობის სპეციფიკურ საკითხებში. აუცილებლობის შემთხვევაში კომისიამ შესაძლებელია თავის სხდომაზე მოიწვიოს პირი, რომელიც დაეხმარება მას ობიექტური გადაწყვეტილების მიღებაში. თუ ამის საჭიროება არსებობს, შესაძლებელია შეიქმნას კომისიის სპეციალიზებული შემადგენლობა, როგორც ეს გათვალისწინებულია „საჯარო სამსახურის შესახებ“ საქართველოს

კანონის 36^1-ე მუხლის მე-3 პუნქტსა და 36^2-ე მუხლის მე-4 პუნქტში. კომპეტენციებზე ორიენტირებული გასაუბრების ჩატარების ინსტრუქცია.

ვაკანტური პოზიციების ძირითადი კომპეტენციების ნუსხის შედგენისას განისაზღვროს, მოცემული კომპეტენციებიდან, იმ სამუშაოებისთვის, რომელსაც ახალი თანამშრომელი უნდა მოერგოს, რომელია ,ყველაზე რელევანტური და მნიშვნელოვანი. ამის გაკეთება/ შემოწმება შესაძლებელია სამუშაოს ანალიზის საფუძველზე. ანალიზის შედეგად განისაზღვრება ძირითადი კომპეტენციები, რომელთა მიხედვითაც უნდა მოხდეს საუკეთესო კანდიდატის შერჩევა. სამუშაოთა უმრავლესობისთვის საკმარისია ქვემოთ მოყვანილი კომპეტენციებიდან ექვსამდე კომპეტენციის შერჩევა:

1. გადაწყვეტილების მიღება და მოქმედების ინიცირება.
2. მართვა და ზედამხედველობა.
3. ადამიანებთან მუშაობა.
4. პრინციპებისა და ღირებულებების დაცვა.
5. ურთიერთობების დამყარება და კონტაქტების მართვა.
6. სხვათა დარწმუნება და გეგავლენა.
7. ინფორმაციის წარდგენა და გადაცემა.
8. წერა და ანგარიშგება.
9. ტექნიკური საშუალებების გამოყენება.
10. კრიტიკული და ანალიტიკური აზროვნება.
11. სწავლა და კვლევა.
12. შემოქმედებითობა და ინოვაცია.
13. სტრატეგიებისა და კონცეფციების შემუშავება.
14. დაგეგმვა და ორგანიზება.
15. შედეგების მიღწევა.
16. ინსტრუქციებისა და პროცედურების დაცვა.
17. ადაპტაცია და ცვლილებებზე რეაგირება.
18. გეწოლის მიმართ მდგრადობა.

19. სამუშაო მიზნების მიღწევაზე ორიენტაცია.

სადისერტაციო ნაშრომში აღწერილია ინფორმაციულ ტექნოლოგიებთან დაკავშირებული რისკების მართვის მეთოდოლოგიის ძირითადი პრინციპები და მექანიზმები, შეფასებულია საფრთხეები და მათთან ბრძოლის ხერხები თავისი დადებითი და უარყოფით მხარეებით.

დისერტაციის პირველ თავში განხილულია საინფორმაციო სისტემებში ცვლილებების მენეჯმენტსა და ინფორმაციულ უსაფრთხიებასთან დაკავშირებული საკითხები. ორგანიზაციაში ცვლილებებზე რეაქცია, მართვის ყველა დონეს ეხება, თუმცა მას აქვს განსხვავებული ხასიათი და განსხვავებულია ცვლილებების შედეგებიც. მაგალითად, თუ რომელიმე კომპანიის უმაღლესი დონის ხელმძღვანელობა გადაწყვეტს მოდერნიზაციას, საშუალო დონის მენეჯერები და სპეციალისტები ამზადებენ ინფორმაციას გასატარებელ ღონისძიებებზე და მოსალოდნელი ხარჯების ალტერნატიულ ვარიანტებზე. ძირეული დონის მენეჯერები პასუხს აგებენ დასახული ღონისძიების პრაქტიკულ რეალიზაციაზე. მუშებიც უნდა გაერკვნენ ცვლილებების არსში, რომ შეძლონ ახალი მოთხოვნილებების შესაბამისად მუშაობა და ხარისხიანი პროდუქციის წარმოება.

დისერტაციის მეორე თავში განხილულია ინფორმაციული რისკების მართვის თანამედროვე სისტემები, აუდიტის როლი რისკების ეფექტურად მართვის პროცესში, მომხმარებლის რესურსთან არასანქცირებული შეღწევის კონტროლის მექანიზმები– დაშვების მოდული (მატრიცა). მოცემულია ვირუსებთან ბრძოლის თანამედროვე მეთოდების ანალიზი წამყვანი კომპანია Symantec– ის უსაფრთხოების სოფტის მაგალითზე და რისკების მართვით ორგანიზაციის უსაფრთხო ფუნქციონირების ანალიზის
პროგრამული კომპლექსების აღწერა.

დისერტაციის მესამე თავში გააანილიზებულია რისკმენეჯმენტის თანამედროვე მეთოდები, მათ შორის ინფორმაციული რისკების ანალიზისა და კონტროლის პროგრამული კომპლექს CRAMM–ის ძლიერი და სუსტი მხარეები, ინფორმაციული რისკების მართვისა და კანონმდებლობის მოთხოვნების უზრუნველყოფის ინფორმაციული ტექნოლოგია Compliance – ის ინფრასტრუქტურა და სტრატეგიული დაგეგმვისა და რისკმენეჯმენტის პროცესების ინტეგრაციის საკითხები.

დისერტაციის მეოთხე თავში წარმოდგენილია რეკომენდაციები საჯარო სექტორში პერსონალის შერჩევა-მიღების მეთოდებისა და ინსტრუქციების დანერგვისა და შემდგომი მონიტორინგის საკითხები.

სადისერტაციო ნაშრომში ჩატარებული კვლევებისა და ანალიზის საფუძველზე გაკეთებულია დასკვნები და წარმოდგენილია კონკრეტული რეკომენდაციები ორგანიზაციაში პერსონალის მიღება-დაგეგმვისა და რისკების მართვის საკითხებში.

.

\

თავი 1. საინფორმაციო სისტემების როლი ტექნოლოგიურ პროგრესში

1.1.საინფორმაციო სისტემების ეფექტიანობის ამაღლების გზები

მსოფლიოში არსებული პრაქტიკის მიხედვით, აუცილებელია პრობლემის წარმოშობისთანავე მოხდეს მისი მონიტორინგი და შესაბამისად დოკუმენტური აღრიცხვა. ზუსტად უნდა გაიწეროს პრობლემის არსი და მისი გადაჭრის გზა, რომელსაც გაივლის სრულ აღმოფხვრამდე. პრობლემის გადაჭრა რამდენიმე ეტაპად იყოფა: პრობლემის იდენტიფიკაცია (აუცილებელია იყოს დროული), შესწავლა და აღმოფხვრა. სწორად შედგენილი აღწერილობისა და გეგმის გამოყენების შემთხვევაში, ჩვენ თავიდან ვიცილებთ ხელახალი შესწავლის ეტაპს და პირდაპირ, არსებული ჩანაწერის მიხედვით, ხარვეზის აღმოფხვრაზე გადავდივართ, რაც მნიშვნელოვნად ამცირებს დროით დანახარჯებს და შესაბამისად ზრდის ეფექტურობას. საქართველოში აღნიშნულ საკითხს სათანადო ყურადღება იშვიათად ექცევა. როგორც წესი, პრობლემაზე მუშაობა ხდება სპონტანურად, ყოველგვარი გეგმისა და წინასწარი ჩანაწერის გარეშე, არ ხდება მისი აღრიცხვა, რაც ინციდენტის განმეორების შემთხვევაში პრობლემის ხელახალი შესწავლისა და მოგვარების გზების ძიების საჭიროებას ქმნის. მსგავსი

მიდგომა პრობლემებისადმი, როგორც წესი მცირე ორგანიზაციებში გვხვდება, სადაც IT დეპარტამენტი, ერთ ან რამდენიმე ინდივიდის პირად ინიციატივაზეა აგებული, რაც შეეხება მსხვილ დაწესებულებებს, აქ საინფორმაციო ტექნოლოგიების განყოფილების სტრუქტურა ბევრად რთული და სრულყოფილია. არსებობს წინასწარ გაწერილი „პოლიტიკა“ რომლის მიხედვითაც უნდა იმოქმედოს თითოეულმა თანამშრომელმა და რომელიც პერსონალს პირადპირ ავალდებულებს დოკუმენტაციის შედგენას. მაგალითად, საქართველოს ეროვნულმა ბანკმა დანერგა ცენტრალიზებული სისტემა, რომელშიც ნაბიჯ-ნაბიჯ აღირიცხება თითოეული პრობლემის გადაჭრის მცდელობები და შედეგი.

საქართველოში. კომუნიკაციის პრობლემა შეიძლება წარმოვიდგინოთ ორი სახის: კომუნიკაცია, როგორც ტექნიკურად კავშირის დამყარების საშუალება (ტელეფონი, ელ. ფოსტა...) და კომუნიკაცია, როგორც ადამიანური ურთიერთობა. პრობლემა არსებობს ორივე მიმართულებით. ხშირად აქვს ადგილი ბიზნესის მხრიდან ვადების არასწორ განსაზღვრას, ხშირად,დასანერგად/პრობლემაზე რეაგირებისთვის, საინფორმაციო ტექნოლოგიების განყოფილებას უწესდება იმაზე მცირე პერიოდი, ვიდრე მას სინამდვილეში ჭირდება. საკითხისადმი მსგავსი დამოკიდებულება იწვევს ხარისხის შემცირებას და მომდევნო ხარვეზებს. ამ პრობლემაში მნიშვნელოვან როლს თამაშობს კომუნიკაციის გზების არასწორი განსაზღვრა. მაგალითად, უცხოეთში აპრობირებულია ე. წ. Help Desk-ის სისტემა. როდესაც მომხმარებელს ექმნება პრობლემა, იგი (უმეტესად გამოიყენება Web-Client) უკავშირდება ბაზას და ხსნის ე.წ. ქეისს, ახდენს პრობლემის ასახვას და სპეციალისტისგან ელოდება გამოხმაურებას. მას ასევე შეუძლია დაუკავშირდეს ოპეარტორს და სატელეფონო ზარის მეშვეობით აცნობოს ხარვეზის შესახებ, მაგრამ ვერანაირ გავლენას ვერ მოახდენს პრობლემის გადაწყვეტის ვადაზე ან მექანიზმზე. ადმინისტრატორი მუშაობს საკუთარი გრაფიკით და განსაზღვრული პრიორიტეტებით. იგი ახდენს პრობლემის სრულყოფილ ანალიზს და დამუშავებას. როდესაც მოიძებნება გამოსავალი, IT სპეციალისტი დაუყოვნებლივ ასახავს მას არსებულ Case-ში. დიალოგი ელექტრონული სახით გაგრძელდება პრობლემის სრულ აღმოფხვრამდე. აღნიშნული მიდგომა საკითხისადმი ეფექტურია რამდენიმე მიზეზის გამო: საინფორმაციო ტექნოლოგიების განყოფილებას აქვს თავისუფლება პრობლემაზე მუშაობისას და არ ხდება მასზე ფსიქოლოგიური გეწოლა, ამასთანავე

ავტომატურად ინახება უკვე არსებული პრობლემების ბაზა და ხარვეზის განმეორების შემთხვევაში უკვე არსებობს გადაწყვეტის მექანიზმი. Help Desk როგორც წესი, არც მომხმარებელს ტოვებს უკმაყოფილოს, იგი პრობლემის გადაწყვეტის პროცესს აფასებს სხვადასხვა კრიტერიუმით (გამოსავლის მოძებნის დროულობით, კვალიფიციური პასუხის მიხედვით და ა.შ), შედეგად საინფორმაციო განყოფილება აანალიზებს დაგროვილ შეფასებებს, ხედავს საკუთარ სუსტ წერტილებს და მუშაობს მის გამოსწორებაზე.

საინფორმაციო ტექნოლოგიებში, აუცილებელია ეფექტიანობის მუდმივი ზრდა. დროსთან ერთად იზრდება ინფორმაციის რაოდენობა, მატულობს სისტემების სირთულე, პრობლემები და შესაბამისად ძალისხმევა, რომელიც გამოწვევებზე სათანადო რეაგირებისათვისაა საჭირო. აუცილებელი ხდება საკითხების ობიექტური შეფასება და ახლებურად დანახვა, რაც მაქსიმალურად გაზრდის პერსონალის შრომის ნაყოფიერებას.

ერთერთი მთავარი ბერკეტი, პრობლემის აღმოფხვრის ეფექტიანობის ზრდისათვის არის გამართული დოკუმენტაციის არსებობა, რომელიც საშუალებას მოგვცემს, ხარვეზის განმეორების შემთხვევაში, უკვე არსებული გეგმის მიხედვით, სწრაფად მოვაგვაროთ პრობლემა. დოკუმენტაციის განახლება უნდა ხდებოდეს მუდმივად, რადგან შესაძლოა არსებული ინციდენტის შემდეგ მიგნებულ იქნას უფრო ეფექტური გამოსავალი.

მომხდარი პრობლემებიდან გამომდინარე, უნდა მოხდეს ანალიზი. აუცილებელია, განვსაზღვროთ ჩვენს ხელთ არსებული საინფორმაციო სისტემების სუსტი მხარეები – გამოვავლინოთ არეები, სადაც ყველაზე ხშირია კრიტიკული სიტუაციების მოხდენის სიხშირე. ანალიზზე დაყრდნობით საჭიროა შემუშავდეს გეგმა, რომელიც აღნიშნული სუსტი მხარების გამოსწორებიაკენ იქნება მიმართული. სტრატეგიის განხორციელება უნდა ეფუძნებოდეს მიზნობრივად შედგენილ ამოცანებს, რომელიც კონკრეტული პრობლემების შემცირებაზე იქნება ორიენტირებული. საქმიანობა ბევრად წარმატებული და უსაფრთხო იქნება, თუ იარსებებს სცენარი, რომელშიც მოსალოდნელი კრიტიკული მომენტის დადგომის შემთხვევაში რეაგირების ინსტრუქციები იქნება გაწერილი.

ნებისმიერ ორგანიზაციას გააჩნია კრიტიკული ინფორმაცია, რომლის დაკარგვა ან დაზიანება მნიშვნელოვან შეფერხებასთან თუ დანახარჯებთანაა

დაკავშირებული. სწორედ ამიტომ, საინფორმაციო სისტემების უდანაკარგო მუშაობა გამართულ ზეა (backup) დამოკიდებული. რეზერვაცია გულისხმობს ჩანაწერების კოპირებას ან არქივაციას (გადატანას) ერთი მანქანიდან სხვა მანქანაზე, ან უბრალოდ მყარ დისკზე უსაფრთხო ადგილას, რათა თავიდან იქნას აცილებული ინფომაციის დაკარგვა.

რეზერვაცია თანამედროვე ტექნოლოგიების განუყოფელი ნაწილია, მასში მოიაზრება ორი ძირითადი პროცესი:

1. კრიტიკული ინფორმაციის არქივაცია;
2. კატასტროფის შემთხვევაში ინფორმაციის აღდგენა.

არსებობს რეზერვაციის უამრავი სახეობა, ისინი ერთმანეთისგან განსხვავდება: მდებარეობის, ინფორმაციის მთლიანობის, ტექნოლოგიებისადა გეოგრაფიული მდებარეობის მიხედვით. გამოყოფენ Local Backup-ს და Offsite Backup-ს. პირველ ტიპს მიეკუთვნება რეზერვაციის პროცესი, როდესაც იგი მიმდინარეობს ერთ კონკრეტულ გეოგრაფიულ მონაკვეთზე, მაგალითად ერთ შენობაში. ხოლო მეორე ტიპი გულისხმობს ფაილების კოპირებას ორ ან რამდენიმე გეოგრაფიულ წერტილს შორის. ინფორმაციის მთლიანობის მიხედვით გამოიყოფა Full (ყოველ ჯერზე ხდება მონაცემების სრულად კოპირება) და Incremental backup (ერთხელ კოპირდება არსებული ინფორმაცია და ყოველ შემდეგ ჯერზე ემატება მხოლოდ განხორციელებული ცვლილების შემცველი ფაილი). ტექნოლოგიური მეთოდის მიხედვით: Mirroring სინქრონულ რეზერვაციას გულისხმობს, ანუ მუშა მანქანაზე/მყარ დისკზე მიმდინარე პროცესები პარალელურად აისახება სარეზერვო სისტემაზე. როდესაც ხდება ჩანაწერის დამატება/წაშლა ერთ მოწყობილობაზე, ავტომატურად იგივე პროცესი მიმდინარეობს მეორეზეც.

მირორინგისთვის, როგორც წესი კლასტერულ არქიტექტურას იყენებენ - კლასტერში შემავალი ერთ-ერთი მანქანის გათიშვის შემთხვევაში, დარჩენილი კომპიუტერი აგრძელებს მიმდინარე პროცესებს და ტექნიკური ხარვეზი მომხმარებლისათვის შეუმჩნეველი რჩება. რეზერვაცია შეიძლება მოხდეს როგორც ლოკალურ ქსელში არსებულ სარეზერვო მანქანაზე, ასევე ინტერნეტ სივრცეშიც, ასეთ მიდგომას Cloud Backup-ს უწოდებენ.

საინფორმაციო სისტემების მენეჯმენტში, ერთერთ ყველაზე აქტუალურ თემას სტანდარტიზაცია წარმაოდგენს. განსაკუთრებით მნიშვნელოვანია შიდა სტანდარტიზაცია და პროცესების გარკვეულ ჩარჩოებში მოქცევა. წინააღმდეგ შემთხვევაში თავს იჩენს აღრიცხვასა და მმართველობით საქმიანობასთან არსებული პრობლემები. ეს საკითხი განსაკუთრებული სიმწვავით დიდ კომპანიებში დგას, რომელთაც ფართომასშტაბიანი კომპიუტერული ქსელის ექსპულატაცია, განვითარება უწევთ. მაგალითად ავიღოთ ორგანიზაციაში არსებული კომუნიკაციის საშუალება. თუ კომუნიკაციისათვის შემოვიღებთ სტანდარტს და ვიტყვით, რომ ურთიერთობისათვის ვიყენებთ Instant Messaging-ს, ყველას ეცოდინება, რომ ნებისმიერ ადამიანთან დაკავშირება იქნება შესაძლებელი ჩატის საშუალებით და ყველა გამოიყენებს ამ საშუალებას. ხოლო თუ მომხმარებლებს მითითებას არ მივცემთ, ინფორმაციის გაგზავნა/მიღებას ყველა განსხვავებული გზით ეცდება. შესაბამისად მრავალი გზავნილი ადრესატამდე ვერ მიაღწევს და წარმოიშვება ქაოსი. ამ სიტუაციის მსგავსად ბუნდოვანი სტანდარტების არსებობა ან საერთოდ მათი არქონა შრომის ნაყოფიერების და დროითი დანახარჯის დეგრადაციას იწვევს.

1.2. საინფორმაციო სისტემების ცვლილებების მენეჯმენტი

რეაქცია ცვლილებებზე ორგანიზაციაში მართვის ყველა დონეს ეხება. თუმცა მას აქვს განსხვავებული ხასიათი და განსხვავებულია ცვლილებების შედეგებიც. მაგალითად, თუ რომელიმე კომპანიის უმაღლესი დონის ხელმძღვანელობა გადაწყვეტს მოდერნიზაციას, საშუალო დონის მენეჯერები და სპეციალისტები ამზადებენ ინფორმაციას გასატარებელ ღონისძიებებზე და მოსალოდნელი ხარჯების ალტერნატიულ ვარიანტებზე. ძირეული დონის მენეჯერები პასუხს აგებენ დასახული ღონისძიების პრაქტიკულ რეალიზაციაზე. მუშებიც უნდა გაერკვნენ ცვლილებების არსში, რომ შეძლონ ახალი მოთხოვნილებების შესაბამისად მუშაობა და ხარისხიანი პროდუქციის წარმოება.

ორგანიზაციული ცვილილება მოიცავს ოთხსაფეხუროვან პროცესს: ცვლილებების იდენტიფიცირება ბიზნეს გარემოში; კომპანიის საჭიროებების

შესაბამისი გადაწყვეტილების განვითარება; თანამშრომელთა გადამზადება შესაბამის ცვლილებებისთვის და თანამშრომელთა მხარდაჭერის მოპოვება.

ცვლილებების მართვის პროცესი, პირველ რიგში გულისხმობს მათი განხორციელების აუცილებლობის გაცნობიერებას. ცვლილებების აუცილებლობის შეგრძნება შეიძლება დაკავშირებული იყოს შემდეგ ფაქტორებთან: კონკურენცია, საერთო ეკონომიკური სიტუაცია, საკანონმდებლო აქტები, მწარმოებლურობის შემცირება, უკიდურესად მზარდი დანახარჯები, კადრების დიდი დენადობა და სხვა. როგორც წესი, ცლილებებს ყოველთვის მოყვება წინააღმდეგობა როგორც პერსონალის, ასევე სხვა შიდა ფაქტორების მხირდან. ცვლილება ყოველთვის გაურკვევლობასთან და სტაბილურობის შემცირებასთანაა დაკავშირებული. წინააღმდეგობის შესამცირებლად საუკეთესო გზაა თანამშრომელთა ჩართვა გდაწყვეტილების მიღების პროცესში. პლურალისტური მიდგომა ოპტიმალური გადაწყვეტილების მიღების წინაპირობაა.

ახალი მოთხოვნების გაჩენა განსხვავებული გამოწვევების წინაშე აყენებს ელექტრონულ ბაზარზს. საინფორმაციო სისტემების განვითარება პირდაპირ კავშირშია კომპიუტერული ტექნოლოგიების პროგრესთან, რომელიც წლიდან წლამდე გეომეტრიული პროგრესიით იზრდება. გამონაკლისი არც ქართული ბაზარია. მწვავე კონკურენციის პირობებში, თითოეული კომპიუტერული პროდუქციის მწარმოებელი ცდილობს რაც შეიძლება მალე განაახლოს საწარმოო ხაზი, რათა არ დაკარგოს საკუთარი პოზიციები. შესაბამისად უკანასკნელი პერიოდის განმავლობაში მკვეთრად შემცირდა სისტემების სასიცოცხლო ციკლი. ყოველდღიურად რაღაც ახლის დამატება, დანერგვა ხდება საჭირო. ეს ყოველივე წინა პლანზე წევს აქამდე ნაკლებად ცნობილ მიმართულებას – ცვლილებების მენეჯმენტს.

საინფორმაციო ტექნოლოგიების განყოფილებები თუ კომპიუტერული კომპანიები იძულებულნი არიან ფეხდაფეხ მიყვნენ არსებულ დაკვეთას. კომპიუტერული ტექნიკის განახლება სერიოზულ ხარჯებთანაა დაკაშირებული. ამიტომ, აღნიშნულ სფეროში მომუშავე სპეციალისტები ეძებენ სისტემების სასიცოცხლო ციკლის გახანგრძლივების გზებს, რაც გარკვეულწილად ღია სისტემების შეძენითა და იმპლემენტაციით მიიღწევა. „გახსნილობა“ გულისხმობს დეველოპერებისათვის მაქსიმალური თავისუფლების მიცემას, მათ შეუძლიათ

მოახდინონ ამგვარი სისტემების არა მარტო მოდერნიზაცია, არამედ მნიშვნელოვანი მოდიფიკაცია, რათა უკეთ მოარგონ საკუთარი კომპანიების ინტერესებს. „ღია სისტემის“ თვალსაჩინო მაგალითია Linux, რომლის უამრავი ვერსია ცნობილი (Fedora, Ubuntu, Minth და ა.შ.) განვითარების დიდი პოტენციალის მიუხედავად, ისევე როგორც ყველა პროდუქტს, საბოლოოდ ღია სისტემებსაც გააჩნია ზღვრული სარგებლიანობა, რაც მის სასიცოცხლო ციკლსაც ბევრად ხანგრძლივს, თუმცა მაინც ვადებში შეზღუდულს ხდის.

ცვლილებები ხდება მუდმივად. იცვლება როგორც პროგრამული, ასევე ტექნიკური უზრუნველყოფის ვერსიები. საჭირო ხდება მუშა სისტემების გარდაქმნა და ამავდროულად შეფერხებების მინიმიზაცია. გამომდინარე აქედან, სისტემის ადმინისტრატორები იძულებულნი არიან ცვლილებები მომხმარებლისათვის უმტკივნეულოდ და ამავდროულად ეფექტურად განახორციელონ. აღნიშნული მოვლენა გუსტ დაგეგმარებას და საფეხურებრივ მოქმედებებს საჭიროებს. გარდაქმნების რევოლუციურმა გზამ, შესაძლოა გამოიწვიოს, როგორც ტექნიკური ხარვეზები, ასევე პერსონალის გაურკვევლობა და უკმაყოფილება. ამ გვერდითი მოვლენების თავიდან ასაცილებლად, საჭიროა საპროექტო ჯგუფმა მუდმივი კონტაქტი იქონიოს მომხმარებელთა ჯგუფთან, რათა დროულად გასცეს საჭირო ახსნა-განმარტებები და მოახდინონ წარმოქმნილი ხარვეზების მინიმალურ დროში აღმოჩენა-გამოსწორება. საკმარისი აღარაა მხოლოდ ტექნოლოგიური პერსონალის გამართული მუშაობა, აუცილებელია, საპროექტო და მომხმარებელთა ჯგუფებმა იმუშაონ გუნდურად საქმიანობის ნაყოფიერების გასაზრდისათვის.

ხარვეზების თავიდან ასაცილებლად, აუცილებელი ხდება ე.წ. სატესტო გარემოს შექმნა, სადაც საინფორმაციო სისტემების სპეციალისტები მოახდენენ სიახლის საპილოტო ვერსიის გაშვებასა და გამოცდას. ხშირად საჭირო ხდება რამდენიმე მსგავსი „გარემოს“ არსებობა:

1) დეველოპერებისთვის (ხალხი, ვინც უშუალოდ ქმნის ახალ პროდუქტს);

2) „ტესტერებისთვის“ (ხალხი, რომელიც ამოწმებს შექმნილ პროდუქტს და იძლევა დასტურს მის გამართულობაზე);

3) რეალურის ანალოგიური გარემო, მასზე მუშაობს პერსონალი, რომელიც უშუალოდ ახორციელებს სიახლის იმპლემენტაციას. ეს უკანასკნელი გაცილებით

რთული შესაქმნელია, ვიდრე წინა ორი და დიდ სიმძლავრეებს საჭიროებს. მიუხედავად ამისა მისი მეშვეობით შესაძლო ხდება პრობლემის დროული აღმოჩენა-გამოსწორება.

ინფორმაციული ტექნოლოგიების სფეროში, თითოეული ცვლილების განხორციელებამდე აუცილებელია მოხდეს მიმდინარე სისტემის რეზერვაცია, რათა არასასურველი სცენარის შემთხვევაში გვქონდეს ძველ ვერსიაზე დაბრუნების საშუალება.

განახლებას განახლება მოსდევს, არსებული დონით დაკმაყოფილება პოზიციების დათმობის წინაპირობაა. საინფორმაციო ტექნოლოგიების მენეჯერებისადმი წარმოიშვა საქმიანობის ახალი სფერო – ცვლილებების მენეჯმენტი, რომელიც მათგან კიდევ უფრო მეტ აქტივობას და ნოვატორობას მოითხოვს.

1.3. ინფორმაციული უსაფრთხოების უზრუნველყოფის ამოცანები

თანამედროვე ეპოქა შეიძლება დავახასიათოთ, როგორც გადასვლა ინდუსტრიული საზოგადოებიდან ინფორმაციულზე. XXI საუკუნეში გაჩნდა ახალი ტერმინი „ინფორმაციული რესურსი“, რომლის ფასი დღითიდღე მატულობს და აღემატება ნებისმიერ მატერიალურ დოვლათს, მათ შორის ფინანსურს. ინფორმაციის ღირებულება ტოლია იმ მოგებისა, რომლის მოტანაც მის გამოყენებას შეუძლია. ინფორმაციული მარაგების სწორად განკარგვა თანამედროვე საზოგადოების პრიორიტეტია. ინფორმაციული რესურსი არის აქტივი, რომელიც არ არის მონოპოლიზებული და სხვადასხვა ობიექტის ხელშია დივერსიფიცირებული. ისევე, როგორც სხვა აქტივების მეპატრონეს, ინფორმაციის მფლობელსაც შეუძლია პირადი სარგებლისთვის გამოიყენოს იგი – შექმნას, გაყიდოს ან გაანადგუროს იგი. მატერიალური რესურსებისგან განსხვავებით, ინფორმაცის ფლობა მეტად საპასუხისმგებლო და მაღალეფექტურია.

თანამედროვე საბაზრო ეკონომიკის პირობებში, ინფორმაცია არის წარმოების უმთავრესი კომპონენტი და მისი ექსკლუზიურად ქონა კონკურენტულ ბრძოლაში გამარჯვების წინაპირობაა. ინფორმაციის უსაფრთხოება, ისევე როგორც ინფორმაციის დაცვა, კომპლექსური და რთული ამოცანაა, რაც მიმართულია უსაფრთხოების უზრუნველყოფისა და სპეციალური სისტემების დანერგვისკენ.

ინფორმაციის დაცვა მთელი რიგი კომპანიებისთვის საკმაოდ პრობლემატური საკითხია და მოიცავს არაერთ ამოცანას. მას შემდეგ, რაც ტექნოლოგიურმა პროგრესმა შეაღწია ყველა სფეროში, მათ შორის ბიზნესშიც, აქტიურად ხდება ინფორმაციის გაცვლა და გადაცემა. ეს ყველაფერი კი ხელს უწყობს იმ საკმაოდ ძვირფასი და ღირებული ინფორმაციის გაძინებას, რასაც კომპანიისთვის სასიცოცხლო მნიშვნელობა აქვს.

კონკურენტულ უპირატესობას მნიშვნელოვნად განაპირობებს მეწარმის ხელთ არსებული ექსკლუზიური ინფორმაცია. კონკურენტების შესახებ ინფორმაციის მოპოვება მუდამ აქტუალური იყო და მისი ისტორია უძველესი დროიდან იღებს სათავეს. თუმცა უკანასკნელ პერიოდში, როდესაც ტექნოლოგიები სწრაფად განვითარდა და ინფორმაციულმა საცავებმა ელექტრონული სახე მიიღო, გაჩნდა ისეთი ტერმინი, როგორიცაა „კიბერშპიონაჟი“. აღნიშნული მოქმედება ტექნოლოგიური საშუალებებით არასანქცირებული, კონფიდენციალური მონაცემების მიღებას გულისხმობს. გამოკვლევების თანახმად არალეგალური ინფორმაციის 40%-ზე მეტი კიბერშეტევების საშუალებითაა მიღებული.

ინფორმაციული შეტევა შეიძლება იყოს მრავალი სახის, მისი ზეგავლენით შესაძლოა მოხდეს ინფორმაციის არასანქცირებული კოპირება, არასანქცირებული მოდიფიკაცია – მთლიანობის დარღვევა, განადგურება, მითვისება. ITIL-ის თანახმად, რომელიც მსოფლიოში IT სერვისების მართვის ერთ-ერთ ყველაზე გავრცელებულ მიდგომას წარმოადგენს, ინფორმაციული უსაფრთხოება თავის თავში მოიცავს მონაცემების კონფიდენციალობას, მთლიანობას და ხელმისაწვდომობას. ამ თეზისის საფუძველზე შემუშავებულია ინფორმაციული უსაფრთხოების სია:

- Confidentiality (კონფიდენციალურობა) – ინფორმაციაზე ავტორიზებული და ლოგიკურად შესაბამისი პირების წვდომა.
- Integrity (მთლიანობა) – ინფორმაციის სისრულე, რაც გულისხმობს მის ნამდვილობას და მთლიანობას.
- Availability (ხელმისაწვდომობა) – საჭიროების შემთხვევაში ინფორმაცია უნდა იყოს წვდომადი.

უსაფრთხოების არსის გასაგებად აუცილებელია მისი კომპონენტების განხილვა. რა არის რისკი? რისკი ეს არის ნებისმიერი სახის გარემოება,

რომელმაც შესაძლოა ზეგავლენა იქონიოს ორგანიზაციის აქტივებზე, ჩვენს შემთხვევაში ინფორმაციაზე და ამ გზით ზიანი მიაყენოს საქმიანობას. რისკი შეიძლება იყოს მრავალმხრივი, ის შეიძლება მომდინარეობდეს როგორც გარე, ასევე შიდა ფაქტორებიდან. რისკი შეიძლება იყოს გამიზნული ან შემთხვევითი მოვლენის შედეგი, თუმცა ნებისმიერი სახის რისკს ჭირდება გაანალიზება და მართვა:

- საფრთხეები და გაურკვევლობები;
- კრიტიკული ინფორმაცია;
- რისკის შეფასება.

ინფორმაციული რისკის ანალიზის საწყის ეტაპზე ხდება მოსალოდნელი საფრთხეების გამოვლენა. განიხილება ფაქტორთა მაქსიმალურად ფართო სპექტრი, რომელმაც შესაძლოა ზიანი მიაყენოს საქმიანობის მიმდინარეობას. მეორე ეტაპზე ხდება უკვე გამოვლენილი რისკების კლასიფიკაცია ობიექტის მიხედვით. ამ ეტაპზე უკვე განიხილება, თუ ინფორმაციის კონკრეტულ ტიპს რა ზიანი შეიძლება მიადგეს. მაგალითად ელექტრონული სახით არსებული ინფორმაცია შესაძლოა დაზიანდეს ელექტრული კვების წყაროს გათიშვის შედეგად, ხოლო ბეჭდურ ინფორმაციას ემუქრებოდეს სხვა საფრთხეები. მესამე ეტაპზე უკვე ხდება გამოვლენილი და დახარისხებული რისკების შეფასება მატერიალურ ერთეულში, ანუ რა ფინანსური ზარალის მიყენება შეუძლია კონკრეტული მონაცემის დაზიანებას ორგანიზაციის საწარმოო პროცესისათვის.

უსაფრთხოების თანამედროვე პოლიტიკის მიზანია მაქსიმალურად პასუხობდეს არსებულ გამოწვევებსა და რისკებს.

უსაფრთხოების განხილვისას, კიდევ ერთი საკვანძო საკითხია ინციდენტი. ინციდენტი ეს არის კონკრეტული მოვლენა, რომელიც უარყოფით ზემოქმედებას ახდენს სისტემის წარმადობაზე, იწვევს ინფორმაციის დაზიანებას ან დაკარგვას. ინციდენტები ხდება ყოველდღიურად, ისინი განსხვავდება სირთულის მიხედვით, ინციდენტი შეიძლება იყოს მარტივი ან რთული. მარტივი ინციდენტის შემთხვევაში, შეცდომა (პრობლემის მიზეზი) და შედეგი (ზიანი) პირდაპირ კავშირშია ერთმანეთთან და მათი გამოვლენა მიზეზ-შედეგობრივი გზით იოლია.

რაც შეეხება რთულ ინციდენტს, ის შეიძლება იყოს ერთმანეთთან დაკავშირებული რამდენიმე ელემენტის შეცდომა. ამ შემთხვევაში, პრობლემის

მიზეზების გამორკვევა შედარებით რთულია, რადგან პრობლემის შედეგი და მიზეზი ერთმანეთისგან მნიშვნელოვნადაა დაშორებული და მათი დაკავშირება რთულ სამუშაოს მოითხოვს.

უსაფრთხოების მიზნებიდან გამომდინარე, ინციდენტების მიერ უარყოფითი ეფექტის შესამცირებლად აუცილებელია არსებობდეს ინციდენტმენეჯმენტის გეგმა, რომელიც მოიცავს როგორც ინციდენტის პრევენციის, ასევე ინციდენტების დამუშავების გეგმას. პრევენციული ღონისძიებები გულისხმობს მოქმედებებს, პროექტებსა და გატარებულ სამუშაოებს, რომლებიც მიმართულია ინციდენტების თავიდან ასაცილებლად, ისინი ეფექტურია პროგნოზირებად რისკებთან მუშაობისას. რაც შეეხება ინციდენტის ესკალაციის დოკუმენტს, იგი წარმოადგენს წინასწარშედგენილ გეგმას, რომელიც ამა თუ იმ ინციდენტის დადგომის შემთხვევაში, პრობლემის მოსაგვარებლად კონკრეტული ღონისძიებების გატარებას გულისხმობს.

ინციდენტების უმეტესობა განმეორებადია, შესაბამისად მსგავსი გეგმის შესადგენად, აუცილებელია, როგორც საკუთარი, ასევე პარტნიორთა თუ კონკურენტთა გამოცდილების გაზიარება.

იმისთვის, რომ შედგეს მოქმედების გეგმა, უნდა მოხდეს წარსული გამოცდილების ანალიზი. პრობლემები უნდა დახარისხდეს ხდომილობის სიხშირის და კრიტიკულობის მიხედვით - თუ რამდენად დიდი ზარალის მიყენება შეუძლია მას. ამის შემდეგ უნდა მოხდეს პრობლემის გადაჭრის გზების აღრიცხვა და ოპტიმიზება. მსგავსი გეგმის არსებობის პირობებში ინციდენტის განმეორების შემთხვევაში, პერსონალს უკვე გააჩნია სამოქმედო გეგმა და არ უწევს სპონტანური გადაწყვეტილებების მიღება, რაც რისკის შემცირებას ახდენს.

ნებისმიერ ინციდენტს გააჩნია სასიცოცხლო ციკლი, რომელიც რამდენიმე ძირითადი ფაზისგან შედგება. ესენია:

- პრობლემის აღმოჩენა;
- პრობლემის მიზეზის იდენტიფიკაცია;
- ინციდენტზე რეაგირება;
- ინციდენტის და მისი აღმოფხვრის გზების აღრიცხვა.

ესა აგზა, რომლის სრულად გავლა მინიმუმამდე ამცირებს საოპერაციო რისკებს და მკვეთრად ზრდის ინციდენტმენეჯმენტის ეფექტურობას.

ინფორმაციული უსაფრთხოება ორგანიზაციის უსაფრთხოების მენეჯმენტის უმნიშვნელოვანესი კომპონენტია და ინფორმაციული ტექნოლოგიების გარდა, ის მოიცავს ინფორმაციული რესურსების ისეთ ნაწილსაც, როგორიცაა ბეჭდური სახით არსებული მონაცემები, სატელეფონო ზარები და ა.შ.. მარტივად რომ ვთქვათ, ინფორმაციული უსაფრთხოება უფრო ფართო ცნებაა ვიდრე IT უსაფრთხოება. იგი მოიცავს მონაცემებს, როგორც ელექტრონული, ასევე ფიზიკური სახით.

IT უსაფრთხოება მოიცავს ელექტრონული სახით არსებულ ინფორმაციულ აქტივებს, რომლებიც ინახება კომპიუტერებში, სმარტფონებში, ფლეშბარათებსა თუ სხვა ელექტრონულ მოწყობილობებზე.

რაც შეეხება უსაფრთოებას, შეიძლება ითქვას, ის ყველაზე ფართო სფეროა ინფორმაციულ ტექნოლოგიებში. ის მოიცავს ყველაფერს, დაწყებულს ფიზიკური უსაფრთხოებიდან, დამთავრებული ვირტუალური დაცვით.

ინფორმაცია, თანამედროვე სამყაროს ყველაზე ძვირადღირებული რესურსია. აქედან გამომდინარე, ინფორმაციის შეძენის შემდეგ, ისევე, როგორც სხვა ნებისმიერი საკუთრების შემთხვევაში, ჩნდება მისი მიზანმიმართულ დაზიანებასა თუ ძარცვასთან დაკავშირებული საფრთხე და მააშასადამე დაცვის აუცილებლობა. უსაფრთხოების უზრუნველყოფისათვის ცენტრალურ როლს თამაშობს ორი კომპონენტი: ფიზიკური უსაფრთხოება, რომელიც მოწყობილობებისა თუ კომუნიკაციის ფიზიკურად დაცვის ღონისძიებებს მოიცავს და ვირტუალური უსაფრთხოება, რომელიც ელექტრონულ ინფორმაციაზე არასასურველი პირების წვდომას გღუდავს ქსელური მოწყობილობების საშუალებით. სწორედ ამ უკანასკნელზე გავამახვილებთ ყურადღებას. პირველ რიგში, დგება ტოპოლოგია და იგეგმება შიდა ქსელის არქიტექტურა. ხდება შიდა ქსელის (LAN) და გარე ქსელის (WAN) წარმოსახვითი გაყოფა. როგორც წესი, უსაფრთხოების დაცვის მიზნით იყენებენ ქსელურ მოწყობილობას Firewall-ს. სახელწოდებიდან გამომდინარე, იგი წარმაოდგენს ერთგვარ წინაღობას გარე ქსელიდან შემომავალი მოთხოვნისათვის. მასში ზედმიწევნითაა გაწერილი, თუ რა ტრაფიკი უნდა იქნას დაშვებული და რა-აკრძალული.

მონაცემთა ბაზები, საინფორმაციო ელექტრონული საცავები თანამედროვე საინფორმაციო სისტემების მთავარი შემადგენელი ნაწილია. ინფორმაციულ საცავში თავს იყრის ორგანიზაციის სრული საინფორმაციო რესურსი, მათ შორის

კონფიდენციალური და კრიტიკული ინფორმაცია, რომლის დაკარგვა – წაშლა, არასანქცირებული მოდიფიკაცია ან ორგანიზაციის გარეთ „გაჟონვა“ მნიშვნელოვან პრობლემებთან იქნება დაკავშირებული.

მონაცემთა ბაზების უსაფრთხოება ცალკე თემად განიხილება უფრო მსხვილ სფეროებში, როგორებიცაა ინფორმაციული უსაფრთხოება, კომპიუტერული უსაფრთხოება და რისკმენეჯმენტი.

მონაცემთა ბაზების უსაფრთხოება მრავალი კომპონენტისგან შედგება:

- რეზერვაცია
- წვდომის კონტროლი
- აპლიკაციის დაცვა
- კრიპტაცია
- აუდიტი

თუ რამდენიმე წლის წინ უსაფრთხოების ძირითადი აქცენტი ქსელის დაცვაზე კეთდებოდა და საფრთხის ძირითად წყაროდ ინტერნეტი ითვლებოდა, თანამედროვე სამყაროში ვითარება რადიკალურად შეცვლილია. ინფორმაციის უდიდესი ნაწილი ორგანიზაციის შიგნით მიმდინარე პროცესებით მიანდება. ეს გამოწვეულია, როგორც კიბერშპიონაჟის გავრცელებით, ასევე თანამშრომელთა დაუდევრობითა თუ დაბალი კვალიფიკაციით. გამომდინარე აქედან, ქსელის უსაფრთხოებასთან ერთად გაჩნდა სისტემების როგორც ფიზიკური ასევე პროგრამული დაცვის აუცილებლობა.

აპლიკაცია სისტემების ერთ-ერთი უმნიშვნელოვანესი ნაწილია. ინფორმაციაზე წვდომისას, პირველ რიგში სწორედ მასთან უწევს შეხება მომხმარებელს. შესაბამისად მისი დაცულობის ხარისხზე დიდათაა დამოკიდებული ინფორმაციის უსაფრთხოება. აპლიკაცია წარმოადგენს მონაცემთა ბაზებზე ზემოქმედების ბერკეტს. ყველა აპლიკაციას შეიძლება ქონდეს განსაზღვრული და შეზღუდული წვდომა კონკრეტული ტიპის ინფორმაციაზე. როგორც წესი, მონაცემთა ბაზები საკმაოდ მყარადაა დაცული, როგორც ფიზიკურ, ასევე ქსელურ დონეზე. იგივეს ვერ ვიტყვით მის ინტერფეისზე. განსაკუთრებით მიმდინარე პერიოდში, როდესაც ვებაპლიკაციები მოქნილობის გამო ჩვენი ცხოვრების განუყოფელი ნაწილი გახდა და მათზე წვდომა მსოფლიოს ნებისმიერი წერტილიდან ღიაღაა

შესაძლებელი. რამდენადაც მოსახერხებელია ის, იმდენად იოლია მასზე ზემოქმედება.

თანამედროვე კიბერ შეტევების უმეტესობა ვებსაიტების გავლით ინფორმაციის დაზიანებასა, თუ მოპარვაზეა ორიენტირებული. ამ პირობებში აპლიკაციის დაცვის აქტუალობა კიდევ უფრო მატულობს. თუ ადრე, დეველოპერები მხოლოდ ინტერფეისის შექმნაზე იყვნენ ორიენტირებულნი, დღეს უკვე მნიშვნელოვანი ძალისხმევა იხარჯება აპლიკაციის წერისას კოდის დახვეწასა და ოპტიმიზაციაზე, ატარებენ ცდებს, რომლებიც სისტემის „გატეხვას“ ისახავენ მიზნად, შედეგად ნაპოვნი სუსტი წერტილების გასაუმჯობესებლად იწყება მუშაობა.

კრიპტაცია, იგივე დაშიფრვა მონაცემების ისეთი სახით შენახვას გულისხმობს, რომელიც აღქმაც გარეშე პირისთვის შეუძლებელია. შიფრაციის დროს, ღია ტექსტი ინახება უშინაარსო სიმბოლოების მეშვეობით. იმისთვის, რომ ამ სიმბოლოების წაკითხვა პირვანდელი სახით მოხერხდეს მისი გაშიფრვაა აუცილებელი.

ცნობილია შიფრაციის ორი ძირითადი მეთოდი: სიმეტრიული (Private key cryptography) და ასიმეტრიული (Public key cryptography). სიმეტრიული შიფრაციის თავისებურება მისივე სახელწოდებიდან გამომდინარეობს – ინფორმაციის დასაშიფრადა და მის გასაშიფრად ერთი და იგივე, იდენტური გასაღები გამოიყენება. რაც შეეხება ასიმეტრიულს შიფრაციას, ის ორი ნაწილისგან შედგება: მონაცემების დაშიფრვა ხდება Public Key-ს მეშვეობით, ხოლო მის წასაკითხად აუცილებელია Private Key, რომლითაც შიფრის საწყის სახეთ გადაქცევა ხდება. [1]

უკანაკნელი მეთოდის შემუშავება 70- იან წლებში დაიწყო და დღეისთვის განსაკუთრებული პოპულარობით სარგებლობს, ვინაიდანის მომხმარებელს აძლევს საშუალებას იოლად მოახდინოს მონაცემების დაშიფრვა და დაცვა.

კიდევ ერთი საკითხი, რომელიც თანამედროვე უსაფრთხოებისათვისაა მნიშვნელოვანი კომპლექსური აუდიტია. გაზრდილი საინფორმაციო ნაკადების კონტროლი და დამუშავება მუდმივად უფრო რთულდება. შესაბამისად, მათი კლასიფიკაციისა და ანალიზისათვის ყურადღების დათმობაა აუცილებელი.

საწარმოს თანამედროვე საინფორმაციო სისტემებს, გააჩნია რა დიდი რაოდენობის პროგრამული და აპარატურული საშუალებები, აქვთ რთული ჰეტეროგენული სტრუქტურა. ბუნებრივია, რომ ასეთ პირობებში ძალზედ რთულია

მოსალოდნელი საფრთხის ან განხორციელებული თავდასხმის როგორც ოპერატიული აღმოჩენა, ასევე მათი სალიკვიდაციო ღონისძიებების დროული ჩატარება. დიდია იმის ალბათობა, რომ ზოგიერთი თავდასხმა ხდომილების შემდგომ იქნეს აღმოჩენილი ან საერთოდ იგნორირებული დარჩეს. აღნიშნული პრობლემის გადასაწყვეტად საჭიროა ინფორმაციული უსაფრთხოების რისკების მართვის კარგად ორგანიზებული სისტემის შექმნა, სადაც მნიშვნელოვანი ადგილი უჭირავს როგორც საინფორმაციო სისტემების მუდმივ მონიტორინგს და კომპლექსური აუდიტის წარმოებას, ასევე აუდიტორული რისკების შეფასებას.

საქართველოში ტექნიკური აუდიტი წლიდან წლამდე უფრო მასიურად იკიდებს ადგილს. თუ რამდენიმე წლის წინ მსგავს მომსახურებას მხოლოდ ფინანსური საქმიანობისთვის იყენებდნენ, დღეისათვის აუდიტი IT საქმიანობის განუყოფელი ნაწილი გახდა, განსაკუთრებით მსხვილ ორგანიზაციებში.

ინფორმაციული სისტემების უსაფრთხოების სფეროში იკვეთება ორი ასპექტი: რეზერვაცია და წვდომის კონტროლი. პირველი მნიშვნელოვანია ორგანისაციის ფუნქციონირებისა და რეზერვაციის შეუფერხებლად განხორციელებისთვის.

ხშირად, ერთი ან რამდენიმე პროგრამული უზრუნველყოფის გაშვება არაა საკმარისი და დამოუკიდებელი სისტემების შექმნა ხდება საჭირო, რომელიც ინფომაციის დაარქივება/გადატანას უზრუნველყოფს. რეზერვაციის სისტემა, თავის მხრივ, ფართო ცნებაა და რამდენიმე კომპონენტს შეიცავს, მათ შორის, ფიზიკურ სერვერს, პროგრამულ უზრუნველყოფას და კარგად დაგეგმილ, აწყოილ ქსელურ ინფრასტრუქტურას. შესანახი ინფორმაციის მოცულობა და არქივების გადატანის ინტენსივობა ერთი მანქანიდან მეორეზე განაპირობებს მოთხოვნას ქსელის გამტარობაზე, ანუ ტრაფიკზე. ხშირია შემთხვევები, როდესაც როუტერი ვერ ახერხებს მიღებული პაკეტების დამუშავებას და „ეკიდება“. არასწორად დაგეგმილმა ქსელმა შესაძლოა გამოიწვიოს არა მარტო ბექაფ სისტემის „ჩავარდნა“ არამედ ყველა იმ პროცესის შეფერხება, რომელიც იგივე შეერთებას იყენებს.

დღეისათვის საკომუნიკაციო საშუალებების სწრაფმა განვითარებამ ინტერნეტის სისწრაფე მკვეთრად გაზარდა, რამაც მონაცემების შენახვის თავისებურებების ცვლილება მოახდინა. ყოველ დღიურად უფრო პოპულარული ხდება ინფორმაციის ინტერნეტ სივრცეში რეზერვაცია. არსებობს მრავალი

ინტერნეტ რესურსი, რომელიც სრულიად უფასოდ გვთავაზობს გარკვეული მოცულობის ინტერნეტსაცავს. კომპანიებს უკვე შეუძლია დამატებითი აპრატურისა და პროგრამული უზრუნველყოფის გარეშე მოახდინონ საკუთარი ინფორმაციის კოპირება ინტერნეტ სივრცეში.

სატელეკომუნიკაციო ქსელების როლის ზრდასთან ერთად მატულობს წვდომის კონტროლის აუცილებლობა. იმ პირობებში, როდესაც მონაცემების დიდი ნაწილი ინტერნეტის გავლით, ორგანიზაციის ფარგლებს გარეთ მოძრაობს, იზრდება მათზე არასანქცირებული ზემოქმედების ალბათობა.

წვდომის კონტროლი ძირითადი სამი საფეხურისგან შედგება:

- იდენტიფიკაცია;
- აუთენტიფიკაცია
- ავტორიზაცია

იდენტიფიკაციის საფეხური მომხმარებლის ვინაობის ავთენტურობის დადგენას გულისხმობს.ამ საფეხურზე განისაზღვრება არის თუ არა მომხმარებელი ნამდვილად ის, ვისი სახელითაც ის ცდილობს სისტემაზე წვდომას.

აუთენთიფიკაციის ეტაპზე სუბიექტი ახდენს გარკვეული ინფორმაციის შეყვანას სისტემაში, რომელიც ადასტურებს მის ავთენტურობას. ამ საფეხურის გასავლელად ყველაზე ხშირად გამოიყენება მომხმარებლის სახელი და პაროლი. აღნიშნულ პუნქტებს შეიძლება დაემატოს ერთჯერადი პაროლი, რომელიც უსაფრთხოების უფრო მაღალ დონეს წარმოადგენს და ძირითადად განსაკუთრებით კრიტიკულ სერვისებზე გამოიყენება, ისეთებზე როგორიცაა მაგალითად, ინტერნეტ ბანკი.

ავტორიზაციის საფეხურზე მოწმდება მომხარებლის უფლებები. მას შემდეგ, რაც სისტემა მომხარებელის მიერ მითითებულ სახელს და პაროლს შეადარებს საკუთარ ჩანაწერებს და იპოვნის დამთხვევას, ხდება უფლებების, როლების გადამოწმება აღნიშნული მომხმარებლისათვის. მაგალითად, ავტორიზებულ პირს შესაძლოა ქონდეს მხოლოდ ინფორმაციის წაკითხვის უფლება და არა რედაქტირების.

წვდომის კონტროლის ყველაზე ფართოდ გავრცელებულ მიდგომას – ფრეიმვორკს წარმაოდგენს „AAA" მოდელი, რომელიც აერთიანებს ავტენთიფიკაციას, ავტორიზაციასა და აღრიცხვას (authentication, authorization, accounting).

აღრიცხვა გულისხმობს მომხმარებლის მიერ მოთხოვნილი რესურსების რაოდენობის კონტროლს. უსაფრთხოების პოლიტიკის თანახმად, მომხმარებელს შესაძლოა დაუდგინდეს წვდომა მონაცემების ლიმიტირებულ რაოდენობაზე (დღეში, თვეში ან ნებისმიერი დროის მონაკვეთით). თუ მომხმარებელი მოინდომებს შეზღუდვის გადაჭარბებას, Accounting მექანიზმი მას ამის საშუალებას არ მისცემს.

შესაძლოა რისკი საერთოდ არ გამომდინარეობდეს ადამიანური არაკეთილსინდისიერებიდან და მას შემთხვევითობა ედოს საფუძვლად. ამის მაგალითია ტექნიკური საშუალების ხარვეზი, ან მონაცემების დაზიანება გადაცემისას საკომუნიკაციო საშუალებების შეფერხების გამო. შემთხვევითი დანაკარგების თავიდან ასაცილებლად, მონაცემებისა თუ ტექნიკური საშუალებების დუბლირება გამოიყენება.

1.4. საჯარო სექტორში კონფიდენციალური ინფორმაციის დაცვის ზოგადი მოდელი

ეფექტური დაცვის საინფორმაციო სისტემების დიზაინის შექმნის დროს უნდა დაისვას შემდეგი ამოცანები:

- კონფიდენციალობის დაცვა. კონფიდენციალობისუზრუნველყოფა მონაცემთა შენახვის, გადამუშავების ან საკომუნიკაციო არხებით გადაცემის დროს (კონფიდენციალობა – ინფორმაციას მახასიათებელი, რომელიც მდგომარეობს იმაში, რომ ინფორმაცია არ შეიძლება მიღებული იქნას არაუფლებამოსილი პირის მიერ ინფორმაციის შენახვის, დამუშავებისა და გადაცემის დროს);
- მთლიანობისუზრუნველყოფა.მთლიანობისუზრუნველყოფამონაცემთა შენახვის, გადამუშავების ან საკომუნიკაციო არხებით გადაცემის დროს.მთლიანობის დროს განიხილება ორი ასპექტი. პირველ რიგში, ეს არისარაუფლებამოსილი პირის უუნარობა შეცვალოს მონაცემები მათი შენახვის, დამუშავებისა და გადაცემის დროს. მეორე, ეს არის სისტემის მთლიანობა, რაც მდგომარეობს იმაში, რომ არც ერთი კომპონენტი ვერ იქნება წაშლილი, შეცვლილი;

- ხელმისაწვდომობის უზრუნველყოფა. მონაცემების ხელმისაწვდომო-ბის უზრუნველყოფა, რომლებიც ინახება ლოკალურ ქსელებში, ასევე მათი დროული დამუშავების და გადაცემის შესაძლებლობა. უზრუნველყოფაგულისხმობს, რომ მომხმარებელს აქვს შესაბამისი უფლებები გამოიყენოს რესურსები განსაზღვრული ვადით, დადგენილი წესით უსაფრთხოების პოლიტიკის შესაბამისად. ხელმისაწვდომობა მიზნად ისახავს სისტემის მუშა მდგომარეობაში შენარჩუნებას, რომელიც უზრუნველყოფს დროულ და ზუსტ ფუნქციონირებას.
- დაკვირვების უზრუნველყოფა. მიზნად ისახავს საშუალება მისცეს IT სისტემებს, ჩაიწეროს ნებისმიერი საქმიანობა, პასიური ობიექტი, თავიდან აიცილოს უსაფრთხოების პოლიტიკის ანგარიშვა-ლდებულების ქმედებები.
- გარანტიის უზრუნველყოფა. მოთხოვნებისკომპლექტი.რათა დადგინდეს ნდობის ხარისხი იმ ფაქტში, რომ:
    - ფუნქციური მოთხოვნები ნამდვილად შემუშავებულია და ხორციელდება სწორად;
    - მიიღოს დამცავი ღონისძიებები, როგორც ტექნიკური ისე ორგანიზაციული, სათანადო დაცვის სისტემების უზრუნველყოფა საინფორმაციო პროცესებისა და რესურსებისათვის;
    - აღეკვატური დაცვა პერსონალის და პროგრამული შეცდომების წინააღმდეგ;
    - აღეკვატური დაცვა სისტემაში განზრახ შეღწევის და მონაცემების გამოყენების წინააღმდეგ.

აღეკვატური ინფორმაციის დაცვა მოითხოვს შესაბამის კომბინაციას უსაფრთხოების პოლიტიკის, ორგანიზაციული უსაფრთხოების ზომების, ტექნიკური საშუალებებით დაცვის, მომხმარებვლების სწავლებას და გამოყენების ინსტრუქტირებას და უწყვეტი ოპერირების გეგმის უზრუნველყოფას.

ინფორმაციის დაცვის მიზანია შესაძლო ზემოქმედებით გამოწვეული ზიანის შემცირება, ასეთი ზემოქმედების პროგნოზირება და პრევენცია.

შესაბამისად, ინფორმაციული უსაფრთხოების კომპონენტებია:

- იმ ობიექტების განსაზღვრა, რომლებზეც შეიძლება იყოს გამიზნული საფრთხეები;
- არსებული და პოტენციური საფრთხეების განსაზღვრა;
- პოტენციური საფრთხის წყაროს განსაზღვრა;
- რისკის შეფასება;
- მეთოდები და საშუალებები მტრული გავლენის განსაზღვისთვის;
- მეთოდები და საშუალებები საფრთხისგან დასაცავად;
- მეთოდები და საშუალებები ინციდენტებზე რეაგირებისთვის.

პერსონალის არასწორი ქმედებებიდან გამომდინარე, არსებობს შემდეგი საფრთხეები:

1. ცუდი შესრულება. ძირითადი მიზეზი მუდმივი ჩარევები, უყურადღებობა და უდისციპლინობა. შესაძლო შედეგები–იზრდება ხარჯები და მომხმარებლის დაკარგვის ალბათობა. ამ შემთხვევაში, საკმაოდ გავრცელებულია უხეში დამოკიდებულება მომხმარებლის მიმართ:
2. არაკომპეტენტური პერსონალი უსაფრთხოების საკითხებში. ძირითადი მიზეზები– უპასუხისმგებლო დამოკიდებულება უსაფრთხოების საკითხებთან. უარყოფითი ეფექტი შესაძლოა საკმაოდ ფართომაშტაბიანი იყოს და შეტევის დროს მოიპოვოს წვდომა უმაღლეს პერსონებზე.
3. თანამშრომლების მიზანმიმართული ქმედებები. ყველაზე გავრცელებული მიზეზი– თანამშრომელთა უკმაყოფილება. უკმაყოფილება შეიძლება გამოწვეული იყოს ხელფასით, უფლებების დარღვევითა და შესაძლებლობების სათანადოდ შეუფასებლობით, რასაც შეიძლება ძალიან საშიში შედეგები მოყვეს. სტატისტიკით შეტევების 80%– ი,თანამშრომლების მიერ ხორციელდება.

განვიხილოთ კონფიდენციალური ინფორმაციის დაცვის ზოგადი მოდელი.

კონფიდენციალური ინფორმაცია შესაძლებელია იყოს ორი სახის კომერციული და პირადი.

კომერციული ინფორმაციები შესაძლოა მივაკუთნოთ:

- კომპანიის შემაჯამებელი ფინანსური ანგარიშები (ყოველთვიური, კვარტალური, წლიური,რამოდენიმე წლის);
- ბანკებთან საკრედიტო ხელშეკრულებები;
- ყიდვა–გაყიდვის ხელშეკრულებები;
- ინფორმაცია ბაზრებზე, წყაროებზე და მომგებიან პარტნიორებზე;
- მონაცემები კონკურენტების ძლიერი და სუსტი მხარეების შესახებ;
- შესრულება, ფინანსური თვალსაზრისით;
- ტექნოლოგიური საიდუმლოება;
- კონკურენტების მიერ მიღებული ზომები მათი მტრების წინააღმდეგ;
- მონაცემები პოტენციურ პარტნიორებზე;
- ინფორმაციას საქონლის შენახვის ,მდებარეობის, დროისა და მარშრუტების შესახებ;
- კომუნიკაცია და მენეჯმენტის შესაძლებლობები;
- მუდმივი მომხმარებლების გამოვლენა.

- პირადი ინფორმაცია შესაძლებელია იყოს:
- შემოსავლის წყარო;
- ინფორმაცია უფროსისა და მისი ოჯახის წევრების პირადი ცხოვრების შესახებ;
- ინფორმაცია ბიზნესისა და პირადი საქმიანობის გრაფიკის, შეხვედრებისა და მისამართების შესახებ;
- ინფორმაცია ფინანსური კეთილდღეობის შესახებ;
- ინფორმაცია ადამიანის სუსტი მხარეების შესახებ;
- ინფორმაცია ცუდი ჩვევების შესახებ;
- ინფორმაცია სექსუალური ორიენტაციის შესახებ;
- ინფორმაცია მეგობრებზე;
- მონაცემებიდასვენებისადგილების,მეთოდებისადაგადაადგილებისმარშრუტების შესახებ;
- ინფორმაციაანაბარზე;
- საცხოვრებელი ადგილი;

- მრუშობა;
- პრობლემა მამებსა და შვილებს შორის.

დღეს არსებული დაცვის მექანიზმები მიმართულია ინფორმაციული უსაფრთხოების უზრუნველყოფის ცალკეული ასპექტების რეალიზაციაზე,რაც ვერ უზრუნველყოფს დაცვის სისტემის მართვის ანალიზისა და სინთეზის ამოცანების კომპლექსურ გადაწყვეტას და ოპტიმალური საპროექტო გადაწყვეტების მიღებას და დაცული ინფორმაციული სისტემებისა და ბაზების შექმნას. აქედან გამომდინარე, ინფორმაციული ტექნოლოგიების დაცვის საკითხები, სულ უფრო სერიოზულ ყურადღებას ითხოვს.

დაცვის ტექნოლოგიისადმი ძირითადი მოთხოვნაა, დაცვის სისტემისა და მონაცემთა ბაზების სახით ინტეგრირებული,მემკვიდრეობითობისა და ოპერაციების თანმიმდევრობის ორგანიზებული ინფორმაციული პროდუქტების შექმნა.

ამჟამად არსებული მეთოდები და ინსტრუმენტალური საშუალებები, მიმართულია მონაცემების კონფიდენციალობისა და მთლიანობის ურღვევობის უზრუნველყოფაზე.მონაცემთა ბაზებში ინახება მრავალფეროვანი ინფორმაცია არა მარტო წარმოდგენის ფორმის თვალსაზრისით, არამედ კონფიდენციალობის დონის მიხედვითაც.როგორც კორპორაციული ინფორმაციული საერთო შეზღუდული გამოყენების რესურსების მუქარების ანალიზმა გვიჩვენა, ინფორმაციული დაცვის სისტემების ორგანიზაციისათვის აუცილებელია დამუშავდეს ინფორმაციული ტექნოლოგია, რომელშიც გათვალისწინებული იქნება შეზღუდული მოხმარების დოკუმენტებთან მუშაობის მოთხოვნები. ეს მოთხოვნები,როგორც წესი, სახელმწიფოში, შესაბამისი კანონით ან კანონებით და სხვა ნორმატიული დოკუმენტებით უნდა იყოს განსაზღვრული.

ტექნოლოგიამ უნდა უზრუნველყოს ინფორმაციასთან დაშვების მრავალდონიანი კონტროლი, კრიპტოგრაფიული დაცვა, სხვადასხვა კონფიდენციალობის მქონე ინფორმაციის მაღალი საიმედობა.

საკომუნიკავიო არხებით დაცვის წარმოდგენილი მოდელის ეფექტურობა უნდა ეფუძნებოდეს ოპტიმალურ ინფორმაციულ უსაფრთხოებას.

მონაცემთა მთლიანობის კონტროლი ხორციელდება ხარისხის შემდეგი კრიტერიუმების მიხედვით:

ა)სისრულე (მონაცემთა სტრუქტურის სრული აღწერის შემოწება);

ბ)არაწინააღმდეგობრიობა (მონაცემებს შორის ლოგიკური კავშირების შემოწმება,ჭარბი და წინააღმდეგობრივი აღწერების გამოვლენა, მნიშვნელობათა დიაპაზონის საზღვრების და თვით მნიშვნელობების დამაჯერებლობის კონტროლი);

გ)აქტუალურობა (ერთდროული და დროული ცვლილებების შეტანის კონტროლი).

მთლიანობის კონტროლის მეთოდები და საშუალებები ეფუძნება შესატანი მონაცემების ანალიზს და მონაცემების მიმართ მოთხოვნების აღწერას.

დასმული ამოცანების გადასაწყვეტად გამოყენებულ იქნა მონაცემთა ბაზების და ინფორმაციული სისტემების თეორიის,სისტემური ანალიზის, მათემატიკური ლოგიკის, სიმრავლეთა თეორიის, აგრეთვე პროგრამირების ტექნოლოგიის მეთოდები და მიდგომები და დაშვების კონტროლთან დაკავშირებული გადაწყვეტილებების მეთოდები.

მრავალდონიანი დაცვის სისტემის ბირთვს წარმოადგენს მოთხოვნების დამუშავების მონიტორი (მდმ), რომელიც ამოწმებს მომხმარებლის ყოველ მიმართვას მონაცემებთან ან პროგრამებთან, თუ რამდენად შეესაბამება ის იმ მოქმედებების სიას, რომელიც დაშვებულია მომხმარებლისათვის. მდმ კონცეფციის გამოყენება ლოგიკური დაშვების კონტროლის მექანიზმების დამუშავებისას, საშუალებას იძლევა თავიდან იქნას აცილებული გაურკვევლობის ელემენტები, პირობების და შიდა შეზღუდვების შესრულების მეშვეობით, როდესაც დარეგისტრირებულ პროცესებს და ფიზიკურ პირებს შეუძლიათ იმის შესრულება, რისი უფლებაც აქვთ.

დამუშავებულია გაფართოებული სია: ძირითადი წესებისა მოთხოვნების ნებართვაზე, დაშვების უფლებამოსილების კონტროლზე და სისტემის მდგომარეობის შეცვლაზე.

კონფიდენციალური ინფორმაციის შენახვის სანდოობის ასამაღლებლად შემოთავაზებულია მატრიცის ბირთვის კრიპტოგრაფიული დაცვა. აღნიშნული

მოდელი, რომელიც რეალიზებულია დაცვის სუბიექტების და ობიექტების ხისებრ სტრუქტურაზე.

თავი 2. ინფორმაციული რისკების მართვის თანამედროვე სისტემები

2.1. უდიტის როლი რისკების ეფექტურად მართვის პროცესში

თანამედროვე კომპანიები აუდიტს განიხილავს არა მხოლოდ ფინანსური ანგარიშების შემოწმებისთვის, არამედ რისკების მართვის, კონსალტინგის, ფინანსური სტაბილურობის ანალიზის, საგადასახადო კონსულტირების და შიდა სისტემის კონტროლისთვის.

კომპიუტერული მონაცემების დამუშავებისას წარმოქმნილი პოტენციური საშიშროებიდან შეგვიძლია გამოვყოთ შემდეგი რისკები:

- შესამოწმებელი ეკონოკური სუბიექტის აპარატული ან პროგრამულ უზრუნველყოფასთან დაკავშირებული რისკები;
- პერსონალის კვალიფიკაციასთან დაკავშირებული რისკები;
- კომპიუტერული მონაცემის აღრიცხვის დაცვის მექანიზმების უქონლობასთან დაკავშირებული რისკები;
- საწყისი მონაცემების შეყვანის კონტროლის არარსებობასთან დაკავშირებული რისკები;
- ინფორმაციის შენახვასა და დაცვასთან დაკავშირებული რისკები;

ზემოთ, ჩამოთვლილ რისკებთან დაკავშირებულ საკითხებს ინფორ-მაციული ტექნოლოგიების აუდიტი ემსახურება.

ინფორმაციული ტექნოლოგიების აუდიტი მსოფლიოში ფართოდ გავრცელებული პრაქტიკაა, თუმცა საქართველოში მხოლოდ ბოლო წლების

მანძილზე დაიწყო ფეხის მოკიდება. მსგავსი ტიპის აუდიტორული მომსახურება, ისევე როგორც ფინანსური ან სხვა სახის, საკმაოდ მაღალ ხარჯებთანაა დაკავშირებული. ქართული კომპანიების დიდ ნაწილს კი არ აქვს მსგავსი მომსახურებით სარგებლობის საშუალება, რადგან მათი შემოსავალი მწირია და ხელფასების დარიგებასა და საოპერაციო საქმიანობაზეა გათვლილი. მიუხედავად ამისა უკანასკნელი რამდენიმე წლის მანძილზე IT აუდიტმა საკმაოდ სწრაფად დაიწყო განვითარება.

დღეისთვის მსხვილ კომპანიათა უმეტესობა იყენებს მსგავს მომსახურებას. მაგალითად, სამთავრობო სტრუქტურების ფინანსურ სექტორში ყოველ წლიურად ატარებენ ინფორმაციული ტექნოლოგიების აუდიტს.

სისტემის შემოწმებისას, აუდიტის ძირითადი მეთოდიკა უნდა შეიცავდეს სამ ძირითად ასპექტს – აუდიტის მუშაობა შიდა კონტროლის სისტემაში, აუდირებული სუბიექტის კომპიუტერული მონაცემების დამუშავების შეფასება და შიდა კონტროლის რისკების შეფასება.

პრაქტიკულად, ამ მიზნის რეალიზაცია შესაძლებელია სხვადასხვა პროცედურების ჩატარებით– დაკვირვება, ინსპექტირება და გამოკითხვა.

დაკვირვება – ყველაზე მარტივია შემოთავაზებული მეთოდებიდან, ვინაიდან ის არ საჭიროებს განსაკუთრებულ უნარჩვევებს. თუმცა ეს მეთოდი შეიძლება იყოს გამოყენებული დოკუმენტირების შეზღუდული რაოდენობის ელემენტებში. მაგალითად, ამ მეთოდის საშუალებით არ შეიძლება სრულად იქნას შესწავლილი თანამშრომლების მუშაობის ხარისხი.

დოკუმენტაციის ინსპექტირება – მეთოდი, რომელიც მოითხოვს აუდიტისადმი გარკვეულ უნარ-ჩვევებს, რადგან გულისხმობს არა მხოლოდ მექანიკურ გადატანას ერთი დოკუმენტიდან მეორეზე, არამედ რეგლამენტების რელევანტობის შეფასებას. მაგალითად, აუდიტორს შეუძლია შეაფასოს საკონტროლო შემოწმებების სიხშირე და ხარისხი, წარმოდგენილი ანგარიშების სიზუსტე და შემოწმების დროს მიღებული გადაწყვეტილებების ადეკვატურობა.

გამოკითხვა შეიძლება ჩატარდეს როგორც ხელმძღვანელებს შორის ასევე აუდირებული კომპანიის სხვა თანამშრომლებში. გამოკითხვის დროს აუდიტორს ეძლევა საშუალება შეაფასოს და მიიღოს ინფორმაცია იმ სფეროებში, სადაც ჯერ არ იყო შეფასებული და განხილული კომპიუტერული მონაცემები.

ტრადიციული, აღნიშნული მეთოდების გარდა (დოკუმენტაციის ინსპექტირება, წერილობითი ან ზეპირი გამოკითხვა) აუდიტორს შეუძლია გამოიყენოს ისეთი მეთოდი როგორიცაა კონცეპტუალური კავშირების მეთოდი.

კონცეპტუალური კავშირების მეთოდის გამოყენებისას (concept mapping), აუდიტს შეუძლია ვიზუალურად წარმოადგინოს სისტემის შიდა კონტროლი – გარემოს ურთიერთქმედებები. ეს მეთოდი წარმოადგენს კავშირის შემოწმებას მოვლენებსა და ობიექტებს შორის, რომლებიც გაერთიანებულია საერთო მიზნით.

კონცეპტუალური კავშირების მეთოდების გამოყენება საშუალებას იძლევა დედუქციის მეთოდით მივიღოთ საჭირო პროცესების სრულად შეცნობის სიღრმე შიდა კონტროლის ეკონომიკური ობიექტის შემოწმებისას.

შიდა კონტროლის გარემოს აღწერის დროს, აუდიტორს ასევე შეუძლია მიმართოს რანჟირების მეთოდს. რანჟირება გულისხმობს პრიორიტეტების გამოყოფას. მაგალითად, ბიზნესის მასშტაბიდან გამომდინარე, ცალკეული სახელფასო სარგებელი შეიძლება იყოს განსხვავებული, ამიტომ აუდიტორმა უნდა გაითვალისწინოს ამ ელემენტის მნიშვნელობა და დეტალურად შეისწავლოს ეს მონაცემები.

რანჟირება, აუდიტორს აძლევს საშუალებას გააკეთოს აქცენტი ყველაზე მნიშვნელოვან ელემენტებზე, უფრო ყურადღებით განიხილოს ეს ელემენტები და შეაფასოს ექსპერტების მოწვევის საჭიროება.

პრიორიტეტების გამოყოფა შემოწმებისას, აუდიტორს აძლევს საშუალებას შეამციროს შეცდომების დაშვების რისკი. რაც იმას ნიშნავს, რომ აუდიტორული პროცესების შესრულებისას, დაშვებული შეცდომები არ უნდა აღემატებოდეს ნორმას.

მიუხედავად შერჩეული მეთოდისა, რომელიც გამოყენებული იქნება საინფორმაციო სისტემის და მონაცემთა ბაზის შესამოწმებლად – პროცესული თუ ელემენტარული, აუდიტორმა უნდა გამოყოს შემდეგი ჯგუფები:

- საწარმოს მდგომარეობის შესწავლის და ანალიზის მეთოდები;
- საწარმოს წარმოდგენის გრაფიკული მეთოდები;

ეკონოკიკური სუბიექტის მდგომარეობის და ანლიზის მეთოდები შეიძლება იყოს შემდეგი:

- ზეპირი და წერილობითი გამოკითხვა;

- წერილობითი ანკეტირება;
- დაკვირვება;
- შეფასება.

განვიხილოთ მეთოდი – ინფორმაციული პროცესების ანალიზი. აღნიშნული რთული მრავალმხრივი მიდგომაა, რომელიც შეიცავს შემდეგ უფრო კონკრეტულ ანალიტიკურ პროცედურებს:

- ინფორმაციული პროცესების მოდელირება;
- სტრუქტურული პროექტირება;
- მოდულების დეკომპოზიცია;
- ინფორმაციული პროცესის მოდულების ანალიზი;
- ეფექტურობის ანალიზი .

ანალიზის ხარისხის გეგავლენა ფინანსურ ანგარიშებზე, თავის მხრივ იყოფა: მოდულების პირდაპირი და ირიბი ექსპოზიციით. აღსანიშნავია, რომ არ არსებობს საინფორმაციო სისტემების ისეთი მოდულები, რომლებიც გეგავლენას არ ახდენს ფინანსურ ანგარიშებზე, ვინაიდან ამ მოდულის მეშვეობით აისახება მთელი საწარმოს საქმიანობა.

ანალიზის ჩატარებისთვის მოდულის ასარჩევად, აუდიტორი ითვალისწინებს საჭიროების დროის ხარჯის დონეს, განსაკუთრებით თუ მოდული ირიბად გავლენას ახდენს ფინანსურ აღრიცხვაზე. სს-ს ელემენტებს შეუძლია ჰქონდეს როგორც მნიშვნელოვანი ასევე სუსტი გეგავლენა ფინანსურ აღრიცხვაზე, რაც ასევე ეხება ირიბი ელემენტების გეგავლენას.

ინფორმაციული სისტემების მუშაობის მნიშვნელოვანი მაჩვენებელია ფიქსატორების მოწყობილობების ქონა, კონტროლის სხვადასხვა წერტილებში, რომლებიც იძლევა საშუალებას დააფიქსიროს შემდეგი მაჩვენებლები:

- პროცესის შესრულების საშუალო დრო;
- გარკვეულ მონაკვეთში პროცესის საშუალო ღირებულება;
- შეწყვეტილი პროცესების რაოდენობა;
- დასრულებული პროცესების რაოდენობა;
- დაყოვნებული პროცესების შესრულების რაოდენობა;

კონტროლის წერტილები ხშირად მდებარეობს ინტერფეისის სხვადსხვა დეპარტამენტში, რომლებიც უკავშირდება ერთი პროცესის შესრულებას და

რომლის განხორციელება ხდება სს-ში. კონტროლის წერტილები, აუდიტორს საშუალებას აძლევს შეამციროს შეუსაბამობის ძიება ანალიზის შესრულების დროს.

ევრისტიკული ანალიზის მეთოდების გამოყენება შესაძლებელია იმ შემთხვევაში, როდესაც აუდიტორი დგება ინფორმაციის უკმარისობის ან ანალიზის პრობლემის წინაშე, რომელიც მოითხოვს მნიშვნელოვან ცოდნას.

სხვადასხვა ევრისტიკული ანალიზის მეთოდების გამოყენების დროს, შეთავაზებულია გამოიყენოს ანალოგიის მეთოდი, გამოკითხვის მეთოდი, საკონტროლო შეკითხვების მეთოდი, ტესტირება, ან გასაუბრება და ასევე გამოცდა.

ანალოგიის მეთოდი ეფუძნება ექსპერტების წარსულ გამოცდილებას, საინფორმაციო სისტემის ანალოგიური ანალიზის განხორციელების დროს. ამ შემთხვევაში, დიდი მნიშვნელობა აქვს მასალებს, რომლებშიც აღწერილია ანალოგიური სისტემები და ასევე, ექსპერტების გამოცდილება.

გამოკითხვის ან საკონტროლო ტესტირების მეთოდი, საჭიროებს ექსპერტების ცოდნას. ტესტირების სტრუქტურა უნდა იყოს ყურადღებით მომზადებული და ზუსტად ასახავდეს მოცემულ თემას. ამ შემთხვევაში აუდიტორს შეუძლია გამოიყენოს თავისუფალი ან ფორმალური კითხვარი. თავისუფალი ფორმატი გულისხმობს ექსპერტების სრულ, ვრცელ პასუხებს და უფრო რთულია ანალიზის გაკეთების დროს. ფორმალური კითხვარი ითვალისწინებს უკვე მოცემულ, რამოდენიმე პასუხს ასარჩევად.

ტესტირების მეთოდი ტარდება კითხვარის შევსებით, რომელშიც:

- წინადადება არ უნდა იყოს ორაზროვანი;
- უნდა იყოს გამოყენებული საერთო ტერმინოლოგია;
- უნდა უზრუნველყოფდეს ერთიან და არაორაზროვან ტესტირების შედეგებს.

გასაუბრება თავის მხრივ გულისხმობს ინტერპერსონალურ ურთიერთობას, ანუ დიალოგს რესპონდენტსა და ინტერვიუერს შორის. ამ მეთოდის დადებითი მხარე არის მომზადებული კითხვების მოდიფიკაციის შესაძლებლობა გასაუბრების დროს.

საკონტროლო კითხვების მეთოდი ეფუძნება ცხრილის ფორმის ანკეტების გამოყენებას, სადაც წინასწარ მითითებულია პასუხები. ექსპერტის ამოცანაა, ამოირჩიოს სწორი პასუხი. კითხვები ასეთი ანალიზის დროს არის ობიექტის შეფასების პარამეტრები, პასუხები კი – პარამეტრების მნიშვნელობა.

ინფორმაციული სისტემის მოდულის ანალიზის დროს, აუდიტორი შეიძლება დადგეს ისეთი პრობლემის წინაშე, რომელიც ტრადიციული ანალიტიკური მეთოდები არ იძლევა პრობლემის საწყისის იდენტიფიკაციის საშუალებას. ასეთ შემთხვევაში, აუდიტორს შეუძლია გამოიყენოს „ტვინის შტურმის“ მეთოდი– შექმნილი სიტუაციის ანალიზისთვის, აუდიტორები იყენებენ სხვადასხვა მეთოდურ რეკომენდაციებს, სახელმძღვანელოებს (სტანდარტებს).

განვიხილოთ, აუდიტის როლის საკითხი, რისკების ეფექტურად მართვის პროცესში

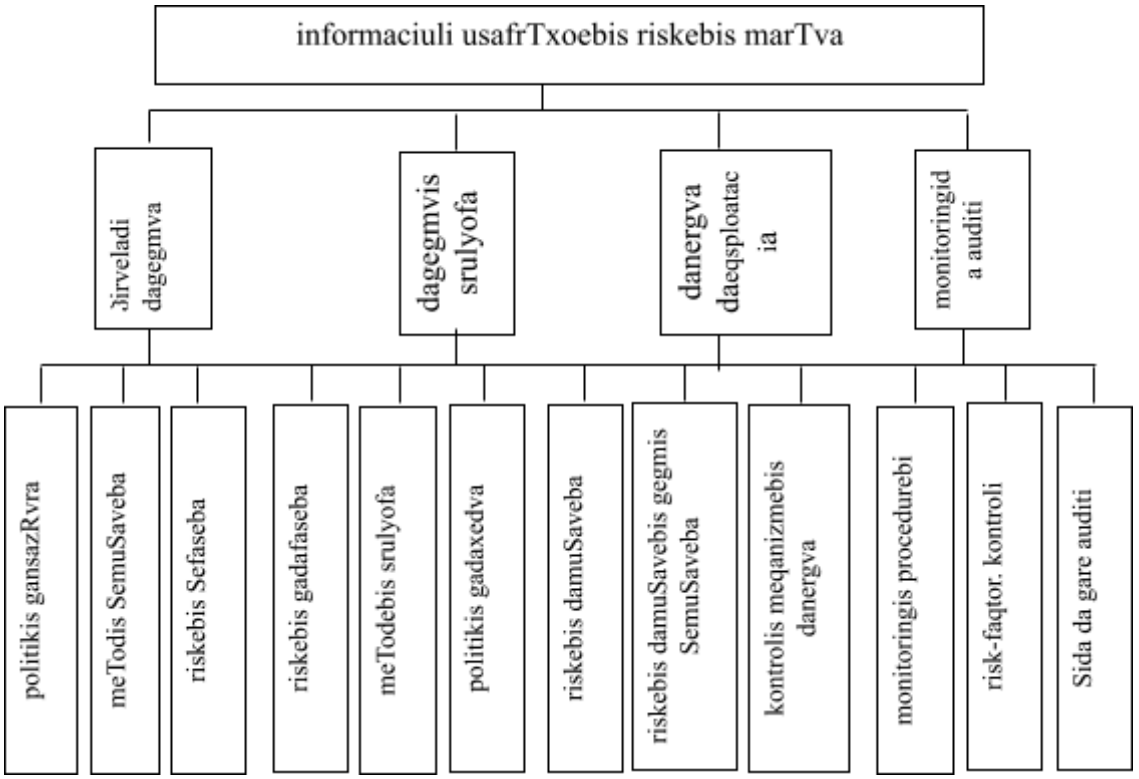
საწარმოს საინფორმაციო სისტემამ სწრაფი ცვლილებები განიცადა, რასაც შედეგად მოჰყვა საინფორმაციო ოპერაციებთან დაკავშირებული კომპლექსური რისკების გაზრდა. აქედან გამომდინარე, გაჩნდა საწარმოს მართვის თანამედროვე სტრუქტურის შექმნის აუცილებლობა, რაც გულისხმობს საწარმოს მენეჯმენტის, პოლიტიკის და პროცედურების აქტიურ ზედამხედველობას, რისკების შეფასებას და დადგენას, მათი მონიტორინგის დაწესებას, შიდა კონტროლის სისტემების დანერგვას.

დაგეგმვის ეტაპზე უნდა განისაზღვროს რისკების მართვის პოლიტიკა და მეთოდოლოგია, ასევე მოხდეს რისკების შეფასება, რომელიც მოიცავს აქტივების ინვენტარიზაციას, საფრთხეებისა და დაუცველი ადგილების პროფილების შედგენას, კონტრზომების ეფექტურობისა და პოტენციური ზარალის შეფასებას, დარჩენილი რისკების დასაშვები დონის განსაზღვრას.

რეალიზაციის ეტაპზე რისკები უნდა დამუშავდეს და დაინერგოს მართვის მექანიზმები, რომელიც გათვლილია რისკების მინიმიზებაზე.

შემოწმების ეტაპზე თვალყური უნდა მიედევნოს მართვის მექანიზმების ფუნქციონირებას, გაკონტროლდეს რისკ-ფაქტორების (როგორიცაა აქტივები, საფრთხეები, დაუცველი ადგილები) ცვლილება, ჩატარდეს აუდიტი და სხვადასხვა მაკონტროლებელი პროცედურები.

ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი შეიძლება დავყოთ ოთხ ეტაპად:



ნახ. 1 ინფორმაციული უსაფრთხოების რისკების მართვის სისტემა

რისკების მართვა სარგებლობას მოუტანს როგორც საწარმოს გედამხედველობის განმახორციელებელ პირებს. რისკების ეფექტიანად მართვით საწარმოს მენეჯმენტს შეუძლია მიიღოს ინფორმაცია მომავალში საწარმოს შესაძლო გარალის შესახებ, ინფორმაციის ხელმისაწვდომობის საფუძველზე გააუმჯობესოს სისტემური გადაწყვეტილებების მიღების მეთოდები და პროცესები, გამოიყენოს როგორც საწარმოს მუშაობის შეფასების უფრო ზუსტი ბაზა, ისე შეაფასოს საწარმოს შედარებით კომპლექსური ინსტრუმენტებისა, თუ ბიზნესსაქმიანობისათვის დამახასიათებელი რისკები და შექმნას რისკების მართვის ისეთი ჯანსაღი ინფრასტრუქტურა, რომელიც საწარმოს კონკურენტუნარიანობას გააძლიერებს.

გედამხედველობის თვალსაზრისით, რისკების მართვის გამოყენება დააჩქარებს საწარმოს შესაძლო იმ გარალის შეფასებას, რომელმაც შესაძლოა ნეგატიური გეგავლენა მოახდინოს საწარმოს მოგებაზე, ამიტომ აუცილებელია,

რომ საწარმოში შეიქმნას რისკების მართვის სტრუქტურა და მასზე აწყობილი რისკების მართვის სისტემა.

საწარმოს საქმიანობის არსიდან გამომდინარე, როგორც მოსალოდნელი, ისე მოულოდნელი რისკი არის პოტენციური მოვლენა, რომელმაც შეიძლება ნეგატიური ზეგავლენა იქონიოს საწარმოს შემოსავალზე და საერთოდ მოგებაზე. იმისათვის, რომ განხორციელდეს რისკის მართვის პროცესი, საწარმომ უპირველეს ყოვლისა, ზუსტად უნდა განსაზღვროს რისკები, აღიაროს და გაერკვეს მისთვის დამახასიათებელ ყველა რისკში, რომელმაც შეიძლება თავი იჩინოს მის მიერ ახალი საქმიანობის განხორციელებისას, მათ შორის შეიძლება იყოს ნებისმიერი რისკი, რომელიც მასთან დაკავშირებულ, თუ სხვა მონათესავე საწარმოებს ახასიათებს.

რისკების ზუსტად განსაზღვრის შემდეგ, საწარმომ თანმიმდევრობით უნდა განახორციელოს მისი შეფასება, მონიტორინგი და კონტროლი. რისკების შეფასების მიზანია, რომ საწარმომ შეძლოს მისი ბიზნეს– საქმიანობისათვის დამახასიათებელი რისკების გაანგარიშება, რათა განისაზღვროს რისკების გავლენა შემოსავლებზე.

ყოველივე ზემოთქმულიდან გამომდინარე უნდა იქნას შემუშავებული რისკების მართვის სწორი პოლიტიკა. ის წარმოადგენს წერილობით დოკუმენტს და უნდა შეესაბამებოდეს საწარმოს ხედვას, მიზნებს და სტრატეგიულ გეგმას. ის უფრო მეტად ფოკუსირებული უნდა იყოს საწარმოს ოპერაციებისთვის დამახასიათებელ რისკებზე. რისკის მართვის პოლიტიკა არის რისკის მართვის სტრატეგიათა გაერთიანება.

აუდიტორული საქმიანობის განვითარების თანამედროვე ეტაპი დაკავშირებულია აღრიცხვების განსახორციელებლად თანამედროვე პერსონალური კომპიუტერებისა და საბუღალტრო პროგრამების გამოყენებასთან, რაც გულისხმობს აუდიტორული მოქმედებების გავრცელების აუცილებლობას შემოწმების სფეროზე.

2.2. ინფორმაციული უსაფრთხოების აუდიტი

ინფორმაციული უსაფრთხოების (იუ) აუდიტის, ქვეშ იგულისხმება ორგანიზაციის იუ-ს მიმდინარე მდგომარეობის ობიექტური, ხარისხობრივი და რაოდენობრივი შეფასების კრიტერიუმებისა და მაჩვენებლების შესაბამისად, უსაფრთხოების უზრუნველყოფის ყველა ძირითად: ნორმატიულ-მეთოდოლოგიურ, ორგანიზაციულ- მმართველობით და პროცედურულ-ტექნიკურ დონეზე, განსაზღვრული სისტემური პროცესი.

ორგანიზაციის იუ-ს კვალიფიციურად ჩატარებული აუდიტის შედეგები საშუალებას იძლევა შეიქმნას, ეფექტიანობისა და დანახარჯების მიხედვით ოპტიმალური, ინფორმაციული უზრუნველყოფის სისტემა (იუუს). ის წარმოადგენს,იუ-ს მართვის მოდელის საფუძველზე გაერთიანებულ, პროცედურულ, ორგანიზაციულ და სამართლებრივ მონაცემთა და ტექნიკურ საშუალებათა კომპლექსს.

აუდიტის ჩატარების საფუძველზე შესაძლებელია მიღებულ იქნას, როგორც ხარისხობრივი, ასევე რაოდენობრივი შეფასება. ხარისხობრივი შეფასებისას, მაგალითად, შეიძლება მიღებულ იქნას პროგრამულ-აპარატურული უზრუნველყოფის, მათი კვალიფიკაციით უსაფრთხოების სამ-დონიანი სკალის მიხედვით, სუსტი (მოწყვლადი) ადგილების ჩამონათვალი: მაღალი, საშუალო, დაბალი. ხარისხობრივი შეფასებები უმეტესად გამოიყენება ორგანიზაციის აქტივებთან დაკავშირებული მუქარების შესაფასებლად, რომლებსაც წარმოშობს უსაფრთხოების მუქარები. რაოდენობრივი შეფასებები შეიძლება იყოს,მაგალითად, რისკის ღირებულება, რისკის ალბათობა, რისკის ზომა და ა.შ.

აუდიტის ობიექტურობას უზრუნველყოფს ის გარემოება, რომ იუ-ს მდგომარეობის შეფასება ხორციელდება სპეციალისტების მიერ განსაზღვრული მეთოდიკის საფუძველზე,რომელიც საშუალებას იძლევა ობიექტურად გაანალიზდეს იუ-ს ყველა მდგენელი.

მიუხედავად იმისა , რომ საერთო აუდიტი შესაძლებელია ჩატარდეს მოწვეული, სპეციალიზირებული ფირმების საშუალებით- იუ-ის შიდა აუდიტი ორგანიზაციამ, აუცილებლად საკუთარი ძალებით უნდა ჩაატაროს, მაგალითად, უსაფრთხოების ადმინისტრატორების მეშვეობით.

ტრადიციულად, გამოყოფენ აუდიტის სამ ეტაპს, რომლებიც განსხვავდება იუუს გასაანალიზებელი კომპონენტებითა და მიღებული შედეგებით, როგორიცაა:

–აქტიური აუდიტი;

–ექსპერტული აუდიტი;

–იუ–ს სტანდარტებთან შესატყვისობის აუდიტი.

ა)აქტიური აუდიტი

აქტიური აუდიტი გულისხმობს იუ–ს გარკვეულ ქვესისტემებს, რომლებიც განეკუთვნება პროგრამულ–ტექნიკურ დონეს, დაცულობის გამოკვლევას. მაგალითად, აქტიური აუდიტის ვარიანტი, რომელსაც ეწოდება ტესტი შეღწევაზე (PENETRATION TEST), გულისხმობს გამოკვლეულ იქნას ქსელური ურთიერთმოქმედებების დაცვის ქვესისტემა. აქტიური აუდიტი მოიცავს:

- იუ–ს ქვესისტემის მიმდინარე არქიტექტურის და ელემენტების მომართვის ანალიზს;
- პასუხისმგებელი და დაინტერესებული პირებისგან ინტერვიუს მიღებას;
- ინსტრუმენტალური შემოწმების ჩატარებას, რომელიც მოიცავს იუ–ს განსაზღვრულ ქვესისტემებს.

იუ–ს ქვესისტემების არქიტექტურისა და ელემენტების მომართვას აწარმოებენ სპეციალისტები, რომლებსაც გააჩნიათ საკმარისი ცოდნა კონკრეტულ ქვესისტემებში, რომლებიც წარმოდგენილია გამოსაკვლევ სისტემაში, აგრეთვე სისტემური ანალიტიკოსები, რომლებიც გამოავლენენ შესაძლო ნაკლს ქვესისტემების ორგანიზაციაში. ამ ანალიზის შედეგს წარმოადგენს გამოკითხვის ფურცლებისა და ინსტრუმენტული ტესტების ნაკრები.

გამოკითხვის ფურცლები გამოიყენება ავტომატიზებული სისტემის ადმინისტრირებაზე პასუხისმგებელი პირისგან ინტერვიუს მიღების პროცესში, რათა მიღებულ იქნას ავტომატიზებული სისტემის სუბიექტური მახასიათებლები, მიღებული საწყისი მონაცემების დასაზუსტებლად და ზოგიერთი ზომების იდენტიფიკაციისთვის, რომლებიც რეალიზებული იყო იუუს ფარგლებში, მაგალითად, გამოკითხვის ფურცლები შეიძლება შეიცავდეს კითხვებს, რომლებიც დაკავშირებულია პაროლების შეცვლისა და დანიშვნის პოლიტიკასთან, ავტომატიზებული სისტემების საციცოცხლო ციკლთან და მისი ცალკეული

ქვესისტემების კრიტიკულობაზე,ავტომატიზებული ინფორმაციული სისტემებისთვისა (აის) და მთლიანად ორგანიზაციის ბიზნესპროცესებზე.

გამოკითხვის პარალელურად, ხორციელდება ინსტრუმენტალური შემოწმებები (ტესტირება), რომლებიც შეიძლება მოიცავდეს შემდეგ ღონისძიებებს:

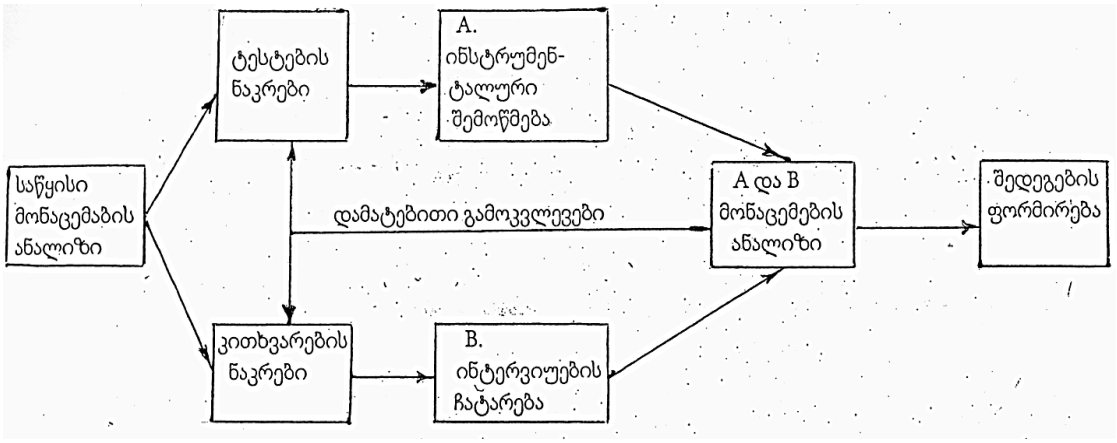
- ნაგებობის, სათავის ვიზუალური დათვალიერება, ნაგებობაში დაშვების კონტროლის სისტემის გამოკვლევა;
- წარმოდგენილ საწყის მონაცემებთან რეალური კონფიგურაციების შესატყვისობის შემოწმება;
- სპეციალური პროგრამული უზრუნველყოფით ქსელის რუქის მიღება;
- დაცულობისსკანერების გამოყენება (როგორც უნივერსალურობის, ასევე სპეციალიზირებულების);
- შეტევების, რომლებიც იყენებენ სისტემის მოწყვლადობების (სუსტი ადგილების) მოდელირება;
- რეაქციების არსებობის გამოვლენა მოქმედებებზე, რომლებსაც ავლენს შეტევების აღმომჩენი და მათზე რეაგირების მექანიზმები.
- „შავი ყუთის“ მოდელი–აუდიტორს არ გააჩნია არანაირი აპრიორული ცოდნა საკვლევ აის–ზე. მაგალითად, გარე აქტიური აუდიტის ჩატარებისას (ანუ სიტუაციაში, როდესაც ხდება ბოროტმზრახველის მოქმედებების მოდელირება, რომელიც იმყოფება საკვლევი ქსელის გარეთ);
- „თეთრი ყუთის“ მოდელი–აუდიტორს გააჩნია სრული ცოდნა საკვლევი ქსელის სტრუქტურაზე. მაგალითად,აუდიტორს შეიძლება გააჩნდეს საკვლევი ქსელის სეგმენტების რუქები, დიაგრამები და დანართის სიები. აღნიშნული მოდელის გამოყენება არასრული სახით ახდენს ბოროტგანმზრახველის იმიტირებას, მაგრამ საშუალებას იძლევა წარმოდგენილ იქნას „უარესი“ სცენარი,როდესაც შემტევს გააჩნია სრული ცოდნა ქსელის შესახებ;
- „ნაცრისფერი ყუთის“ მოდელი – აუდიტორი, ახდენს შიდა მომხმარებლების იმიტირებას, რომელსაც გააჩნია ქსელში დაშვება გარკვეული უფლებამოსილებით. აღნიშნული მოდელი საშუალებას

იძლება შეფასდეს რისკი, რომელიც დაკავშირებულია შიდა მუქარებთან, მაგალითად, კომპანიის არასანდო თანამშრომლებთან.

აუდიტორმა ყოველი ტესტი, ცოდნის მოდელი, რომელიც გამოიყენება ტესტში და ტესტის შესაძლო ნეგატიური შედეგები, უნდა შეათანხმოს პირებთან, რომლებიც დაინტერესებულნი არიან აის-ის უწყვეტი მუშაობით.

ინსტრუმენტული შემოწმების შედეგების მიხედვით ხორციელდება წინასწარი ანალიზის შედეგების გადახედვა და შესაძლოა, მოხდეს დამატებითი გამოკვლევების ორგანიზება.

აქტიური აუდიტის შედეგების მიხედვით იქმნება ანალიზური ანგარიში, რომელიც მოიცავს იუ-ს ტექნიკური ნაწილის მიმდინარე მდგომარეობის აღწერას, აის-ში აღმოჩენილი მოწყვლადი ადგილების სიას მათი კრიტიკულობის შეფასებით და რისკების გამარტივებული შეფასების შედეგებს, რომელიც მოიცავს დამრღვევის მოდელს და მუქარების მოდელს. დაატებით შეიძლება დამუშავებულ იქნას იუუს ტექნიკური ნაწილის მოდერნიზაციის სამუშაოების გეგმა, რომელიც შედგება რისკების დამუშავების რეკომენდაციების ჩამონათვალისგან.



ნახ. 2 იუ-ს აქტიური აუდიტის ჩატარების სქემა

ექსპერტული აუდიტის დანიშნულებაა მოხდეს იუ-ს მიმდინარე მდგომარეობის შეფასება ნორმატიულ-მეთოდოლოგიურ, ორგანიზაციულ-მმართველობით და პროცედურულ დონეებზე. ექსპერტული აუდიტი, უმეტეს შემთხვევებში, ხორციელდება მოწვეული აუდიტორების მიერ.

ორგანიზაცია- აუდიტორის თანამშრომლები, დამკვეთის წარმამადგებლებთან ერთად, ატარებენ შემდეგი სახის სამუშაოებს:

- აის-ის შესახებ საწყისი მონაცემების შეგროვება-ეს მონაცემებია მის ფუნქციონირებასა და თავისებურებებზე, ინფორმაციის ავტომატიზებული დამუშავებისა და გადაცემაზე გამოყენებული ტექნოლოგიების შესახებ, განვითარების უახლესი პერსპექტივებით;
- იუ-ს უზრუნველყოფის შესახებ ორგანიზაციულ- განმკარგულებელი დოკუმენტების შესახებ ინფორმაციის შეგროვება და ანალიზი;
- იუუს დასაცავი აქტივების, როლების და მათი პროცესების განსაზღვრა.

ექსპერტული შეფასების უმნიშვნელოვანეს ინსტრუმენტს წარმოადგენს აის-ის შესახებ ინფორმაციის მოგროვებას,დამკვეთის ტექნიკური სპეციალისტებისა და ხელმძღვანელებისაგან ინტერვიუების ჩამორთმევით.

ორგანიზაციის ხელმძღვანელობის შემადგენლობის გამოკითხვის ძირითადი მიზნებია:

- ხელმძღვანელობის პოლიტიკისა და სტრატეგიისა გარკვევა იუ-ს უზრუნველყოფის საკითხებში;
- გარკვევა იმ მიზნებისა რომლებიც დასახულია აის-ის წინაშე;
- იმ მოთხოვნების გარკვევა, რომლებიც წაეყენება იუ-ს ინფორმაციის დამუშავების ამა თუ იმ ქვესისტემებას;
- ამა თუ იმ ინციდენტებისას კრიტიკულობისა და ფინანსური დანაკარგების შეფასების მიღება;

ტექნიკური სპეციალისტების გამოკითხვის ძირითადი მიზნებია:

- ინფორმაციის მოგროვება აის-ის ფუნქციების შესახებ;
- აის-ში ინფორმაციული ნაკადების სქემის მიღება;
- ინფორმაციის მიღება იუუს ტექნიკური ნაწილის შესახებ;
- იუუს მუშაობის ეფექტურობის შეფასება.

ექსპერტული აუდიტის ჩატარებისას წარმოებს შემდეგი ორგანიზაციულ-განმკარგულებელი დოკუმენტების შეფასება: უსაფრთხოების პოლიტიკა, დაცვის გეგმა და სხვადასხვა სახის დებულებები და ინსტრუქციები.

აღნიშნული კატეგორიის დოკუმენტები ფასდება იუ-ს მიზნებისა და ზომების თვალსაზრისით - არის თუ არა ის საკმარისი და ხომ არ ეწინააღმდეგება დასახულ მიზნებს.

ექსპერტული აუდიტის შედეგები შეიძლება მოიცავდეს იუუს ნორმატიულ - მეთოდოლოგიური, ორგანიზაციულ- მმართველობითი და პროცედურული კომპონენტების სრულყოფის შესახებ.

ინფორმაციული უსაფრთხოების სტანდარტებთან შესატყვისობის აუდიტი

მთელ რიგ შემთხვევებში ტარდება იუ-ს სტანდარტებთან შესატყვისობის აუდიტი. აუდიტის შედეგების საფუძველზე სპეციალური უფლებამოსილი ორგანიზაცია -აუდიტორები ღებულობენ გადაწყვეტილებას და გასცემენ დამადასტურებელ დოკუმენტს იუუს შესატყვისობისა ამა თუ იმ ეტალონურ სტანდარტთან (ატარებენ სერტიფიკაციას). სერტიფიკაცია წარმოადგენს იუუს ხარისხის მაჩვენებელს და მაღლა სწევს ორგანიზაციის პრესტიჟს და მისდამი ნდობას.

სტანდარტებთან შესატყვისობაზე აუდიტი უმეტეს შემთხვევაში გულისხმობს აქტიური და ექსპერტული აუდიტების ჩატარებას. შედეგებზე დაყრნდობით შეიძლება მომზადდეს ანგარიშები, რომლებიც შეიცავს შემდეგ ინფორმაციას:

-შემოწმების მიხედვით შეესაბამება,თუ არა,ინფორმაციული სისტემა არჩეულ სტანდარტებს და რა ხარისხით;

-მიღებული შეუსაბამობების და შენიშვნების რაოდენობა და კატეგორიები;

-რეკომენდაციები იუუს აგებაზე ან მოდიფიკაციაზე, რაც საშუალებას იძლევა დამყარდეს განსახილველ სტანდარტებთან შესაბამისობა.

ინსტრუმენტალური შემოწმების ჩატარების მეთოდები

ინსტრუმენტალური შემოწმებები (იშე) სრულდება იუ-ს აქტიური აუდიტისას. იშე-ი წარმოადგენს წინასწარ შეთანხმებული ტესტების ნაკრებს, რომელიც მიმართულია გაირკვეს იუ-ს ქვესისტემების დაცულობის დონეები. ინსტრუმენტალური შემოწმებების ჩატარებისათვის შეიძლება შემოთავაზებულ იქნას შემდეგი მეთოდიკა, სავარაუდო ტესტირება ინფორმაციასთან არასანქცირებულად შეღწევის შესაძლებლობის,როგორც ორგანიზაციის შიგნიდან, ასევე გარეშე ქსელებიდან.

მეთოდიკა მოიცავს სამ ეტაპს: აის–ის სტრუქტურის ანალიზი,შიდა აუდიტი,გარე აუდიტი.

ინფორმაციული უსაფრთხოების პოზიციიდან აის–ის სტრუქტურის ანალიზის ეტაპზე, ტარდება ინფორმაციული რესურსებისა და გამოთვლითი ტექნიკის საშუალებების ანალიზი და ინვენტარიზაცია: ფორმირდება დასაცავი ცნობების ჩამონათვალი, აღიწერება აის–ის ინფორმაციული ნაკადები,სტრუქტურა და შემადგენლობა; ხდება დასაცავი რესურსების კატეგორირება.

მეორე ეტაპზე ხორციელდება აის–ის შიდა აუდიტი, რომელიც მოიცავს ინფორმაციული უსაფრთხოების თვალსაზრისით მისი მომართვების ანალიზს. მოცემულ ეტაპზე ოპს–ის და ინფორმაციის დაცვის სპეციალიზებული საშუალებების ცნობილი ნაკლოვანებების გათვალისწინებით ხორციელდება დაცულობის ანალიზი შიდა საშიში ზემოქმედებისგან. ხდება გამოკვლევა კომპიუტერული ქსელის ლეგალური მომხმარებლების არასანქცირებული მოქმედებების შესაძლებლობის, რომლებმაც შეიძლება გამოიწვიონ კონფიდენციალური მონაცემების მოდიფიკაცია, კოპირება ან დარღვევა. ანალიზი ხორციელდება დაცვის საშუალებების უსაფრთხოების მომართვების დეტალური შესწავლით, რისთვისაც გამოიყენება როგორც ხაკერების არსენალში არსებული საშუალებები, ასევე აის–ის სუსტი მხარეების გამოსავლენად სპეციალურად შექმნილი ავტომატიზებული საშუალებები. ანალიზდება აის–ის შემდეგი კომპონენტები:

- პერსონალური კომპიუტერის (პკ) დაცვის საშუალებები– დაცვის პროგრამულ–აპარატული სისტემების გამორთვის შესაძლებლობა გამორთულ სადგურებთან ფიზიკური დაშვებისას;
- ანტივირუსული დაცვის მდგომარეობა– აის–ში მავნე პროგრამების არსებობა, მათი შეტანის შესაძლებლობა მანქანური მატარებლებიდან, ინტერნეტიდან;
- ოპს–უსაფრთხოების მოთხოვნილი (საჭირო) მომართვების არსებობა;

- პაროლური დაცვა ოპს–ში შესაძლებლობა ფაილების მიღებისა დაშიფრული პაროლებით და მათი შემდგომი დაშიფრაცია; ცარიელი პაროლებით მიერთების შესაძლებლობა, პაროლების მარგების შესაძლებლობა, მათ შორის ქსელიდანაც.

- აის-ის მომხმარებლების რესურსებთან დაშვების გამიჯვნის სისტემა- დაშვების მატრიცის ფორმირება; დაშვების უფლების მიცემისას დუბლირების და სიჭარბის ანალიზი; ყველაზე უფრო ინფორმირებული მომხმარებლების და კონკრეტული რესურსების დაცულობის დონის განსაზღვრა; სამუშაო ჯგუფის ფორმირების ოპტიმალურობა;
- ქსელური ინფრასტრუქტურა- შესაძლებლობა ქსელურ მოწყობილებებთან მიერთებისა დასაცავი ინფორმაციის ხელში ჩასაგდებად და ქსელური ტრაფიკის გასაანალიზებლად; ქსელური პროტოკოლების და სამსახურების მომართვები;
- უსაფრთხოების მოვლენების აუდიტი- აუდიტის პოლიტიკის მომართვა და რეალიზაცია;
- გამოყენებითი პუ - გამოყენებული ავტომატიზებული სამუშაო ადგილების დაცვის ელემენტების საიმედოობა; ინფორმაციის გაჟონვის შესაძლო არხები; გამოყენებულუ პუ-ს ვერსიის ანალიზი სუსტი ადგილების არსებობაზე;
- ინფორმაციის დაცვის საშუალებები (იდს): გამოყენებული იდს-ების საიმედოობა და ფუნქციურობა; დაცვაში სუსტი ადგილების არსებობა; იდს მომართვები.

მესამე ეტაპზე ხორციელდება აის-ის გარეგანი აუდიტი, რომელიც აფასებს ორგანიზაციის რესურსების დაცულობას არასანქცირებული შეღწევებისაგან (არსშ), გარეშე ქსელებიდან, მათ შორის ინტერნეტიდანაც. თანმიმდევრობით ანალიზდება გარედან შეღწევის შემდეგი შესაძლებლობები:

- მონაცემების მიღება აის-ის შიდა სტრუქტურის შესახებ - web-სერვისებზე კონფიდეციალური ხასიათის ინფორმაციის არსებობა; dns-და საფოსტო სერვისის ისეთი მომართვების გამოვლენა, რომლებიც საშუალებას იძლევიან მიღებულ იქნას ინფორმაცია აის შიდა სტრუქტურების შესახებ;
- გამოვლენა კომპიუტერებისა, რომლებიც მიერთებული არის ქსელთან და ხელმისაწვდომი არის ინტერნეტიდან- სკანირება პროტოკოლებით icmp,tcp,udp; განსაზღვრა ხელმისაწვდომობის ხარისხის ინფორმაციისა აის-ში გამოყენებული პუ-ს და მისი ვერსიების შესახებ; აქტიური ქსელური

სამსახურების გამოვლენა; განსაზღვრა ოპს-ის, ქსელური დანართების და სამსახურების ტიპის და ვერსიების;

- ინფორმაციის მიღება სააღრიცხვო ჩანაწერებზე, რომლებიც დარეგისტრირებულია აის-ში, კონკრეტული ოპს-თვის სპეციალური უტილიტების გამოყენებით;
- მიერთება ხელმისაწვდომ ქსელურ რესურსებთან- ხელმისაწვდომი ქსელური რესურსების არსებობის და მათთან მიერთების შესაძლებლობების განსაზღვრა;
- ქსელთაშორისი ეკრანის პროგრამულ უზრუნველყოფაში ცნობილი მოწყვლადობების გამოყენება, ქეკ-ის არასწორი კონფიგურირების გამოვლენა;
- ოპს-ის და ქსელური დანართების ვერსიების გამოვლენა, რომლებიც მიდრეკილია „უარი მომსახურებაზე“ ტიპის შეტევებზე;
- ქსელურ დანართებზე შეტევების შესაძლებლობების ტესტირება -web-სერვერების დაცულობის ანალიზი, მოშორებული მართვის სისტემების მედეგობის ტესტირება, არსებული მოდემური შეერთების მეშვეობით შეღწევის შესაძლებლობების ანალიზი.

ტესტირების შედეგების საფუძველზე ფორმირდება საექსპერტო დასკვნა, რომელიც აღწერს აის-ის გარე და შიდა მუქარებისაგან დაცულობის რეალურ მდგომარეობას, შეიცავს უსაფრთხოების სისტემების მომართვაში არსებული ნაკლოვანებების ჩამონათვალს. მიღებული დასკვნების საფუძველზე მუშავდება რეკომენდაციები აის-ის დაცულობის ხარისხის ამაღლებაზე, სისტემების ადმინისტრირებაზე,ინფორმაციის დაცვის საშუალებების გამოყენებაზე.

მეთოდიკის რეალიზაცია მოითხოვს დაცვის სისტემებში აღმოჩენილი ნაკლოვანებების შესახებ ცოდნის მუდმივ განახლებას. მეთოდიკის ყველა ეტაპი შეიძლება არ იქნას ავტომატიზებული, უმეტეს შემთხვევაში საჭიროა ისეთი ექსპერტის მონაწილეობა, რომელსაც გააჩნია შესაბამისი კვალიფიკაცია.

ასს აუდიტი- ზოგიერთი მითითებები

ასს-ის ადმინისტრატორს ქსელის კონტროლისა და მისი მუშაობის უზრუნველყოფის პროცესში უხდება მთელი რიგი აუცილებელი სამუშაოების ჩატარება, რაც დაკავშირებულია გამოყენებული საკაბელო თუ სხვა ტიპის

საკომუნიკაციო სისტემის, აქტიური მოწყობილებების, ოპერაციული სისტემების და გამოყენებითი პროგრამების სპეციფიკასთან . ქსელების უსაფრთხოების უზრუნველყოფის პრობლემა მრავალასპექ-ტრიანი ერთ-ერთი ასპექტთაგანია ქსელში მიმდინარე პროცესების აუდიტი.

აუდიტის სწორად გამოყენების შემთხვევაში, დამატებითი ფინანსური დანახარჯების გარეშე შეიძლება მნიშვნელოვნად გაიზარდოს არსებულ კომპიუტერულ ქსელში ინფორმაციის უსაფრთხოება.

მარეგლამენტირებელი დოკუმენტები. ვინაიდან ერთი კომპიუტერის ოპერაციული სისტემის ფარგლებშიც კი სისტემურ მოვლენათა და რესურსების აუდიტი ხორციელდება სხვადასხვანაირად, აუცილებელია რომელიმე დოკუმენტში (დებულება ან ინსტრუქცია) დაფიქსირდეს რა და როგორი პერიოდულობით კონტროლდება ქსელი; რა დროის განმავლობაში ინახება ქსელის აუდიტის მასალები; ვის მიერ ხდება მისი დათვალიერება და ანალიზი და ა.შ.

ნებისმიერ ორგანიზაციაში, რომელსაც გააჩნია რთული კომპიუტერული ქსელი აუცილებელია დოკუმენტი, რომელშიც რეგლამენტირებული იქნება ქსელის აუდიტის საკითხები. აღნიშნული დოკუმენტი გახდება ინფორმაციული უსაფრთხოების დამატებითი გარანტი.

2.2. რისკების მართვისა და უსაფრთხოების სისტემების სქემების აგების მეთოდები

განვითარებად სახელმწიფოებში, არსებობს მთელი რიგი პრობლემები, რომლებსაც აწყდება ორგანიზაციები რისკების მართვისას. როგორც ანალიზმა გვიჩვენა ეს ძირითადი პრობლემები ასეთია:

1. გავრცელებულია აზრი, რომ სისტემური რისკ-მენეჯმენტი - ესაა გადაწყვეტილება მხოლოდ მსხვილი ბიზნესისთვის, რომელსაც შეუძლია საკუთრ თავს მისცეს ნება ეწეოდეს მეცნიერულ ფანტასტიკას, რათა მიიღოს დადასტურება შესატყვისობაზე ეს პირველ რიგში მსოფლმხედველობის პრობლემაა. ეს სრულებით არ ნიშნავს იმას, რომ რისკების მართვა - ესაა მხოლოდ მსხვილი ბიზნესის ტექნოლოგია. ხშირად რისკ-მენეჯმენტის ტექნოლოგიის დანერგვას აღიქვამენ როგორც გადაწყვეტილებას, რომელიც თავისი სირთულით ერთ რიგში დგას ERP სისტემის ძვირადღირებული,

მოდულური პროგრამული კომპლექსის SAP- ის დანერგვასთან ერთად. SAP-ი მართლაც იძლევა გადაწყვეტილებებს რისკების მართვისთვის, მაგრამ რისკების მართვის სისტემის დანერგვა არ მოითხოვს ასეთ ინვესტიციებს და არ გულისხმობს ასეთი სირთულის ინფორმაციული სისტემის დანერგვის აუცილებლობას. რისკების მართვის სისტემა თავისუფლად შეიძლება შეიქმნას Excel- ის ბაზაზე, ანუ გაცილებით მცირედი დანახარჯით.

2. რისკების ინტუიციური, არასისტემური მართვა. ზოგიერთი ხელმძღვანელისთვის, რომ იგი ყოველგვარი დამატებითი ტექნოლოგიების გარეშე ხედავს თავისი მდგომარეობისა და მიზნების სრულ სურათს და ინტუიციურად გრძნობს რისკს. მართლაც ნიჭიერ მენეჯერს გააჩნია შესანიშნავი ინტუიცია, „ბიზნეს შეგრძნება“, მოვლენათა განვითარების სხვადასხვა ვარიანტების ქვეცნობიერი გათვლა და გაუცნობიერებელი გადაწყვეტილების მიღება, მაგრამ,რა თქმა უნდა, შესაძლებელია მისი გაუმჯობესება, ცალკე აღებული ადამანის სუბიექტური რისკ – მენეჯერი რისკს „გადახარშავს“ საკუთარ თავში, ხოლო შეგნებული რისკ – მენეჯერი გადაწყვეტილებას მიიღებს ობიექტური კორპორაციული ტექნოლოგიების გამოყენებით, რომელიც არაა დამოკიდებული ხელმძღვანელის განწყობილებაზე, ამინდზე და ა. შ. უფრო მეტიც, ტექნოლოგია, გამრავლებადი და ადვილად გავრცელებადია მთელი ორგანიზაციის ფარგლებში.
3. რისკების არასრული განსაზღვრა. ხშირად მენეჯერები რისკებს განსაზღვრავენ დამოუკიდებლად, ტექნოლოგიის „შეცნობილი სისტემური რისკ-მენეჯმენტის გამოყენების გარეშე, მაგრამ თუ ჩვენ სრულად არ მოვახდენთ რეალიზებული რისკების ფორმალიზაციას (ხოლო ნებისმიერი ინციდენტი, შეფერხება ბიზნესის მუშაობაში – ესაა რეალიზებული რისკი), მაშინ ალბათ – ის გარანტირებულად განმეორდება და კიდევ უფრო გაზრდის ორგანიზაციის დანაკარგებს.
4. რისკების ზუსტი მართვა. ნებისმიერი ბიზნესი მიდრეკილია რისკების სიმრავლეზე. საკრედიტო რისკებზე, ინფორმაციულ ტექნოლოგიების რისკებზე, საბაზრო რისკებზე და ა. შ. ერთი რისკის დანახვა- შემსუბუქება – სულაც არ ნიშნავს რისკების მართვას, თუ ორგანიზაციას არ ექნება ყველა

რისკის თავიდან აცილების საშუალება, როგორც მინიმუმ ის შეძლებს ამ რისკისთვის მომზადებას.

5. უმნიშვნელო რისკებზე კონცენტრაცია (პრიორიტეტიზაციის შეცდომები). იმის გარდა, რომ რისკები შეიძლება იყოს ტიპის მიხედვით სხვადასხვა, ისინი შესაძლებელია განსხვავდებოდეს თავისი მნიშვნელობით ბიზნესისა და საერთოდ, ორგანიზაციის მიზანდასახული საქმიანობისთვის. იმისათვის, რომ გასაგები იყოს თუ რომელ რისკებთან უნდა მოხდეს კონცენტრირება, პირველ რიგში, საჭიროა მათი ადექვატური შეფასება. რისკების რაოდენობრივი შეფასების მეთოდები, უმეტეს შემთხვევაში, ძალიან რთულია და ყოველთვის არ იძლევა მარტივი შეფასების საშუალებას. აქედან გამომდინარე, აუცილებელია, რომ რისკების შეფასების მეთოდები ორგანიზაციის შესაბამისი სამსახურისთვის სრულიად გასაგებ ენაზე იყოს მიწოდებული.
6. რისკების მართვის არაეფექტური სტრუქტურა. ხშირად, რისკების განსაზღვრისა და მათი შემოწმებისას მენეჯერები კონცენტრაციას აკეთებენ მათ განსაზღვრებასა და რაოდენობრივ შეფასებაზე, მოქმედებებზე, რასაც თავისთავად არ მოაქვს დამატებითი სარგებელი ბიზნესის მართვის,სტრატეგიის რეალიზაციისა და არ მიღებული მოგების შემცირების საკითხებში. რეალურად არსებობს რისკების მართვის ტიპიური სტრატეგიები (რისკის მიღება დივერსიფიკაცია, დაზღვევა, აუტრორსინგი და ა. შ.), რომლებიც შეიძლება გამოდგეს გადაწყვეტილებების მიღების კარგ ინსტრუმენტად.. რისკების მართვის სტრატეგიის გამოყენებას შეუძლია ოპტიმალურად განსაზღვროს, რა უნდა გაკეთდეს ამა თუ იმ რისკის მიმართ.

პრაქტიკაში რისკების მართვის სტრატეგიის სისტემატიური რეალიზაცია, საშუალებას იძლევა მოხდეს ბიზნესუსაფრთხრების უზრუნველყოფა, რომელიც იქმნება ვიდრე საჭიროა და ორგანიზაციას ეძლევა შესაძლებლობა განუწყვეტლივ გააუმჯობესოს საკუთარი მდგომარეობის დაცულობისა და კონკურენტუნარიანობის დონე.

უსაფრთხოება წარმოადგენს სასიცოცხლო აუცილებლობას ნებისმიერი სისტემისთვის. აუცილებელია გავაანალიზოთ წესები, რომელთა დაცვასაც გვთავზობენ სპეციალისტები.

რისკებს მართავს ყველა- დაწყებული კერძო სუბიექტიდან, მსხვილი სახელმწიფო თუ ბიზნეს ორგანიზაციებით დამთავრებული და ამას ვიღაც ახორციელებს უკეთესად, ვიღაც კი უარესად. ის ორგანიზეციები, რომლებიც რისკებს მართავს უფრო უარესად – გამოიმუშავებს უფრო ნაკლებს, ვიდრე შეუძლია და მეტს კარგავს (ვიდრე შეეძლო დაეკარგა).

ნებისმიერი მიზანდასახული სისტემა დამოუკიდებლად იმისა, სახელმწიფოა ეს, კომპანია თუ ადამიანი, მიისწრაფვის გადარჩეს, იარსებოს, და განვითარდეს. უსაფრთხოების უზრუნველყოფის გარეშე. ეს პროცესი შეუძლებელია, უსაფრთხოება წარმოადგენს ნებისმიერი სისტემის სასიცოცხლო მოთხოვნილებას და მის სასიცოცხლო ღირებულებას.

კორპორაციული უსაფრთხოების სისტემის დაცვის ობიექტს წარმოადგენს ყველაზე რესურსი: ინფორმაცია, ინტელექტუალური საკუთრება, აქტივები, ქონება, კლიენტები, პერსონალი, ტექნოლოგიები და ა.შ. თვით ორგანიზაციის მართვის სისტემა ასევე წარმოადგენს გარკვეულ რესურსს და საჭიროებს დაცვას. მართვა ისე უნდა იყოს აგებული, რომ უსაფრთხოების სისტემა არ ჩაიკეტოს ცალკე სტრუქტურაში.

უსაფრთხოების უზრუნველყოფა – ესაა არა მარტო უსაფრთხოების სამსახურის საზრუნავი, არამედ ორგანიზაციის მთელი მენეჯმენტის სისტემა.ის უნდა მოიცავდეს ყველა თანამშრომელს, პრეზიდენტიდან დაწყებული-ტექნიკურ პერსონალამდე. უსაფრთხოების მართვის ლოკალიზეცია ცალკე დანაყოფში (მაგალითად დეპარტამენტში) შეიძლება იყოს ეფექტური მხოლოდ იმ შემთხვევაში, თუ ბიზნესი გამაგრდა და არაფერი იცვლება, მაგრამ როდესაც ბაზარი დინამიურად იცვლება, საჭიროა მოქნილი სისტემა. უსაფრთხოების მართვა განვითარებადი პროცესია.

უსაფრთხოება ეს არის ადამიანების პრობლემა და აქედან გამომდინარე, მუქარის წყაროს წარმოადგენს არა მარტო ბუნებრივი კატაკლიზმები. არამედ, ადამიანებიც. უსაფრთხოების სისტემას აგებენ ადამიანები და მართავენ ადამიანები. უსაფრთხოების მოთხოვნებს თანამშრომლები უნდა იცავდნენ უთქმელად და ყოველგვარი გადახვევების გარეშე, ასეთმა მიდგომამ შეიძლება ორგანიზაციას სერიოზული პრობლემები ააცილოს.

განვიხილოთ, უსაფრთხოების სისტემების სქემების აგების მეთოდები

უსაფრთხოების სისტემის აგების უნივერსალური სქემაპრაქტიკულად არ არსებობს. უსაფრთხოების ყოველი სისტემა – ესაა უნიკალური პროდუქტი. ის უნდა აიგოს, საწარმოს მიზნებიდან, კავშირებიდან და ბიზნესპროცესებიდან გამომდინარე. სავაჭრო საწარმო და საფინანსო კომპანია ძალიან განსხვავდება ერთმანეთისგან, მიუხედავად ამისა არსებობს მუქარების ლოკალიზაციის ზოგადი ალგორითმი, რომელიც მისაღებია ნებისმიერი მიზანდასახული სისტემისთვის, მათ შორის:

1. მუქარათა (რისკების) წყაროების იდენტიფიკაცია.
2. მუქარის სერიოზულობის შეფასება, მუქარის წყაროს რესურსების დონე და მისი მიზნები – საწარმოს რესურსების შესაძლო ზარალი.
3. მუქარების წყაროების გამოყოფა ჯგუფების, მიზნებისა და რესურსების მიმართ ინტერესების მიხედვით.
4. მუქარების ლოკალიზაციის დაცვის სისტემის ალგორითმის აგებაზე რესურსების ოპტიმალური გამოყოფა, ამორჩევა და გამოყენება, იდენტიფიკაცია, რანჟირება, ყველაზე სერიოზული რისკის არჩევა, ხოლო შემდეგ რისკების ოპტიმიზაცია და მათი რეგულირება – ასეთია მესაკუთრეობაში ცოდნით აღჭურვილი რისკ – მენეჯმენტის საფუძველი.

უსაფრთხოების სისტემის აგებისას უნდა იქნას გათვალისწინებული ასევე შემდეგი რამოდენიმე მნიშვნელოვანი მომენტი.

1. არსებობს სამი ცნება: უსაფრთხოება, სისწრაფე დ სიიაფე. სისტემის აგებისას შეიძლება არჩეულ იქნას ორი მათგანი. სისტემა შეიძლება იყოს უსაფრთხო და სწრაფი, მაგრამ ის ამ დროს შეიძლება აღმოჩნდეს ძალიან ძვირი. ის შეიძლება იყოს იაფი და სწრაფი, მაგრამ არა უსაფრთხო, ის შეიძლება იყოს უსაფრთხო და იაფი, მაგრამ ის იქნება ძალზე ნელი.

ოპტიმალური კომბინაციის შერჩევა გადაწყვეტილებათა მიმღები პირების პრეროგატივაა. რისკების განულება შეუძლებელია, მაგრამ ეფექტურ უსაფრთხოების სამსახურს შესწევს იმის უნარი, რომ ეს რისკი გახადოს ოპტიმალური.

2. უსაფრთხოების მართვაში, მოქმედებს ყველა ეკონომიკური კანონები და ცნებები, მაგალითად ეფექტურობა, თუმცა მისი გაანგარიშება ჩვეულებრივი

ეფექტურობის გათვლაზე, შედარებით რთულია, ვინაიდან აქ ეფექტს წარმოადგენს არა მოგება, არამედ ეკონომია.

3. უსაფრთხოება და სირთულე. რაც უფრო რთულია პროცესი, მით უფრო მეტია პრობლემები უსაფრთხოებაში, მით ნაკლებად საიმედოა ის, რაც უფრო რთულია საკითხები, მით უფრო ძვირად ღირებული სისტემაა საჭირო.

4. უსაფრთხოება ემორჩილება სინდერის სამართებლის წესს. სხვა ფაქტორების არ არსებობის შემთხვევაში ყოველთვის გამოიყენეთ ვარიანტი ყველაზე მაღალი უსაფრთხოებით. ეს სამართლიანია ბიზნესში ნებისმიერი გადაწყვეტილების მიღებისას.

5. უსაფრთხოება – ინვესტიცია, და არა გასავალი. ის ძვირი ღირს, მაგრამ ეს გამართლებულია, მაგრამ ეს სრულებით არ ნიშნავს, რომ მასში უნდა ხდებოდეს შემდგომი გაზრდა პრაქტიკულად არ ბრდის უსაფრთხოების დონეს. ამ მომენტის სწორად განსაზღვრა ნიშნავს ეკონომიკურად ეფექტურ მუშაობას.

6. უსაფრთხოების ნებისმიერი სისტემა ამუხრუჭებს სისტემის განვითარებას მთლიანობაში. ერთადერთი გამოსავალი – ესაა მოყოლა ცვლილებები. უნდა იცვლებოდეს ბიზნესთან ერთად. ყველაზე უფრო ეფექტური უსაფრთხოების მართვა იქ სადაც ის ჩართულია უშუალოდ ბიზნეს – პროცესში. მაგალითად, კორპორაციებში, სადაც ხდება მსხვილი პროექტების რეალიზება, ყოველ მათგანში ხდება უსაფრთხოების მენეჯერის ჩართვა, რომელიც თვალყურს მიადევნებს რისკებს თავისი მიმართულებით და ღებულობს გადაწყვეტილებას, როგორ იქნას თავიდან აცილებული მუქარები, ისე რომ არ დაქვეითდეს მუშაობის ეფექტურობა და სისწრაფე.

მთავარი სირთულე, რასთანაც დაკავშირებულია უსაფრთხოების სამსახურის მოღვაწეობა, მდგომარეობს ადამიანის ფსიქოლოგიაში. თანამედროვე უსაფრთხოების სამსახურის ეფექტური მუშაობა შეუძლებელია გაგებისა და ნდობის გარეშე, კომპანიის მართვის ყველა დონეზე.

2.3. მომხმარებლის რესურსთან არასანქცირებული შეღწევის კონტროლის მექანიზმები– დაშვების მოდული (მატრიცა)

. კომპიუტერული უსაფრთხოების მუქარათა მთელი სპექტრი შეიძლება დაიყოს ორ დიდ ჯგუფად: შიდა და გარეშე IT –ის მუქარები.

– კონფიდენციალური ინფორმაცია აპრიორულად წარმოადგენს არასანქცირებული შეღწევის ობიექტს, ვინაიდან გააჩნია სამომხმარებლო ღირებულება ბოროტგანმზრახველისთვის, ანუ წარმოადგენს საქონელს.

ინსაიდური მომხმარებლები, რომლებიც დაშვებული არიან კონფიდენციალური ინფორმაციის დამუშავებასთან თავისი სამსახურებრივი მოვალეობების ფარგლებში. სწორედ სანქცირებული მომხმარებლები არიან ყველაზე მეტი მუქარის მატარებლები, საწარმოს კონფიდენციალური ინფორმაციის დატაცების თვალსაზრისით. მისი გადაწყვეტა უნდა დაეკისროს დამატებით დაცვის საშუალებებს.

კონფიდენციალური ინფორმაციის დაცვის დამატებითი საშუალება, რომელიც გამოიყენება კორპორაციულ დანართებში უნდა იყოს კომპლექსური – უნდა წყვეტდეს ინფორმაციის დაცვის ამოცანას, როგორც შიდა, ასევე გარეშე IT – მუქარებისადმი წინააღმდეგობის გაწევის ნაწილში.

რესურსებთან შეღწევის კონტროლის მექანიზმების დანიშნულება ინფორმაციის დაცვის საკვანძო მექანიზმს წარმოადგენს რესურსთან შეღწევის კონტროლი, რომელიც ეფუძნება მომხმარებლისათვის რესურსებთან შეღწვის გამიჯვნის წესების დადგენასა და რეალიზაციაზე.

შეღწევის მოცემული წესები ყოველთვის შესაძლებელია წარმოდგენილი იქნას შესაბამისი მოდელით (ან დაშვების მატრიცით).

ვთქვათ, S= {O; წკ; ჩწ} შესაბამისად, შეღწევის სუბიექტებისა და ობიექტებისწრფივად მოწესრიგებული სიმრავლეა. შეღწევის სუბიექტად მოიაზრება, როგორც ცალკეული სუბიექტები, ასევე სუბიექტების ჯგუფი, რომლებსაც გააჩნია შეღწევის ერთნაირი უფლებები, შესაბამისად შეღწევის ობიექტად Qi მოიაზრება როგორც ცალკეული ობიექტები, ასევე ჯგუფი ობიექტებისა, რომლებიც ხასიათდება მათთან შეღწევის ერთიანი წესებით.

ვთქვათ S= {O; წკ; ჩწ} არის შეღწევის სიმრავლე, სადაც “O” ნიშნავს სუბიექტის ობიექტთან შეღწევის არარსებობას„წკ“ – ნებართვა შეღწევაზე ობიექტის წასაკითხად „ჩწ“ – ნებართვა შეღწევაზე ობიექტში ჩაწერაზე.

შეღწევის კონტროლის კანონიკური მოდელი შეიძლება წარმოვადგინოს შეღწევის D მატრიცის მეშვეობით, რომელსაც აქვს შემდეგი სახე.

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \cdot \\ \cdot \\ O_{k-1} \\ O_k \end{array} \begin{bmatrix} C_1 & C_2 & \ldots & C_{k-1} & C_k \\ \text{Cw/wk} & 0 & \ldots & 0 & 0 \\ 0 & \text{Cw/wk} & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \text{Cw/wk} & 0 \\ 0 & 0 & \ldots & 0 & \text{Cw/wk} \end{bmatrix}$$

აქ წარმოდგენილი D მატრიცის მთავარი დისტონატი ელემენტები იძლევა სუბიექტების ობიექტებთან სრული შეღწევის წესს, ხოლო დანარჩენი ელემენტები 0-ი კრძალავს სუბიექტების ობიექტებთან ინფორმაციის დამუშავების შეღწევას.

შევნიშნავთ, რომ შეღწევის კანონიკური მოდელი აღწერს იზოლირებულ რეჟიმს, რომლის დროსაც ობიექტებს არ შეუძლიათ შეასრულონ სუბიექტების ურთიერთქმედების არსების როლი.

დღეს IT-ი მუქარებისადმი წინააღმდეგობის გაწევის კერძო გადაწყვეტებში ფართოდ გამოიყენება შეღწევის სრულუფლებიანი კონტროლი მისი პრაქტიკული გამოყენება განპირობებულია იმით, რომ კორპორაციულ სისტემებში როგორც წესი, ერთი და იგივე კომპიუტერზე ხდება კონფიდენციალური თვალსაზრისით სხვადასხვა დონის ინფ-ის დამუშავება, რაც საშუალებას იძლევა მოხდეს მისი კატეგორირება („ღია“, „კონფიდენციალური“, „მკაცრად კონფიდენციალური“ და ა. შ.) ამ დროს აუცილებელია უზრუნველყოფილ იქნას სხვადასხვა კატეგორიის ინფორმაციის დამუშავების სხვადასხვა რეჟიმები კატეგორირებულ ობიექტებთან შეღწევის სუბიექტებისათვის შესაბამისი უფლებამოსილებების მინიჭების საფუძველზე.

შეღწევის სრულუფლებიანი კონტროლის საფუძველს შეადგენს ცნებების „მომხმარებლების ჯგუფი“ და „ობიექტების ჯგუფი“ ფორმულირების წესი უფლებამოსილებათა სკალის შემოტანის გზით. პრაქტიკაში ყველაზე უფრო გავრცელებულია უფლოებამოსილებათა იერარქიული სკალა, რომელიც ეფუძნება მონაცემების კატეგორირებას (ღია, კონფიდენციალური, მკაცრად კონფიდენციალური და ა. შ.) და მომხმარებლებთან მონაცემების შეღწევის უფლებებს. მივიღოთ, რომ რაც უფრო მაღალია სუბიექტის უფლებამოსილება და ობიექტების სიმრავლეებში $C=\{C_1,\ldots, C_k\}$ და $O=\{O_1.,,,.O_k\}$

სუბიექტების ობიექტებთან შეღწევის წესების შესაბამისი ფორმალიზაცია, როგორც წესი დაიყვანება შემდეგზე

· სუბიექტს უფლება აქვს ობიექტს „ჩწ/წკ“ შეღწევებსა, თუ სუბიექტის უფლებამოსილება და ობიექტის კატეგორია ერთმანეთს ემთხვევა;

· სუბიექტს უფლება აქვს ობიექტზე „წკ“ შეღწევისა, თუ სუბიექტის უფლებამოსილება უფრო მაღალია ვიდრე ობიექტის კატეგორია;

· სუბიექტს უფლება არ აქვს ობიექტზე შეღწევის უფლებათუ მისი უფლებამოსილება უფრო დაბალია ვიდრე ობიექტის კატეგორია.

ამ შემთხვევაში მატრიცა D ექნება სახე:

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \cdot \\ \cdot \\ O_{k-1} \\ O_k \end{array} \begin{bmatrix} C_1 & C_2 & \dots & C_{k-1} & C_k \\ \text{Cw/wk} & 0 & \dots & 0 & 0 \\ \text{wk} & \text{Cw/wk} & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \text{wk} & \text{wk} & \dots & \text{Cw/wk} & 0 \\ \text{wk} & \text{wk} & \dots & \text{wk} & \text{Cw/wk} \end{bmatrix}$$

ამრიგად, ძირითადი ამოცანა, რომელიც წყდება შეღწევის კონტროლის მოცემული წერისას მდგომარეობს თავიდან იქნას აცილებული ინფორმაციის კატეგორიის დაქვეითება მისი დამუშავებისას. ზოგჯერ ხდება დამატებითი წესის შემოტანა, რომელიც ნებას რთავს მოხდეს უფრო დაბალი კატეგორიის ინფორმაციის ჩაწერა, უფრო მაღალი კატეგორიის ობიექტებში, რომლებიც ასევე არ ეწინააღმდეგება ინფორმაციის კატეგორიის დაქვეითებას არ დაშვების იდეას. მატრიცა D–ს ამ შემთხვევაში ექნება სახე:

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \cdot \\ \cdot \\ O_{k-1} \\ O_k \end{array} \begin{bmatrix} C_1 & C_2 & \dots & C_{k-1} & C_k \\ \text{Cw/wk} & \text{Cw} & \dots & \text{Cw} & \text{Cw} \\ \text{wk} & \text{Cw/wk} & \dots & \text{Cw} & \text{Cw} \\ \dots & \dots & \dots & \dots & \dots \\ \text{wk} & \text{wk} & \dots & \text{Cw/wk} & \text{Cw} \\ \text{wk} & \text{wk} & \dots & \text{wk} & \text{Cw/wk} \end{bmatrix}$$

რესურსებთან შეღწევის ალბათური კონტროლის მოდელი

ინფორმაციის დაცვის კლასიკური ამოცანის ნაწილი მისი ხელმისაწვდომობის და მთლიანობის უზურნველყოფა .

ამ შემთხვევაში განსაკუთრებული ყურადღება უნდა მიექცეს ინფორმაციის მაკროვირუსებით შესაძლო „დასნებოვნებისათვის“ წინააღმდეგობის გაწევას,

რაც წარმოადგენს უკვე გარეშე IT – მუქარებისათვის წინააღმდეგობის გაწევის ამოცანას.

განვიხილოთ თუ რაში მდგომარეობს განსახილველი დანართების (ინფ. დამუშავება საწარმოში) თავისებურება.

1) კატეგორირებული ინფორმაციის მაგ. „კონფიდენციალური“ და „ღია“ დამუშავება აპროირულად გულისხმობს, რომ პირველ რიგში დაცვის ობიექტის აქტს წარმოადგენს უფრო მაღალი კატეგორიის ინფ–ია (კერძოდ, პირველ რიგში დაცული უნდა იქნას კონფიდენციალური ინფ., ხოლო მუშაობა ღია ინფ – თან მოცემულ დანართებში ოფიციალურია და მისი დაცვა არც იმდენადაა მნიშვნელოვანი).

2) კატეგორირებული ინფორმაციის (მაგ: „კონფიდენციალური“ და „ღია“) აპრიორულად გულისხმობს დამუშავების და შენახვის სხვადასხვა რეჟიმებს, თანაც, რაც უფრო მაღალი ინფ. კატეგორია, მით უფრო მკაცრი მოთხოვნები წარედგინებათ მათ დამუშავებას (კერძოდ კონფიდენციალური ინფ–ია როგორც წესი ნებადართულია შეიქმნას მხოლოდ საწარმოს გამოთვლით საშუალებებზე თანაც დანართების გარკვეული ნაკრებით, შენახვა მხოლოდ საწარმოს გამოთვლით საშუალებებზე თანაც დანართების გარკვეული ნაკრებით, შენახვა და გაცვლა მოცემულ ინფორმაციული ქსელით მხოლოდ მობილური მაგროვებლების გამოყენებით აგრეთვე ხორციელდება გამოთვლით საშუალებებს შორის კორპორაციული ქსელისა, რომლებიც უნდა იყოს დაცული, რასაც მოითხოვს კონფინდენციალური მონაცემების დამუშავება, ღია ინფორმაცია შეიძლება შემოდიოდეს შეუმოწმებელი წყაროებიდან, არ ითვალისწინებს რაიმე რეგლამენტაციას მისი შექმნის, დამუშავებისა და შენახვისას).

როგორც შედეგი, ალბათობა იმისა. რომ მაკროვირუსით „დასნებოვნებული“ ღია დოკუმენტი მთელი რიგით უფრო მაღლაა ვიდრე კონფიდენციალურის, შესაბამისად რაც უფრო მაღალია დოკუმენტის კატეგორია (უფრო მკაცრია დამუშავების კუთხე), მით უფრო დაბალია ალბათობა იმისა, რომ დოკუმენტი დასნეოვნებულია მაკროვირუსით.

შეიძლება გაკეთდეს მნიშვნელოვანი დასკვნა რაც უფრო დაბალია დოკუმენის კატეგორია, მით ნაკლებად საჭიროებს ის დაცვას „დასნებოვნებისგან“, რაც მათ

შორის დაეტყობა მისი დამუშავების რეჟიმებს, როგორც შედეგი, მით უფრო მაღალია ალბათობა, რომ ის აღმოჩნდეს „დასნებოვნებული“.

იმის გამო, რომ ერთი და იგივე კომპიუტერზე მუშავდება როგორც ღია (რომელსაც გააჩნია მაღალი ალბათობა „დასნებოვნებისა“) ასევე კონფიდენციალური (რომელიც უნდა იქნას დაცული „დასნებოვნებისაგან“) ინფორმაცია, შეიძლება ფორმურირებულ იქნას ანტივირუსული დაცვის ამოცანა შემდეგნაირად: უზრუნველყოფილ იქნას კონფიდენციალური ინფორმაციის დაცვა მაკროვირუსებისგან, რომლებითაც შეიძლება „დასნებოვანებული“ იყოს დიდი ალბათობით ღია დოკუმენტები, ანუ აღიკვეთოს ვირუსის გავრცელება კონფიდენციალურ მონაცემებზე. ზოგად შემთხვევაში (როცა არსებობს კონფიდენციალობის რამოდენიმე კატეგორიის ამოცანა) შეიძლება ფორმურილებულ იქნას შემდეგნაირად: აღიკვეთოს ვირუსების გავრცელება უფრო მაღალი კონფიდენციალურობის კატეგორიის მონაცემებზე.

ავღნიშნოთ Pi ალბათობა იმისა, რომ i კატეგორიის დოკ-ნტი „დასნებოვნებული“ იქნება მაკროვირუსით, ამ დროს, როგორც ზემოთ იქნა აღნიშნული აპრიორი გვაქვს

$P_1 < P_2 < \ldots < P_k$

თუ მივიღებთ მხედველობაში იმ ფაქტს, რომ მაკროვირუსი მოქმედებას იწყებს (რაც თავის თავში შეიძლება შეიცავდეს „დასნებოვნების“ მუქარას) მხოლოდ შესაბამისი დანართის მიერ მის წაკითხვის შემდეგ და რომ თავიდან უნდა ავიცილოთ უფრო მაღალი კატეგორიის დოკ – ის „დასნებოვნება“ მაკროვირუსით უფრო დაბალი კატეგორიის დოკ – დან (დანართის მიერ მის წაკითხვის შემდეგ) მივიღებთ შეღწევის შემდეგ მატრიცას F რომელიც აღწერს ალბათურ მოდელს შეღწევის კონტროლისა, რომელიც რეალიზდება ანტივირუსული წინააღმდეგობისთვის:

$$F = \begin{array}{c} \\ O_1(P_1) \\ O_2(P_2) \\ \cdot \\ \cdot \\ O_{k-1}(P_{k-1}) \\ O_k(P_k) \end{array} \begin{bmatrix} C_1 & C_2 & \ldots & C_{k-1} & C_k \\ Cw/wk & wk & \ldots & wk & wk \\ Cw & Cw/wk & \ldots & wk & wk \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ Cw & Cw & \ldots & Cw/wk & Cw \\ Cw & Cw & \ldots & Cw & Cw/wk \end{bmatrix}$$

ვხედავთ, რომ მოცემული მოდელის რეალიზაციის ნებადართული ჩაწერა დოკ – ებისა, რომელიც გააჩნიათ უფრო ნაკლები ალბათობა მაკროვირუსით „დასნებოვნებისა“ ობიექტში, რომლებშიც დოკუმენტებს გააჩნია მაკროვირუსით დასნებოვნების დიდი ალბათობაა – საპირისპირო აკრძალულია, ანუ ხდება თავიდან აცილება უფრო მაღალი კონფიდენციალობის დოკ – ების „დასნებოვნების“ ალბათობის ამაღლებისა, იმის ხარჯზე, რომ ერთი და იგივე კომპიუტერზე შეიძლება იქმნებოდეს, მუშავდებოდეს და ინახებოდეს უფრო დაბალი კატეგორიის დოკ – ები, რომელთა მაკროვირუსებით „დასნებოვნების“ ალბათობა მაღალია.

კერძო გადაწყვეტის ნაკლოვანებები. კორპორატიულ დანართებში რესურსებთან შეღწევის კონტროლის რეალიზაციისადმი კომპლექსური მიდგომა

შევადაროთ D და F მატრიცები, როგორც ვხედავთ, ისინი სრულად ერთმანეთის საწინააღმდეგოა, ანუ მოთხოვნა– შეღწევის სრულუფლებიანი კონტროლისადმი ინფორმაციის დაცვის ალტერნატიული ამოცანების გადაწყვეტისას არა ის რომ იყოს სხვადასხვა – ისინი ერთმანეთის საწინააღმდეგოა.

გარეშე IT – მუქარებისადმი, კერძოდ კი ანტივირუსული დაცვის წინააღმდეგობის გაწევის თვალსაზრისით პრაქტიკული გამოყენება შეღწევის სრულუფლებიანი კონტროლის მექანიზმებისა დაუშვებელია. ეს განპირობებულია იმით, რომ როგორც ჩატარებული გამოკვლევებიდან ჩანსს კერძო გადაწყვეტის რეალიზაციისას, რომელიც ეფუძნება შეღწევის სრულუფლებიან კონტროლს გამოიყენებს კარდინარულად ქვეითდება გარეშე IT – მუქარებისადმი წინააღმდეგობის გაწევის ეფექტურობა.

უნდა შევნიშნოთ, რომ კონფიდენციალურ მონაცემებზე ვირუსული ზემოქმედების ალბათობის ამაღლება – ეს არაა ერთადერთი მიზეზი გარეშე IT – მუქარებისადმი წინააღმდეგობის გაწევის ეფექტურობის შემცირებისა შეღწევის სრულუფლებიანი კონტროლის გამოყენებისას, ამ დროს იხილება წარმატებული ქსელური შეტევის ალბათობა ვინაიდან ამ შემთხვევაში ქსელური სამსახურების გაშვება ხდება რიცხვითი ჩანაწერების ქვეშ, რომლებსაც დაშვება აქვთ კონფიდენციალურ ინფ – თან, და სხვა.

ჯერ განვიხილოთ, რომელი ინფორმაციის კატეგორირებას ვახდენთ. ანტივირუსული დაცვის ამოცანის გადაწყვეტის თვალსაზრისით. ბუნებრივია, რომ დამუშავების ხარისხობრივი განსხვავება გააჩნია, ჩვენ შეგვიძლია გამოვყოთ ორი ძირითადი კატეგორია „ღია“ და „კონფიდენციალური“. ამ დროს სხვადასხვა კატეგორიის კონფიდენციალური ინფორმაციის დამუშავება საწყისად იყოს „დასნებოვნებული“ მაკროვირუსით, ალბათობის ნაწილში უკვე განსხვავდება არც ისე არსებითად.

ნათქვამიდან გამომდინარე პრაქტიკულად აქვს აზრი განხილულ იქნას ალბათობათა ისეთი თანაფარდობა, რომ დოკუმენტი i–ური კატეგორიას „დასნებოვნებული“ მაკროვირუსით, თუ აღვნიშნავთ კატეგორიიას „ღია“ როგორც K გვექნება:

$P_1=P_2=...=P_{k-1}<<P_k$

ბუნებრივია, თუ ჩვენ არ შეგვიძლია ნება დავრთოთ არც წაკითხვაზე, არც ჩაწერაზე (ვინაიდან ეს მოთხოვნები ერთმანეთის საწინააღმდეგოა დაშვების მატრიცებში), მაშინ დაგვრჩენია ერთადერთი გადაწყვეტილება, რომელიც დაკავშირებულია დაშვების სრულ აკრძალვასთან, ნათქვამის გათვალისწინებით ვღებულობთ შეღწევის სრულუფლებიანი კონტროლის მოდელს, რომლის რეალიზაციაც საშუალებას გვაძლევს განსახილველი ალტერნატიული ამოცანები გადაწყდეს კომპლექსში, რომელიც აღიწერება დაშვების მატრიცით D(F):

$$D(f)=\begin{array}{c} \\ O_1 \\ O_2 \\ \cdot \\ \cdot \\ O_{k-1} \\ O_k \end{array}\begin{bmatrix} C_1 & C_2 & \dots & C_{k-1} & C_k \\ \text{Cw/wk} & 0 & \dots & 0 & 0 \\ \text{wk} & \text{Cw/wk} & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \text{wk} & \text{wk} & \dots & \text{Cw/wk} & 0 \\ \text{wk} & \text{wk} & \dots & \text{wk} & \text{Cw/wk} \end{bmatrix}$$

უნდა შევნიშნოთ, რომ შეღწევის სრულუფლებიანი კონტროლისადმი რეალიზაციისადმი ასეთი მიდგომისას ღია მონაცემების დამუშავება სრულადაა იზოლირებული კონფიდენციალური მონაცემების დამუშავებისაგან.

ასეთი გადაწყვეტის შედეგებზე, რომელიც არავითარ შემთხვევაში არ ეწინააღმდეგება მონაცემთა დამუშავების იდეას მომხმარებელთა უფლებამოსილების და ობიექტების კატეგორიების საფუძველზე წარმოადგენს ის, რომ ღია მონაცემების მაკროვირუსით „დასნებოვნების“ ალბათობის ამაღლება

არანაირ გამვლენას ვერ ახდენს კონფიდენციალური ინფ – ის მაკროვირუსით „დასნებოვნების“ ალბათობაზე, რაც განისაზღვრება პირობით:

$P_1=P_2=...=P_{k-1}<<P_k$

აქ მნიშვნელოვანია ის მომენტი, რომ თუ ღია მონაცემების მაკროვირუსით „დასნებოვნების“ ალბათობაზე გავლენის მოხდენა პრაქტიკულად შეუძლებელია, ვიდრე შემცირდეს მისი ალბათობა, სპეციალური დაცვის ანტივირუსული საშუალებების გამოყენებით (რაც ერთის მხრივ არ იძლევა გადაწყვეტას საერთო სახით, ვინაიდან სიგნაციურული ანალიზი საშუალებას იძლევა ნაპოვნი იქნას ცნობილი მაკროვირუსები, მეორეს მხრივ, მოცემულ დანართში უცნაურად გამოიყურება – ვიცავთ ღია მონაცემებს, რომლებიც ზოგადად რომ ვთქვათ, არ საჭიროებენ დაცვას ვინაიდან საბოლოო ჯამში „დასნებოვნებისაგან“ დავიცვათ კონფიდენციალური მონაცემები, ალბათობა ინფ–ის მონაცემების მაკროვირუსებით „დასნებოვნების“ ალბათობა შეიძლება არსებითად შემცირდეს.

თუ ცალკე აღრიცხვითი ჩანაწერით რეალიზდება შეღწევა გარეშე ქსელში, თანაც ამ აღრიცხვითი ჩაწერით არაა დაშვებული შეღწევა კონფიდენციალურ მონაცემებთან, მაშინ მნიშვნელოვნად მცირდება კონფიდენციალურ ინფ – თან შეღწევის ალბათობა ქსელიდანაც.

მატრიცა D(F) ილუსტრაციაა იმისა, რომ კომპიუტერზე მხოლოდ ორი კატეგორიის ინფორმაციის დამუშავებისას („ღია“ და „კონფიდენციალური“ – ყველაზე უფრო გავრცელებული შემთხვევაა), ინფორმაციის კომპლექსში დაცვის ამოცანის გადაწყვეტის თვალსაზრისით გამოიყენება შეღწევის სრულუფლებიანი კონტროლი დაუშვებელია.

უნდა შევნიშნოთ, რომ საერთო შემთხვევაში, აღნიშნული მიდგომის გამოყენებით (შესაბამისი შეღწევის უფლების აკრძალვით) შეიძლება ფორმირებულ იქნას შეღწევის კონტროლის სხვადასხვა წესები (სხვადასხვა ვარიანტები კონფიდენციალური მონაცემების დაცვისა მაკროვირუსით „დასნებოვნებასთან“). ერთ – ერთი მაგალითი შეღწევის შესაბამისი მატრიცისა (ხდება იზოლირება ყველაზე მაღალი კატეგორიის მონაცემები (დამუშავებისა) მოყვანილის ქვემოთ.

ამრიგად, დაცვის საშუალება უნდა წყვეტდეს კომპლექსური საჭირო დაცვის ამოცანების ნაკრებს, რომლებიც აქტუალურია კონკრეტული დანართისათვის,

კერძოდ, კონფიდენციალური ინფორმაციისთვის უზრუნველყოფილ იქნას წინააღმდეგობის გაწევა, როგორც შიდა , ასევე გარეშე IT – მუქარებისადმი.

$$D(f) = \begin{array}{c} \\ O_1 \\ O_2 \\ \cdot \\ \cdot \\ O_{k-1} \\ O_k \end{array} \begin{bmatrix} C_1 & C_2 & \dots & C_{k-1} & C_k \\ \text{Cw/wk} & 0 & \dots & 0 & 0 \\ 0 & \text{Cw/wk} & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \text{wk} & \dots & \text{Cw/wk} & 0 \\ 0 & \text{wk} & \dots & \text{wk} & \text{Cw/wk} \end{bmatrix}$$

კერძოდ, გადაწყვეტილებების რეგისტრაციაში არ უნდა დააქვეითოს ინფორმაციის დაცვის ეფექტურობა, რაც შესაძლებელია იმის გამო, რომ გადაწყვეტილებები ალტერნატიული ტიპის მუქარებისათვის შეიძლება აღმოჩდეს ურთიერთ გამომრიცხავი, რის გამოც კერძო გადაწყვეტილების რეალიზაციამ შეიძლება გამოიწვიოს ერთი ტიპის მუქარებისათვის წინააღმდეგობის გაწევის ეფექტურობის ამაღლება, სხვა ტიპის მუქარებისადმი წინააღმდეგობათა გაწევის ეფექტურობის დაქვეითების ხარჯზე.

2.4. ვირუსებთან ბრძოლის თანამედროვე მეთოდების ანალიზი, წამყვანი კომპანია Symantec– ის უსაფრთხოების სოფტის მაგალითზე

ფართო მასების მხრიდან ანტივირუსებით დაინტერესებას მარტივი ახსნა გააჩნია. რაც უფრო იმატებს აქტიური კომპიუტერთა რიცხვი და რაც უფრო ვითარდება ტექნოლოგიები, მით მეტად იზრდება საფრთხე რიგითი მომხმარებლის კომპიუტერის დავირუსებისა.

დღეისათვის კომპანია Symantec უსაფრთხოებისათვის განკუთვნილი სოფტის საკმაოდ კონკურენტულ სამყაროში უდიდესი გამოცდილებისა და არგი რეპუტაციის ლიდერად გვევლინება. ის მნიშვნელოვანი პრობლემის გადასალახავად Norton 360, იყენებს, რომელიც მეტად ეფექტურია. ის ინსტალაციის პროცესში პრობლემების აღმოჩენისთანავე, უკავშირდება სერვერს და თუ წარმატებით მოახდინა პრობლემის იდენტიფიცირება, მისგან იღებს დასაფიქსად საჭირო სკიპტს. ამგვარად Norton 360, ნაბიჯ – ნაბიჯ მაგრამ მაინც ინსტალირდება malware – ების მიერ უკვე დაპყრობილ სისტემაზე.

Norton Managment ფუნქცია, რომელიც Symantec 2012 სერიის პროდუქტებში გვხვდება საკმაოდ კარგი გამოდგა ლოკალური უსაფრთხოების სისტემების მართვისათვის. ასე მაგალითად Managment მეშვეობით შესაძლებელია Symantec დაცვის აღჭურვილი კომპიუტერების ონლაინ მართვა. ასევე მისი მეშვეობით მარტივად შეძლებთ Norton Internet Security, Norton Antivirusy, Norton Anty-Theft და Norton Mobile Security პროდუქტების ლიცენზიების მართვას. სასურველი სოფტის წაშლას, ისე, რომ ლიცენზია არ დაიკარგოს და ა. შ. ეს სერვისი თითქმის ანალოგიურია Mc Afee All Access თუმცა აქ ცალკეული სოფტებისათვის დამოუკიდებლად შეიძლება ლიცენზიის შეძენა.

ჭკვიანი ფაერვოლი Norton 360, - ის ფაერვოლი უსაფრთხოების სისტემის შემადგენელი ეს მნიშვნელოვანი ელემენტი, ახდენს პორტების სტელს რეჟიმში გადაყვანას, რითაც კომპიუტერს უხილავს ხდის.გარე ქსელიდან ფაერვოლის ავტოკონფიგურაცია მთლიანად ეფუძნება Norton Insignet მონაცემთა ბაზას. ამ გზით ის ადგენს მავნე ან პოტენციურად საშიში პროგრამების და ლინკების სიას, რათა დაბლოკოს ის. Core IM-PACT Penetration tool - ით განხორციელებული ტესტირებისას ფაერვოლმა პირველივე ცდაზე სატესტო სისტემის IP-ს შავ სიაში შეიყვანა და დაბლოკა, რაც შეეხება Norton Interney Security - ების პოვნას და მათ მოცილებას, ამ მხრივ Norton 360,ზუსტად იგივე მაჩვენებლით გამოირჩევა, როგორიც Norton Security გაააჩნდა 91%, თუმცა ჩამოყალიბდა Webroot აღნიშნული ოფცია გულისხმობს 2 გიგაბაიტი მოცულობის ონლაინ სივრცეს ბექაფისათვის, თუმცა დაბექაფებული ინფორმაციის შენახვა ლოკალურ ინფორმაციის მატარებლებზე შეიძლება.

დღეისათვის, როცა უამრავი ვირუსი და მავნე პროგრამა არსებობს, უსაფრთხოების საკითხი უდავოდ პრიორიტეტულია. ამ მხრივ არაერთი სოფტ დეველოპერი მუშაობს და საკმაოდ პროდუქტიულადაც.

განვიხილოთ სიტუაცია, როცა მავნე პროგრამა უკვე მყარადაა ჩამჯდარი სისტემაში და Real-Time Protection უკვე აზრს მოკლებულია. ხშირად ხდება, როცა მყარად ფესვგადგმული ვირუსი ბლოკავს ნებისმიერ ინსტალაციის მცდელობას და მისი მოცილება სისტემიდან დამხმარე სოფტის მეშვეობით შეუძლებელი ხდება. სწორედ ასეთი შემთხვევისათვის შეიქმნა Comodo Cleaning

Essentials. ის ინსტალაციის გარეშე ეშვება. მაგალითად USBფლეშ მეხსიერებიდან და მის სამიზნეს პოსტინფორმაციული სისტემა წარმოადგენს.

პროგრამის ინტერფეისი მარტივია. ის სულ სამი განყოფილებისგან შედგება smart scan მოიცავს სკანირების ე. წ. ჭკვიან მეთოდს. full scan- ის მეშვეობით Comodo Cleaning Essentials ძირეულად შეამოწმებს სისტემას და დიდი ალბათობით აღმოაჩენს ვირუსს. დამატებითი ეფექტისთვის შესაძლებელია დეტალური კონფიგურაციის შემუშავებაც. ასე მაგალითად დასაშვებია Master Boot Record (MBR) სკანერის ჩართვაც, რაც მიმდებარე სივრცეს შეამოწმებს ვირუსებზე.

გაშვებისთანავე სოფტი სისტემას გადატვირთავს და სტარტაპის შემდგომ ინტერნეტიდან განაახლებს საკუთარ თავს. ამის შემდეგ იგი უკვე სრულიად მზადაა ებრძოლოს rootkit – ებს და ათასი ჯურის მავნე პროგრამებს. სრული სკანირების დასრულების შემდეგ (რაც საკმაო ხანი გრძელდება). პროგრამა დეტალურ რეპორტს წარმოგვიდგენს, სადაც ასახულია ყველა მავნე სკრიპტი. მომხმარებელს შეუძლია თითოეული მათგანისათვის განსაზღვროს შესაძლო მოქმედებები, იქნება ეს წაშლა, იგნორირება თუ გაწმენდავირუსებისაგან. შესაძლებელია წინასწარ სპეციფიკური ფაილის იგნორირებაც მოვახდინოთ რათა სოფტმა შემთხვევით ისინიც არ გაისტუმროს წაშლილ ფაილთა სანაგვეზე. გამომდინარე უსაფრთხოების კონცეფციიდან Comodo Cleaning Essentials აქვს ფუნქცია რეპორტის Comodo სპეციალისტისათვის გაგზავნისა, ამ გზით ხდება სტატისტიკის შეგროვება და სოფტის მომავალი გაუმჯობესებების დაგეგმვა.

მას შემდეგ რაც პროგრამა სრულად ამოიცნობს ყველა მეტ – ნაკლებად მავნე სკრიპტს ის გადატვირთავს სისტემას, რათა საბოლოოდ განადგურდეს ვირუსები. ამის შესახებ კი ცალკე ანგარიშს შექმნის, სადაც წარმატებით დასრულებულ ოპერაციებთან ერთად malware – ებიც იქნება ასახული. მიუხედვად პლუსებისა სოფტს თავისი ნაკლიც აქვს. მას ხშირად გამორჩება ხოლმე წვრილმანი ელემენტები მავნე პროგრამებისა, თუმცა აღსანიშნავია, რომ მათ ბირთვს ის სრულად ანადგურებს და შემორჩენილი დეტალები უკვე არსებით საფრთხეს აღარ წარმოადგენს. ყველაზე ეფექტური Comodo Cleaning Essentiale rootkit – ებთან ბრძოლაში გამოდგა ტესტირებისას მან 100% – იანი შედეგი აჩვენა.

დამატებით ფუნქციებად შეიძლება განვიხილოთ Autorun Analyzer რომელიც მავნე პროგრამების გაშვების თექვსმეტ სხვადასხვანაირ ვარიანტს აანალიზებს და საჭიროების შემთხვევაში ბლოკავს მათ. ასევე Task Manager რომელიც ერთგვარი Comdo Cleaning Essentials არის, თუმცა მისი ძირითადი ფუნქცია მავნე პროცესების ამოცნობა და გაუვნებელყოფაა. იდეალური გადაწყვეტილება გამოდგა პოსტინფიცირების პერიოდში მყიფი სისტემის გასაცოცხლებლად, თუმცა ის რეალურ დროში დაცვის კუთხით უძლურია. შესაბამისად მისი გამოყენება რეკომენდირებულია მხოლოდ სანდო ანტივირუსთან ერთად პრიციპით. თუ ანტივირუსმა ვერ შეძლო საფრთხის გაუვნებელყოფა საქმეში ერთვება Comdo Cleaning Essentials. კომპიურტერული უსაფრთხოების მუქარათა მთელი სპექტრი

2.5. რისკების მართვით ორგანიზაციის უსაფრთხო ფუნქციონირების ანალიზის პროგრამული კომპლექსები

განვითარებულ ქვეყნებში კომპანიებს უჭირს გაერკვეს იუ – ს უზრუნველყოფისათვის სახსრების დაბანდების აუცილებლობაში, ძნელი წარმოსადგენი არაა თუ რამდენად პრობლემურია განვითარებას ქვეყნებში არა მარტო აღნიშნული ამოცანის გადაწყვეტა, არამედ თვით ბიზნესპროცესების, ორგანიზაციული მართვის ავტომატიზაციისა და მისი დონის განსაზღვრა და შესაბამისად, ამისათვის ინვესტიციების განხორციელების აუცილებლობა. ასეთ პირობებში განვითარებად ქვეყნებში ბიზნესის განვითარების, სხვადასხვა მასშტაბისა და დანიშნულების ორგანიზაციების, ეფექტურად ფუნქციონირებისთვის მნიშვნელოვანი ბიძგის მიმცემი იქნება ისეთი პროგრამული კომპლექსის ან კომპლექსების არსებობა, რომელთა მეშვეობითაც შესაძლებელი იქნება შეფასდეს ნებისმიერი ორგანიზაციის მიერ უკვე დასაბუთებული, რეალიზებადი მიზნის ეფექტურად მიღწევის შესაძლებლობა მის განკარგელებაში არსებული რესურსების პირობებში. ამასთანავე პროგრამული კომპლექსი უნდა იძლეოდეს არა მარტო ორგანიზაციული მართვის ინფორმაციული სისტემის იუ – ს უზრუნველყოფის ანალიზისა და აუდიტის შესაძლებლობას, არამედ თვით საწყისი მიზნის რეალურობის შეფასების, მომავალი ორგანიზაციის შექმნა – გაშვების $Z_{ს\text{ფ}}$

პროცესის წარმართვას რისკების მართვით ორგანიზაციის უსაფრთხო ფუნქციონირების ანალიზის შესაძლებლობაც.

ორგანიზაციის შექმნა – გაშვების პროექტში ბევრად ეფექტურია იყოს დაცული მიზანდასახული სისტემის ევოლუციური განვითარების „კიბის“ კანონი, რაც ტოლფასია იმისა, რომ უკვე რეალური მიზანი წარმოვადგინოთ მიზანთა სიმრავლის სახით

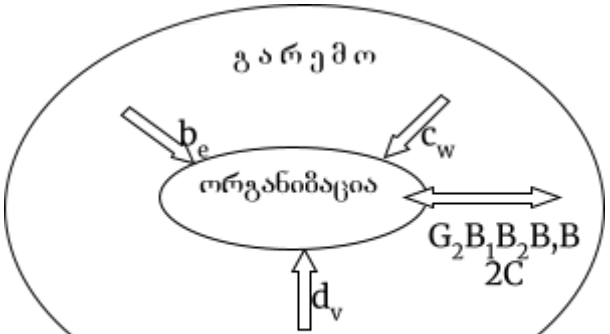
$Z_{ს\text{ფ}} \Rightarrow Z_{ს} = \{zi\}$ $i = \overline{1, I}$ (2.1.)

რომლის რეალიზაციისათვის მას გააჩნია რესურსების სიმრავლე

$R_e = \{z_{ei}\}$ $j = \overline{1, J}$ (2.2)

ორგანიზაციას შექმნა – გაშვების ეტაპზე განსაზღვრული უნდა ჰქონდეს ფუნქციათა ის სიმრავლე $Ф = \{Фn\}$, $n = \overline{1, N}$ რომელთა მეშვეობითაც ის შეცდება მიზნის რეალიზებისა და ჩამოყალიბების ორგანიზაციის ფუნქციურ სტრუქტურას, რომლის მეშვეობითაც მან უნდა წარმართოს შესავალი რესურსების მეშვეობით მოღვაწეობის შედეგების გამომუშავების პროცესები $\Psi_1^n, \Psi_2^n, ..., \Psi_m^n,\ m = \overline{1, M}$

იმას ნიშნავს, რომ თითოეული ფუნქციის Фm შესრულება დამოკიდებულია m პროცესზე, ისეთნაირად, რომ მაქსიმალურად ეფექტურად შესრულდეს ნებისმიერი n– ური ფუნქცია ორგანიზაციისა ამას კი ჭირდება ორგანიზაციაში ტექნოლოგიის ისე აწყობა, რომყოველი პროცესისათვის უზრუნველყოფილი იყოს შესაბამისი პარამეტრები $Q_1^n, Q_2^n, ..., Q_k^n,\ k = \overline{1, K}$ როგორც ორგანიზაცია ფუნქციონირებს ცალკეულ გარემოში და მან მიზნის რეალიზებისას აუცილებლად უნდა გაითვალისწინოს გარემოს ირიბი და პირდაპირი ზემოქმედებით შექმნილი გარემოს პარამეტრები (ნახ. 3):



ნახ. 3 ორგანიზაცია და მისი გარემო

1. გარემოს ორგანიზაციის წინააღმდეგ მომქმედი პარმეტრები $b_1, b_2,...,b_e$, $e = \overline{1,L}$

2. გარემოს ნეიტრალური (შემთხვევითი) პარამეტრები $C_1, C_2,...,C_w$, $w = \overline{1,W}$

3. გარემოს ხელშემწყობი პარამეტრები $d_1,d_2,...,d_v$, $v = \overline{1,V}$

რაც შეეხება ურთიერთობებს ორგანიზაციის (კომპანიის) სახელმწიფოსთან G2B პარტნიორებთან და სხვა ორგანიზაციებთან (კომპანიებთან) B2B მოლვაწეობის შედეგების მომხმარებლებთან (კლიენტებთან) B2C ეს პროცესები უნდა განვიხილოთ, როგორც აუცილებელი შემადგენელი ნაწილი ორგანიზაციის გარემოსთან ურთიერთობის პროცესის , რომელიც შეიძლება წარმოვადგინოთ ფუნქციონალის სახით:

$$\Psi_m^{(1)} = \Psi_m^{(1)}(\{Q_k^{(1)}\},\{be\},\{Cw\},\{dv\},t);\ m = \overline{1,M}, k = \overline{1,K}, \square = \overline{1,L}, w = \overline{1,W}, v = \overline{1,V} \quad (2.2.)$$

ცხადია ორგანიზაციას გააჩნია თავის შიდა პროცესები, რომლებიც შეიძლება წარმოდგენილი იყოს რამოდენიმე იერარქიის სახით:

$$\Psi_m^{(1)} = \Psi_m^{(1)}(\{Q_k^{(1)}\},\{be\},\{Cw\},\{dv\},t);\ e = \overline{1,E}, m = \overline{1,M}, k = \overline{1,K}, \square = \overline{1,L},, w = \overline{1,W}, v = \overline{1,V}$$

(2.3.)

სადაც E – ორგანიზაციისათვის საჭირო იერარქიათა რაოდენობაა.

თავის მხრივ სისტემის პარამეტრები {Qn} შეიძლება იცვლებოდეს გარემოს შესწავლისას, ის დამოკიდებულია მიზანდასახულ სისტემაში მიმდინარე პროცესებზე და წარმოდგენილია მდგომარეობათა ფუნქციონალის სახით

$$Q_k^{(1)} = Q_k^{(1)}(\Psi_1^{(2)}, \Psi_2^{(2)}, ..., \Psi_n^{(2)}) = Q_k^{(1)}(\{\Psi_m^{(2)}\}),\ k = \overline{1,K}, m = \overline{1,M}, \quad (2.4)$$

ორგანიზაციაში მიმდინარე პროცესების E იერარქიის სახით წარმოადგენისას მიზანდასახული სისტემის შესაძლო მდგომარეობები წარმოიდგინება პარამეტრების სიმრავლით E დონემდე: $Q = \{Q^{(1)}, Q^{(2)}, ..., Q^{(E)}\}$.

წარმოდგენილი მოდელი, სრულ სურათს იძლევა იმისა თუ როგორაა დამოკიდებული ორგანიზაციის მიზნის მისაღწევად საჭირო ფუნქციების განხორციელების პროცესები მიზანდასახული სისტემის მიერ უზრუნველყოფილ პარამეტრებზე გარემოს პარამეტრების გათვალიწინებით და ყველაფერი ეს უნდა კონტროლირდებოდეს მიზნობრივი ფუნქციების შესრულება არ შესრულებაზე. ამისათვის საჭიროა წარმოდგენილ მოდულში გათვალიწინებული იყოს ეფექტურობის ფუნქციონალი, რომელიც რაოდენობრივად ან ხარისხობრივად აღწერს კომპანიის მოღვაწეობას – აღნიშნული ფუნქციების შესრულება არ შესრულებას. კომპანიის მიერ n– ური ფუნქციის შესრულების ეფექტურობა

$$Э_n = Э_n(\Phi_n) = Э_m(\Psi_1^{(2)}, \Psi_2^{(2)}, ..., \Psi_m^{(2)}, ..., \Psi_M^{(2)}) = Э_n(\{\Psi_m^{(1)}\}),\ n = \overline{1,N}, m = \overline{1,M}, \quad (2.5)$$

ხოლო ორგანიზაციის ფუნქციონირების სართო ეფექტურობა ფასდება უკვე ვექტორი – ფუნქციონალით $Э = \{Э_n\}_n$ აქვე უნდა გავითვალისწინოთ ის გარემოება, რომ კომპანიაში მიმდინარე პროცესების სიმრავლე აქტიურობის მიხედვით შეიძლება დაიყოს ორ ძირითად სახედ: განმეორებადი (რომლებიც ხორციელდება პერიოდულად ან რაღაც ხდომილების დადგომის ფაქტის მიხედვით) და ერთჯერადი(ერთეულოვანი) პროცესებად, აქტიურობისპირველ სახეს უწოდებენ პროცესებს (ბიზნესპროცესებს), ხოლო მეორეს– პროექტებს. პროცესების წარმართვა გულისხმობს, რომ ორგანიზაციას გააჩნია შესაბამისი რესურსები (ყველაფერი ის რაც საჭიროა მიზნობრივი ფუნქციების პროცესების ისეთნაირად წარმართვისათვის, რომ მიღწეული იყოს ორგანიზაციის ძირითადი მიზანი). თუ ამ რესურსებს გავაიგივებთ ორგანიზაციის მიზნის რეალიზებისათვის საჭირო ინვესტიციასთან, მაშინ კომპანიის საქმიანობის საერთო ეფექტურობა, კოეფიციენტის სახით, უნდა აღემატებოდეს ერთს ან რაიმე წანასწარ გაანგარიშებულ სიდიდეს (რაღაც ერთზე მეტ ზღურბლურ მნიშვნელობას „z“

$$R_{oi} = \frac{mogeba - xarjebi}{investicia} > z > 1$$

(2.6)

ამის მიღწევა პირდაპირ კავშირშია ორგანიზაციის უნართან და შესაძლებლობასთან გაანალიზოს გარემოს პარამეტრების სიმრავლეები {be}– აქტიურად ორგანიზაციის ეფექტურობის დაქვეითების წინააღმდეგ მიმართული; {cv} – ნეიტრალურები, მაგრამ მათმა ცვლილებამ შემთხვევით შეიძლება გამოიწვიოს მიზნობრივი ფუნქციების პროცესის ეფექტურობის როგორც შემცირება, ასევე გაზრდა {dv} – ხელშემწყობი და ამას შეცნობა და გამოყენება უნდა.

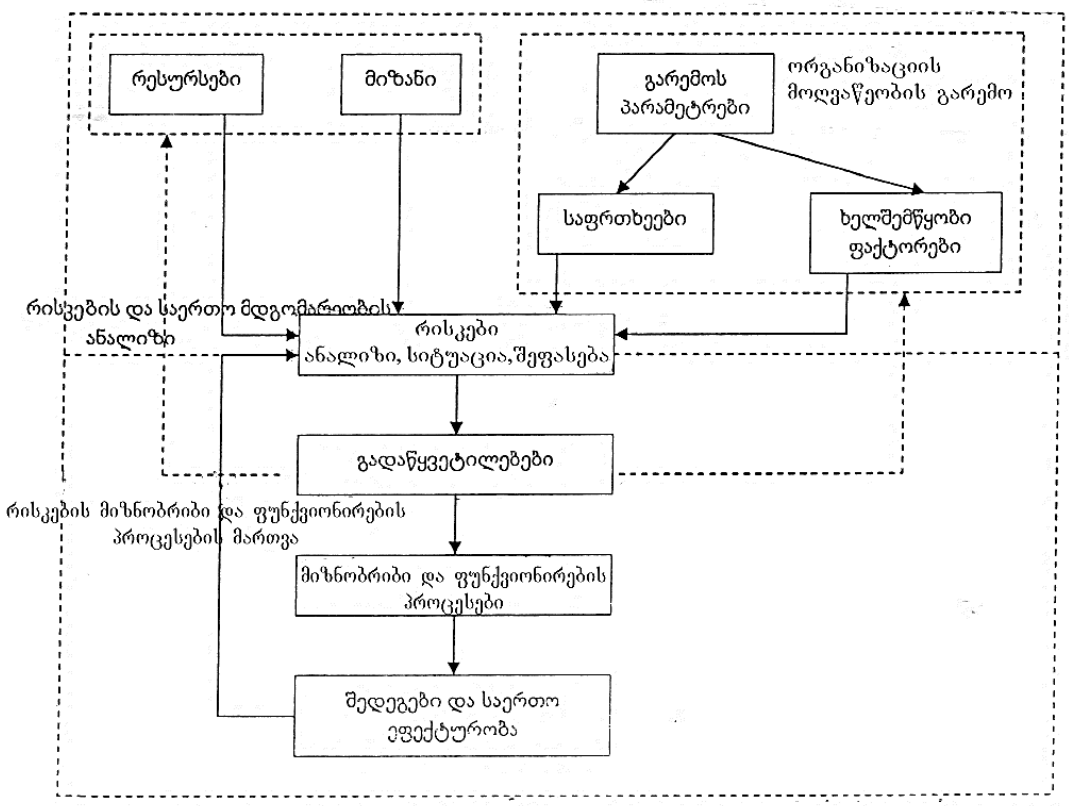
ფაქტიურად ფუნქციონირების გარემოს ყველა პარამეტრების სიმრავლე {dv} გამოკლებით სრულად გარკვეული საფრთხეების მატარებელია ორგანიზაციისთვის, რომლის შეუფასებლობამ ორგანიზაცია შეიძლება ძალიან სწრაფად მიიყვანოს კატასტროფამდე, შეწყვიტოს არსებობა. ორგანიზაციას ოპერატიულად უნდა შეეძლოს რეაგირება აღნიშნული პარამეტრების ცვლილებაბებზე რათა ისე შეცვალოს საკუთარი პროცესები და პარამეტრები, რომ წინ აღუდგეს მათი გავლენით მიზნობრივი ფუნქციონირების პროცესის ეფექტურობის რაიმე მერიოზულ დაქვეითებას, საჭიროების შემთხვევაში შეცვალოს საკუთარი ფუნქციებიც კი, ხოლო კატასტროფული რისკის წარმოშობისას შეცვალოს ორგანიზაციის მიზანი და ამოცანები, ე.ი. ფაქტიურად გარდაქმნას ორგანიზაცია სხვა მიზანდასახულ სისტემად. ძნელი არაა იმის დანახვა, რომ აქ საქმე გვაქვს საკმაოდ დინამიურ პროცესთან – საკუთრივ ორგანიზაციის მიზნობრივ ფუნქციონირების პროცესი პლუს გარემოს პარამეტრების ცვლილებები, ასეთ შემთხვევაში ორგანიზაციას უნდა გააჩნდეს იმის უნარი, რომ მაქსიმალურად ოპერატიულად მართოს შიდა პროცესები, გარემო პროცესების სისტემატური კონტროლის და თავისი წილი ზემოქმედებების ამის საფუძველზე კი გამოიმუშაოს მომავალი შესაძლო ღონისძიებათა გეგმა.

რისკების შეფასების ქვეშ იგულისხმება საერთო სიტუაციის შეფასება – არსებული გარემო პირობების, რუსურსების, ორგანიზაციის მიზნის და ამ მიზნის რუალიზეციის პროცესების და შედეგების მიხედვით ხდება გადაწყვეტილების

მიღება გაგრძელდეს პროცესი ადრინდელი სახით, ან შეიცვალოს პარამეტრები, ან საერთოდ შეიცვალოს მიზანი, ან კომპანიამ ეწყვიტოს ფუნქციონირება და ა. შ.

იმის გათვალისწინებით, რომ თანამედროვე პირობებში მცირე ბიზნესის წარმართვაც კი წარმოუდგენელია IT – ტექნოლოგიების გარეშე, ცხადია ორგანიზაციის სასიცოცხლო ციკლისათვის აუცილებელია IT- ტექნოლოგიების გამოყენებით მოხდეს რისკების და საერთო მდგომარეობის ანალიზის, ასევე მიზნობრივი ფუნქციების პროცესების ავტომატიზება, რაც საშუალებას იძლევა სწრაფად მოხდეს წარმოდგენილი კონცეფციის იმიტაციული მოდელის შექმნა და მისი დახმარებით ოპერატიულად გადაწყდეს რამდენად სარისკოა დასახული მიზნის არსებული რესურსების და გარემოს პირობებში ორგანიზაციის შექმნა და საქმიანობის წამოწყება, მისი წარმატებით განხორციელება და სასიცოცხლო ციკლის საჭირო ეფექტურობით წარმართვა.

გემოთ მოყვანილი გარემოებების გათვალისწინებით ორგანიზაცია საქმიანობის ავტომატიზებას, თან ახლავს სრულიად ახალი რისკები, რომლებიც დაკავშირებულია ორგანიზებული მართვის ავტომატიზებული სისტემის ინფორმაციული უსაფრთხოების უზრუნველსაყოფად, თან ეს რისკები აშკარად კატასტროფული ხასიათის მატარებელია, ვინაიდან მათმა შეუფასებლობამ ან გაუთვალიწინებლობამ, შესაძლებელია ძალიან ადვილად გამოიწვიოს ორგანიზაციისათვის სერიოზული ზიანის მიყენება. ამის მაგალითად ისიც საკმარისია თუ გავიხსენებთ, რომ ბანკები მილიონებს ხარჯავს თავისი ავტომატიზებული სისტემის იუ-ს უსაფრთხოების და კატასტროფამედეგობის უზურნველყოფაში.



ნახ. 4 მოქმედი ორგანიზაციის სასიცოცხლო ციკლი

თავი 3 რისკმენეჯმენტის თანამედროვე მეთოდები

3.1 ინფორმაციული რისკების ანალიზისა და კონტროლის თანამედროვე კომპლექსები– პროგრამული კომპლექს CRAMM–ის ძლიერი და სუსტი მხარეები

თანამედროვე მსხვილი ბიზნესისთვის გადამჭრელი (სასიცოცხლო) მნიშვნელობა აქვს ინფორმაციულ უსაფრთხოებას, ამიტომ თანამედროვე ბიზნესისთვის ძირითადი საკითხია – როგორ შეფასდეს იუ – ში დაბანდების საჭირო დონე მოცემულ სფეროში ინვესტიციის მაქსიმალური ეფექტურობის უზურნველსაყოფად. ამ საკითხის გადასაწყვეტად არსებობს ერთი ხერხი – გამოყენებულ იქნას რისკების სისტემური ანალიზი, რომელიც საშუალებას იძლევა შეფასდეს სისტემაში არსებული რისკები და შეირჩეს ეფექტურობის თვალსაზრისით ოპტიმალური ვარიანტი (შეფარდებით სესტემაში– არსებული რისკების/შეფარდება იუ –ზე ხარჯებთან).

განვიხილოთ, კომპანიის ინფორმაციული უსაფრთხოებაში ინვსტიციების აუცილებლობის საკითხები. პირველ რიგში განვსაზღვროთ ის ფაქტორები რაც ხელს უშლის კომპანიას იუ – ს უზრუნველყოფის ზომების გატარებაში. ეს ფაქტორებია:

· ბიუჯეტის შეზღუდვა;

· ხელმძღვანელობის მხრიდან მხარდაჭერის არ არსებობა;

ფაქტიურად აქ საქმე გვაქვს შემთხვევასთან, როცა კომპანიის ხელმძღვანელობა ვერ აცნობიერებს, თუ რატომ უნდა ჩადოს ფული იუ – ს უზრუნველყოფაში. ხშირად ითვლება, რომ ძირითადი პრობლემა მდგომარეობს იმაში, რომ IT– ის სპეციალისტებს თვითონაც უჭირთ შეაფასონ, თუ რაში უნდა დაიხარჯოს ფული, რამდენად არის ეს საჭირო კომპანიის სისტემის დაცულობის უზრუნველსაყოფად და,რომ ხარჯები არ აღმოჩნდა ფუჭი ან გადაჭარბებული.

თუ IT – მენეჯერს ნათლად აქვს წარმოდგენილი, რა თანხა შეიძლება დაკარგოს კომპანიამ მუქარების რეალიზაციის შემთხვევაში სისტემის ყველაზე მოწყვლად (სუსტ) ადგილებში, რა ზომები უნდა გატარდეს დაცულობის დონის ასამაღლებლად ზედმეტი ფულის დახარჯვის გარეშე და ყველაფერი ეს დადასტურებულია დოკუმენტალურად, მაშინ კომპანიის ხელმძღვანელობის

დარწმუნების ამოცანა გადაწყვეტილიადა ის, დიდი ალბათობით, ყურადღებას მიაქცევს და გამოყოფს სახსრებს იუ – ს უზრუნველსაყოფად.

ინფორმაციული რისკების სისტემურ ანალიზთან დაკავშირებული ამოცანების გადასაწყვეტად, ინფორმაციული ტექნოლოგიების მსოფლიოს წამყვან კომპანიებში დამუშავებულ იქნა ინფორმაციული რისკების ანალიზისა და კონტროლის პროგრამული კომპლექსები, ასე მაგალითად, დიდ ბრიტანეთში პროგრამული კომპლექსი CRAMM, აშშ-ში პროგრამული კომპლექსი Risk Wotsh და რუსეთში პროგრამული კომპლექსი ГРИФ.

მოკლედ დავახასიათოთ პროგრამული კომპლექსი CRAMM

პროგრამული კომპლექსი CRAMM შეიქმნა დიდ ბრიტანეთში 1985 წელს და დღემდე, მთელ მსოფლიოში დიდი პოპულარობით სარგებლობს. რისკების ანალიზის გარდა ეს პროგრამული კომპლექსი საშუალებას იძლევა გადაწყდეს მთელი რიგი აუდიტორული ამოცანები, როგორიცაა:

· ინფორმაციული სისტემის გამოთვლების ჩატარება და თანმხლები დოკუმენტაციის გამოშვება მისი ჩატარების თითოეულ ეტაპზე;

· აუდიტის ჩატარება ბრიტანეთის მთავრობის მოთხოვნების, ასევე სტანდარტის BS7799: 1935 შესაბამისად - Code of Practice for Information Security Management BS7799

· უსაფრთხოების პოლიტიკის და ბიზნესის უწყვეტობის უზრუნველყოფის გეგმის დამუშავება;

GRAMM მეთოდს საფუძვლად უდევს რისკების შეფასებისადმი კომპლექსური მიდგომა , რომელშიც შეხამებულია რაოდენობრივი და ხარისხობრივი ანალიზის მეთოდები. მეთოდი უნივერსალურია და შეიძლება გამოყენებულ იქნას, როგორც დიდი, ასევე მცირე ორგანიზაციებისთვის, როგორც სახელმწიფო ასევე კომერციული სექტორებიდან.

ანალიზის და კონტროლის პროგრამული კომპლექსებიCRAMM პუ – ს ვერსიები, რომლებიც ორიენტირებულია სხვადასხვა ტიპის ორგანიზაციებზე. ერთმანეთისგან განსხვავდებიან თავისი ცოდნის ბაზებით. კომერციული ორგანიზაციისთვის არის კომერციული პროფილი, სამთავრობო ორგანიზაიციისთვის – სამთარობო პროფილი. ეს ბოლო ვარიანტი საშუალებას იძლევა ჩატარდეს აუდიტი აშშ – ს სტანდარტთან ITSBC(„ნარინჯისფერი წიგნი“)

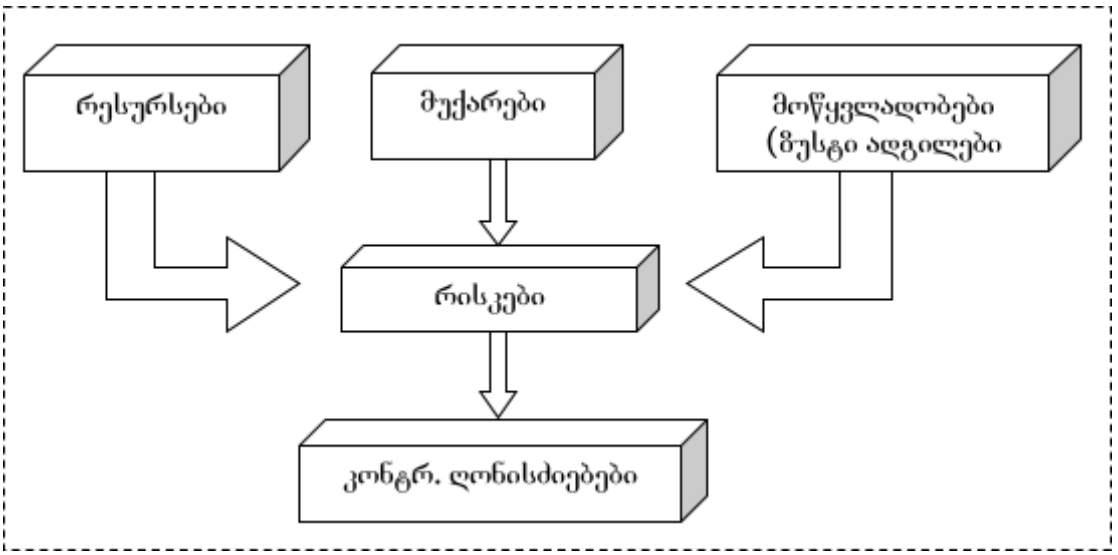
შესატყვისად. საბოლოო ჯამში მეთოდი საშუალებას იძლევა შემუშავებულ იქნას რისკების მართვის ეკონომიურად დასაბუთებული სტრატეგია, მოხდეს საშუალებების ეკონომია და თავიდან იქნას აცილებული გაუმართლებელი ხარჯები.

CRAMM- ში გათვალისწინებულია სამი ეტაპი:

- პასუხი უნდა გაეცეს კითხვას: „საკმარისია თუ არა სისტემის დასაცავად ბაზური დონის საშუალების გამოყენება, რომელიც ახორციელებს უსაფრთხოების ტრადიციული ფუნქციების რეჟიმების დეტალურ ანალიზს.
- ხდება რისკების იდენტიფიკაცია და ფასდება მათი სიდიდე;
- წყდება ადეკვატური კონტრღონისძიებების არჩევის საკითხი.

აღნიშნული მეთოდი, ღონისძიებების თანმიმდევრული ჩატარების ყოველი ეტაპისთვის განსაზღვრავს საწყისი მონაცემების, სიების შემოწმებისა და საანგარიშო დოკუმენტების ნაკრებს.

ახალი კონტრზომების დანერგვის და ძველების მოდიფიკაციის შესახებ გადაწყვეტილების მიღებისას შესაძლებელია აუდიტორს დაეკისროს ახალი კონტრზომების დანერგვის გეგმის შედგენა და მისი გამოყენების ეფექტურობის შეფასება. ამ ამოცანების გადაწყვეტა გამოდის CRAMM მეოთდიკის ჩარჩოებიდან.



ნახ. 5 კონტრღონისძიებების არჩევის სქემა

რა ნაკლოვანებები გააჩნია CRAMM- ს:

- ამ მეთოდის გამოყენება მოითხოვს აუდიტორის სპეციალურ მომზადებას და მაღალ კვალიფიკაციას;
- ეს მეთოდი ბევრად უფრო უკეთესადაა მორგებული უკვე არსებული ს აუდიტისთვის, რომლებიც იმყოფება ექსპლუატაციაში, ვიდრე პროექტირების სტადიაში მყოფისთვის;
- ამ მეთოდით აუდიტი – საკმაოდ შრომატევადი პროცესია და შეიძლება დასჭირდეს აუდიტორის თვეობით მუშაობა;
- CRAMM პროგრამული ინსტრუმენტი გენერირებს დიდი რაოდენობით ქაღალდის დოკუმენტაციას. რომელიც პრაქტიკაში ყოველთვის როდი დარჩება სასარგებლო;
- აღნიშნული მეთოდი არ იძლევა იმის საშუალებას, რომ შეიქმნას საკუთარი შაბლონი ან მისცეს არსებულის მოდიფიცირება.
- CRAMM- ის ცოდნის ბაზაში დამატების შესაძლებლობა მიუწვდომელია მომხმარებლებისთვის; რაც ქმნის გარკვეულ სირთულეებს ამ მეთოდის კონკრეტული ორგანიზაციის საჭირო მოთხოვნებთან ადაპტაციისას.
- CRAMM- ს არსებობს მხოლოდ ინგლისურ ენაზე;
- ლიცენზიის მაღალი ღირებულება.

  CRAMM მოიცავს აუდიტებისა და რისკების ანალიზის შემდეგ საშუალებებს;

· Rick watch for Physical Security – ის დაცვის ფიზიკურ მეთოდებისთვის;

· Rick watch for Information Systems – ინფორმაციული რისკებისთვის;

· Heppa-Watch for Healthcare Industry -HIPAA – სტანდარტთან შესატყვისობის შესაფასებლად.

რისკების შეფასებისა და მართვის აღნიშნული მეთოდი, კრიტერიუმების სახით, იყენებს „წლიური დანაკარგების წინასწარმეტყველებას“ და „ინვესტიციებისაგან დაბრუნების“ შეფასებას.

ამ მეთოდში შედის პროგრამული პროდუქტების მთელი ოჯახი, რომელსაც გააჩნია შემდეგი დადებითი თვისებები:

- მეთოდი გვეხმარება ჩატარდეს რისკების ანალიზი და განხორციელდეს დაცვის ზომებისა და საშუალებების დასაბუთებული შერჩევა.

პროგრამაში გამოყენებული მეთოდიკა მოიცავს 4 ფაზას:

I ფაზა – კვლევის საგნის განსაზღვრა. ამ ეტაპზე ხდება ორგანიზაციის პარამეტრების აღწერა – ორგანიზაციის ტიპი, საკვლევი სისტემის შემადგენლობა, ბაზური მოთხოვნები უსაფრთხოების სფეროში. ხდება მთელ რიგ ქვეპუნქტებში აღწერების ფორმატიზირება რომლებიც შეიძლება შეირჩეს უფრო დეტალური შესწავლისთვის ან საერთოდ, გამოტოვებულ იქნას.

ანალიტიკოსის მუშაობის შესამსუბუქებლად, ყველა არჩეული პუნქტი აღიწერება დეტალურად. შაბლონებში აისახება დასჯადი რესურსების კატეგორიების დანაკარგების, მუქარების, მოწყვლადობებისა და დაცვის ზომების ნუსხა. ამ ჩამონათვალიდან უნდა შეირჩეს ის, რომლიც რეალურად არის ორგანიზაციაში გამოვლენილი.

II ფაზა – შეტევა იმ მონაცემებზე, რომლებიც აღწერს სისტემის კონკრეტულ მახასიათებლებს. შესაძლო მოწყვლადობების გამოსავლენად გამოიყენება კითხვარი, რომლის ბაზაც შეიცავს 600 – ზე მეტ შეკითხვას. შეკითხვები დაკავშირებულია რესურსების კატეგორიებთან. დასაშვებია შეკითხვების კორექტირება, ამოსაღების გამოვლენა ან ახლის დამატება. გაანალიზდება ისეთი მონაცემები, როგორიცაა: ყოველი გამოყოფილი მუქარის წარმოშობის სიხშირე, მოწყვლადობის ხარისხი და რესურსების ფასი (ღირებულება, მნიშვნელობა). ყოველივე ეს გამოიყენება დაცვის საშუალებების დანერგვის ეფექტურობის შესაფასებლად.

III ფაზა – რისკების შეფასება თავდაპირველად ხდება რესურსებს, დანაკარგებს, მუქარებსა და მოწყვლადობებს შორის, რომლებიც გამოყოფილი იქნა წინა სტადიებზე,კავშირების დამყარება. რისკებისთვის ხდება მოსალოდნელი დანაკარგების მათემატიკური მოლოდინის გათვლა წლის განმავლობაში . ფორმულით

$$m = P * V$$

სადაც P – მუქარის წარმოშობის სიხშირეა წლის განმავლობაში, V – რესურსის ღირებულება, რომელიც განიცდის მუქარის ზემოქმედებას.

მაგალითად, თუ სერვერის ღირებულებაა 150 000, ხოლო ალბათობა იმისა, რომ ის იქნება განადგურებული ხანძრის შედეგად ტოლია 0, 01, მაშინ მოსალოდნელი დანაკარგი იქნება

m = 0,01 x150 000 = $1500

დამატებით განიხილება სცენარები „რა თუ...“, რომლებიც საშუალებას იძლევა აღიწეროს ანალოგიური სიტუაციები დაცვის საშუალებების დანერგვის პირობებში, მოსალოდნელი დანაკარგების დაცვის ღონისძიებების შედარებით– დანერგვით და მის გარეშე, ით. შესაძლებელია შეფასდეს ასევი ღონისძიებების დანერგვის ეფექტიანობა.

IV ფაზა – ანგერიშების გენერაცია. ანგარიშების ტიპებია:

– ელემენტების შესახებ მოკლე და სრული ანგარიშები, რომლებიც აღწერილია პირველ და მეორე სტადიებზე;

– დასაცავი რესურსების ღირებულების ანგარიშები,მათ შორის მოსალოდნელი დანაკარგების, მუქარების რეალიზაციის შემთხვევაში. ანგარიშების, მუქარებისა და უკუზემოქმედების ზომებისა დაანგარიში უსაფრთხოების აუდიტის შედაგების შესახებ.

მეთოდის ნაკლოვანებები:

·მეთოდი არ ითვალისწინებს იუ – თან კომპლექსურ მიდგომას.

ასეთი ნაკლოვანებები მისაღებია, თუ არ არის საჭირო რისკებისანალიზის ჩატარება, დაცვის პროგრამული, ტექნიკური დონის, ორგანიზაციული და ადმინისტრაციული ფაქტორების გათვალისწინება.ამ შემთვევაში, რისკების მიღებული შეფასება, ვერ ამოწურავს რისკის გაგებას სისტემური პოზიციებიდან

· Risk watch– პუ არსებობს მხოლოდ ინგლისურ ენაზე.

· ლიცენზიის მაღალი ღირებულება (15 000 დოლარი ერთი სამუშაო ადგილი, არც ისე დიდი კომპანიისთვის; 125 000 დოლარი კორპორაციული ლიცენზიისთვის).

ინფორმაციული რისკების სრული ანალიზის ჩასატარებლად, პირველ რიგში აუცილებელია აიგოს ინფორმაციული სისტემის სრული მოდელი, ინფორმაციული უსაფრთხოების თვალსაზრისით. ГРИФ გააჩნია მომხმარებლისთვის მარტივად, ინტიუტიურად გასაგები ინტერფეისი, მაგრამ გარეგნული სიმარტივის შიგნით,

იმალება რისკების ანალიზის რთული ალგორითმი, რომელიც ითვალისწინებს 100 – ზე მეტ პარამეტრს, რომელიც საშუალებას იძლევა მიღებული იქნას ინფორმაციულ სისტემაშიარსებული რისკებისმაქსიმალურად ზუსტი შეფასება, რომელიც ეფუძნება ინფორმაციულ სისტემის პრაქტიკული რეალიზაციის ღრმა ანალიზს.

ГРИФ სისტემის ძირითადი ამოცანაა – მისცეს შესაძლებლობა IT – მენეჯერს დამოუკიდებლად (ექსპერტების მოწვევის გარეშე) შეაფასოს რისკების დონე ის – ში, შეაფასის კომპანიაში არსებული უსაფრთხოების უზრუნველყოფის პრაქტიკა და დაუმტკიცოს კომპანიის ხელმძღვანელობას კომპანიის ინფორმაციულ უსაფრთხოების სფეროში ინვესტიციების ჩადების აუცილებლობა.

I – ეტაპი – ხდება IT მენეჯერის გამოკითხვა, რათა გაირკვეს კომპანიისთვისღირებული. ინფორმაციული რესურსების სრული ნუსხა

II ეტაპი – ხდება IT – მენეჯერის გამოკითხვა იმ მიზნით, რომ ГРИФ – ში შეტანილი იქნას კომპანიისთვისფასეული ყველა ინფორმაციულისახეობა;

დასკვნითი ფაზა – მითითებული იქნას ზარალი ყოველი ღირებული ინფორმაციის ჯგუფისთვის, რომლებიც განლაგებულია შესაბამის რესურსებში, ყველა სახის მუქარების მიხედვით.

III ეტაპი – თავიდან ხდება მომხმარებელთა ჯგუფების დადგენა (მომხმარებლთა რაოდენობა ყოველ ჯგუფში). განისაზღვრება რესურსების რომელი ჯგუფის ინფორმაციასთან აქვს დაშვება თითოეულ მომხმარებლს. დასკვნითი ნაწილში განისაზღვრება სახე (ლოკალური და /ან დაშორებული) და მომხმარებლის. ყველა რესურსთან, რომელიც შეიცავს ღირებულ ინფორმაციას, დაშვებისუფლებები (წაკითხვა. ჩაწერა, მოშორება).

IV ეტაპი – ხდება IT – მენეჯერის გამოკითხვა იმ დაცვის საშუალებების დასადგენად, რომლითაც დაცულია ღირებული ინფორმაცია. გარდა ამისა სისტემაში ხდება ერთჯერადი, გამოყენებული დაცვის საშუალებების შეძენისა და ტექნიკური მხარდაჭერისთვის ყოველწლიური დანახარჯების,ასევე კომპანიის იუ – ს სისტემის თანხლებაზეყოველწლიური დანახარჯების შესახებ ინფორმაციის შეტანა.

V ეტაპი – დასკვნით ეტაპი. ამ ეტაპზე მომხმარებელმა უნდა უპასუხოს სისტემაში რეალიზებულდაცვის პოლიტიკის შესახებშეკითხვების ჩამონათვალს, რაც

საშუალებას მოგვცემს შეფასდეს სისტემის დაცულობის რეალური დონე და მოხდეს რისკების დეტალიზაცია.

პირველ ეტაპზე, აღნიშნული ინფორმაციული დაცვის საშუალებების არსებობა, მათი არაადექვატური გამოყენებისა და დაცვის კომპლექსური პოლიტიკის არარსებობის (რომელიც უნდა ითვალისწინებდეს დაცვის ყველა ასპექტს) შემთხვევაში,თავისთავად ვერ გახდის სისტემას უფრო დაცულს. გათვალისწინებული უნდა იყოს უსაფრთხოების ყველა ასპექტი: ორგანიზაციული დაცვის, ფიზიკური უსაფრთხოებისადა პერსონალის უსაფრთხოების. და ა. შ. საკითხები.

ჩამოთვლილი, ყველაეტაპის შესრულების შედეგად, ფორმირდება დაცვის ინფორმაციული უსაფრთხოების მოდელი, რომელიც საშუალებას იძლევა მოხდეს გადასვლა შეტანილი მონაცემების პროგრამულ ანალიზზე, რათა მიღებულ იქნას რისკების კომპლექსური შეფასება და მოხდეს ჯამური ანგარიშის ფორმირება .

მეთოდის ნაკლოვანებები:

1. არ არსებობს მიბმა ბიზნესპროცესებთან, 2. არ არის შესაძლებლობა ჩატარდეს დაცულობის უზრუნველყოფის კომპლექსური ზომების დანერგვის სხვადასხვა ეტაპისანგარიშების შედარებითი ანალიზი,
3. არ არსებობს შესაძლებლობა დამატებულ იქნას მოცემული კომპანიისათვის სპეციალური უსაფრთხოების პოლიტიკის მოთხოვნები.

3.2. ინფორმაციული რისკების მართვისა და კანონმდებლობის მოთხოვნების უზრუნველყოფის ინფორმაციული ტექნოლოგიები , Compliance – ის ინფრასტრუქტურა.

თანამედროვე ცივილიზაცია სულ უფრო დამოკიდებული ხდება ინფორმაციულ ტექნოლოგიებზე, მათ ფართო გამოყენებაზე ადამიანის მოღვაწეობის თითქმის ყველა სფეროში. დღეისათვის განვითარებული ქვეყნების არსებობაც კი წარმოუდგენელია ელექტრონული ხელისუფლების გარეშე. სრული მასშტაბით ხდება მსხვილი, საშუალო თუ მცირე ბიზნეს კომპანიებსა და სხვა ტიპის საწარმოებში ავტომატიზებული სისტემების დანერგვა – განვითარება. მოკლედ,

ინფორმაციული ტექნოლოგიების გამოყენება იქცა ნებისმიერი მასშტაბისა და ტიპის მიზანმიმართული სისტემის განუყოფელ ნაწილად და ცხადია, პირველ პლანზეა ასეთი სისტემების ფუნქციონირების, მათში მონაცემების პერსონალებიდან დაწყებული კორპორაციული და სახელმწიფო მნიშვნელობის მონაცემებით დამთავრებული, სახელმწიფო დონეზე საკანონმდებლო – ნორმატიული მხარდაჭერა. პერსონალური მონაცემების დაცვის უზრუნველყოფა მხოლოდ ნაწილია იმ რთული ღონისძიებების კომპლექსისა, რომელმაც უნდა უზრუნველყოს ინფორმაციული ტექნოლოგიების ეფექტური მართვა, რისკების მართვა და კანონმდებლობის მოთხოვნების შესრულება.

ღონისძიებათა ერთობლიობას, რომელიც მიმართულია აღნიშნული პრობლემის გადასაწყვეტად, ეწოდება GRC-Governance, risk management and compliance - ეფექტური მართვა, რისკების კონტროლი და კანონმდებლობის მოთხოვნების შესრულება. ხოლო ღონისძიებათა ერთობლიობამ, რომელიც მიმართულია პრობლემის გადასაწყვეტად, მიიღო სახელწოდება Compliance infrastructure Market, ბაზრის ინფრასტრუქტურა - გადაწყვეტილებები, რომლებიც მიმართულია კანონმდებლობის მოთხოვნების შესასრულებლად.

Compliance Infrastructure Market - ესაა აპარატურულ და პროგრამულ უზრუნველყოფაზე გაწეული ხარჯებისერთობლიობა, აგრეთვე იტ-ისიმ მომსახურეობაზე, რომელიც განკუთვნილია ეფექტური მართვის, რისკების კონტროლისა და კანონმდებლობის მოთხოვნების უზრუნველყოფაზე. აუცილებელი ზომების გასატარებლად.

SOX (Sarbanes – Oxley Act) - სერბეინს - ოქსლის კანონი, რომელიც ამყარებს მოთხოვნებს ფინანსურ ანგარიშგებასა და მისი მომხადების პროცესზე. ამ კანონის თანახმად ღია სახის სააქციო საზოგადოებისთვის იქმნება ფინანსული მოღვაწეობის კონტროლისა და რეგულირების ახალი რეჟიმი, ხორციელდება არსებითი ცვლილებები ინფორმაციის მართვისა და გახსნის მოთხოვნათა სფეროში. დოკუმენტებში განხილულია საკითხები: აუდიტორების დამოუკიდებლობაზე, კორპორაციული პასუხისმგებლობაზე. ფინანსურ გამჭირვალეობაზე, ინტერესების კონფლიქტზე და სხვა.

Basel II - ნორმატიული დოკუმენტი, რომელიც მიმართულია საბანკო საქმეში რისკების მართვის ხარისხის ამაღლებაზე. დოკუმენტი ითხოვს ბანკებიდან

დანერგონ არა მარტო რისკებისადმი უფრო მგრძნობიარე, საკრედიტო რისკების შეფასებები, არამედ ამაღლებულ ყურადღებას ოპერაციული რისკების მიმართ, რომელიც წარმოადგენს საბანკო პრობლემების მთავარ მიზეზს.

Corporate governance - ნორმატიული დოკუმენტები, რომლებიც განსაზღვრავს კორპორაციის მუშაობის მართვისა და კონტროლის პროცესს.ეს არის სისტემა, რომლის საშუალებითაც ხდება აქციონერული საკუთრების უფლების რეალიზება, რომელიც წარმოადგენს მენეჯმენტს, დირექტორთა საბჭოს, ინვესტორებსა და გავლენის სხვა ჯგუფებს შორისურთიერთობისკომპლექსს.

eDiscovery - ნორმებისერთობლიობა, რომლებიც არეგლამენტებს სასამართლო განხილვებზე ელექტრონული დოკუმენტების წარმოადგენას. მოცემული პროცედურა დაკავშირებულია ელექტრონული სახით წარმოადგენილი ინფორმაციის ანალიზთან.

დღეს,საწარმოების უმეტესობა მნიშვნელოვანი ინფორმაციის ნაწილს ინახავს ელექტრონულ ფორმატში. ელექტრონულ ინფორმაციას, როგორც წესი თან ახლავს მეტამონაცემები. ოპერაციები ელექტრონულ დოკუმენტებზე, კერძოდ კი ოპერაციები მეტამონაცემებზე, ქმნის დოკუმენტების ფალსიფიკაციის შესაძლებლობას. eDiscovery წარმოადგენს სამოქალაქო და სისხლის სამართლის პროცესების მნიშვნელოვან ნაწილს და დაკავშირებლუია ელექტრონული დოკუმენტების უტყუარობის (ნამდვილობის) დამტკიცების პროცედურებთან. თუ კომპანია ჩართულია სასამართლო გარჩევაში, არსებობს ალბათობა იმისა, რომ მისგან მოითხოვენ პოტენციური სამხილები ციფრულ ფორმატშიწარდგენას. მასალების წარმოდგენისუუნარობა შეიძლება იქცეს სასამართლო პროცესის ხელშემშლელ ბარიერადდა შეამციროს კომპანიის სასამართო საქმის მოგებისშანსი.

HIPAA – ნორმატიული დოკუმენტი, რომელიც არეგლამენტირებს ზოგიერთ ასპექტს, რომელიც დაკავშირებულია სამედიცინო დაზღვევებთან, კერძოდ მოწოდებულია დაიცვას პერსონალური სამედიცინო ონფორმაციის პრივატულობა.

SB13.86 - ნორმატიული აქტი, რომელიც ახდენს პერსონალური მონაცემების პრივატულობის რეგლამენტაციას.

FISMA – ნორმატიული დოკუმენტი, რომელიც ახდენს ინფორმაციული რესურსების დარღვევის საკითხების რეგლამენტაციას, რომელმაც შეიძლება ზიანი მიაყენონ აშშ – ს ეკონომიკურ და ნაციონალურ უსაფრთხოებას.

GLBA – კანონი, რომელიც რეგლამენტაციას უკეთებს „ფინანსური ინსტიტუტების“ კლიენტების პერსონალური ინფორმაციის უსაფრთხოებასა და კონფიდენციალობას.

აღნიშნული დოკუმენტები მოიცავსრისკებისყველა დონეს, რომლიც დაკაშირებულია ინფორმაციის შექმნის, შენახვისა და გადაცემის წესების დარღვევასთან, როგორც სახელმწიფო და კორპორაციულ, ასევე პერსონალურ დონეზე.

Compliance – ინფრასტრუქტურამ უნდა უზრუნველყოს მოღემული ნორმატიული აქტების მთელი ერთობლიობისშესრულება. ამავე დროს ცხადია, რომ ნორმატიული აქტები ატარებს აღწერილობით ხასიათს. კომპანიის, რომელიც ქმნის Compliance – ინფრასტრუქტურას, ამოცანაა გადაიტანოს ეს წესები იტ –ის პოლიტიკის ნაკრებში, მოახდინოს კომპანიის მონაცემების შექმნას, მხარდაჭერასა და გაცვლასთან დაკავშირებული ყველა იტ რესურსის იდენტიფიცირება, რაც ამავდროულად, უნდა შეესაბამებოდეს ამ პოლიტიკას. აგრეთვე, ორგანიზაცია გაუკეთოსიმ გადაწყვეტილებებს, რომლებიც მხარს დაუჭერს მოცემულ იტ –ის პოლიტიკას დანართების, მონაცემებისა და ინფორმაციის შენახვის სისტემებთან მიმართებაში და უზრუნველყოფს მათი შესრულების კონტროლს.

Compliance – ის ინფრასტრუქტურამ უნდა უზრუნველყოს საქმიანი ინფორმაციის უსაფრთხო გამოყენება და გაცვლა, როგორც კომპანიის შიგნით, ასევე კომპანიებს შორის, უზრუნველყოს ინფორმაციის შეღწევადობა და ურღვევობა, საშუალება მისცეს მეწარმეებს უკეთ მოახდინოს მასთან კორპორაციული იტ – ის გარემოს ცვლილებები, უზრუნველყოსიტ–ის პროცესებისმომსახურება და შეღწევადობა (ხელმისაწვდომობა)იმ დონეზე, როგორც ეს SLA –შიადაფიქსირებული.

ამ სფეროში გადაწყვეტილებები დაიყვანება ჩანაწერების, იტ–ის ინფრასტრუქტურის, იტ–ის ოპერაციების, განრიგების ხელმისაწვდომობისა და უსაფრთხოების მართვაზე.

GRC შეიძლება პირობითად დაიყოს ორ ნაწილად – GRC ინფორმაციის მართვის და GRC იტ – მართვის. GRC ინფორმაციის მართვა პირველ რიგში აკონტროლებს ელექტრონული ინფორმაციის შექმნისა და შენარჩუნების საკითხებსა და მონაცემების კონფიდენციალობის უზრუნველყოფას.

GRC იტ – ს მართვა ფოკუსირებულია იტ – ის ინფრასტრუქტურის ურღვევობის და იმ პროცესების უწყვეტობას, რომლებიც ახორციელებს ინფორმაციის შენახვასა და დაცვის უზრუნველყოფას. ამ დროს ცხადია, რომ ორივე GRC ეფუძნება მთელ რიგ საერთო შენახვის, დაცვისა და ინფორმაციული სისტემების მხარდამჭერ ქვესისტემებს.

3.3 სტრატეგიული დაგეგმვისა და რისკმენეჯმენტის პროცესების ინტეგრაცის საკითხები

თანამედროვე ორგანიზაციები, კომპანიები აწყდება რისკებისმთელ სპექტრს: სტრატეგიულ, ოპერაციულ, სავალუტო და ა. შ. დღე არ გადის მორიგი ჩამოწერების, ზარალისა და გაკოტრებების გარეშე, რომელთა მიზეზიც გახდა რისკების მართვის დაბალი ხარისხი. რა არის კორპორატიული რისკების მართვა (ERM, Enterprise Rick Management) და როგორ იყენებს წამყვანი კომპანიები ამ მეთოდიკას, რომ არ გაკოტრდეს მძიმე პერიოდებში?

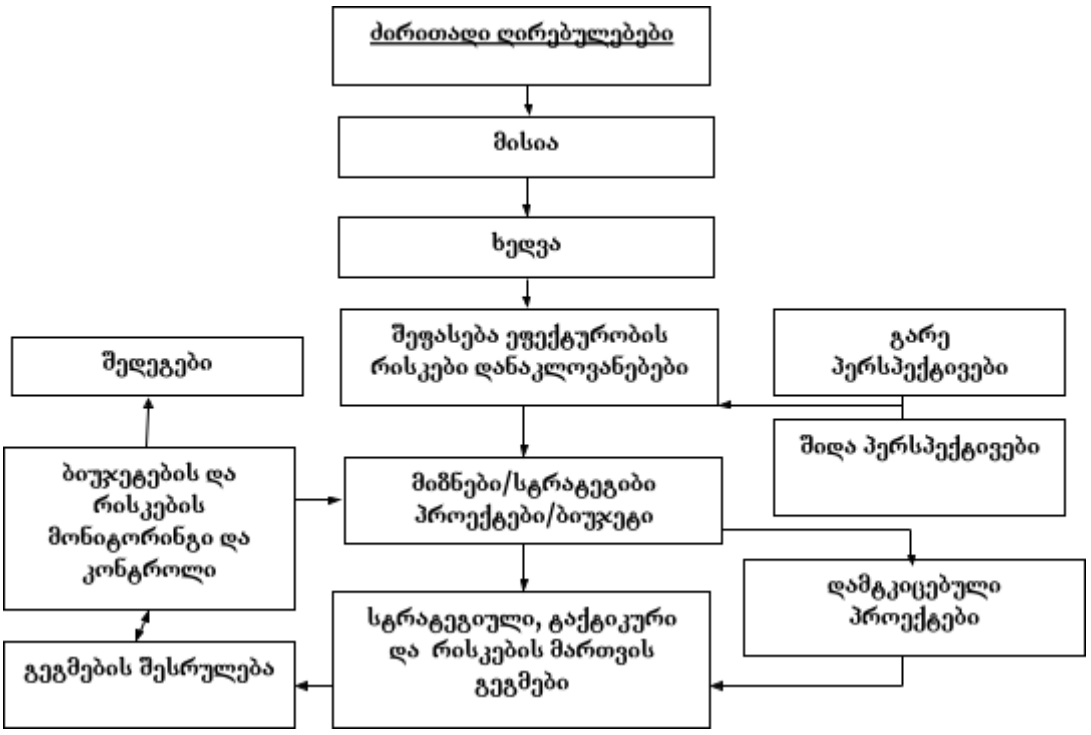
ა) პროცესებზე დაფუძნებული სტრატეგიული მენეჯმენტი,- UI –United Illuminating comping მაგალითზე.

UI– ის სტრატეგიული მომსახურების დანაყოფის ვიცე პრეზიდენტი ედვარდ დრიუ აღნიშნავს: მკაფიო გასაგები და კარგად სტრუქტურიზებული მართვის პროცესი კომპანიას საშუალებას აძლევს აამაღლოს მუშაობის ხარისხი, ეხმარება გაავრცელოს ცოდნა და ამაღლებს ხელმძღვანელობის დროის გამოყენების ეფექტურობას. სტრატეგიული მაჩვენებლები როგორც წესი განისაზღვრება ხანგრძლივი პერიოდისთვის, ხოლო შედეგების შეფასება ხორციელდება უწყვეტად, რომელიც საშუალებას იძლევა გაირკვეს რა შესრულდა და არა და სად უნდა მოხდეს კორექტივების შეტანა.

UI – ში რისკების მართვის ამოცანები დაკისრებული აქვს სტრატეგიული მომსახურების დანაყოფს (სმდ), რომელიც პასუხისმგებელია სტრატეგიულ დაგეგმვაზე. ეს დანაყოფი პირდაპირ ექვემდებარება გენერალურ დირექტორს.

UI – პროცესული ორგანიზაციაა, მაგრამ ამავე დროს ის,ბიუჯეტისა და პერსონალის სამართავადიყენებს ტრადიციულ ვერტიკალურ სტრუქტურას. რისკების ანალიზს, პროცესების თვალსაზრისით, მკაცრად ფუნქციონალურ მიდგომასთან შედარებით, გააჩნია არსებითი უპირატესობა. მაგალითად ,თუ რისკი განხაზღვრულ იქნა. ფუნქციონალური შეზღუდვების თვალსაზრისით, მაშინ ის შეიძლება მოხვდეს კომპანიის სხვა დანაყოფში, ხოლო ამანვე, თავის მხრივ, შეიძლება ზიანი მიაყენოს ორგანიზაციას მთლიანობაში.

ვთქვათ, არასანქცირებული შეჭრა UI – ს ობიექტზე (ელექტრონულ ქვესადგურებზე) – ესაა რისკი საზოგადოებრივი უსაფრთხოების სისტემისთვის. პასუხისმგებლობა ასეთი რისკის ექვემდებარება დაზღვევას, მაშასადამე, ის იმყოფება ფინანსური რისკმენეჯმენტის ფუნქციის კომპეტენციაში, ოღონდ UI პროცესული მიდგომა გულისხმობს, რომ რისკების ეფექტური მართვა უნდა მოიცავდეს ფუნქციის „ელექტრობის



ნახ. 6 სტრატეგიული დაგეგმვისა და რისკმენეჯმენტის პროცესების ინტეგრაცია

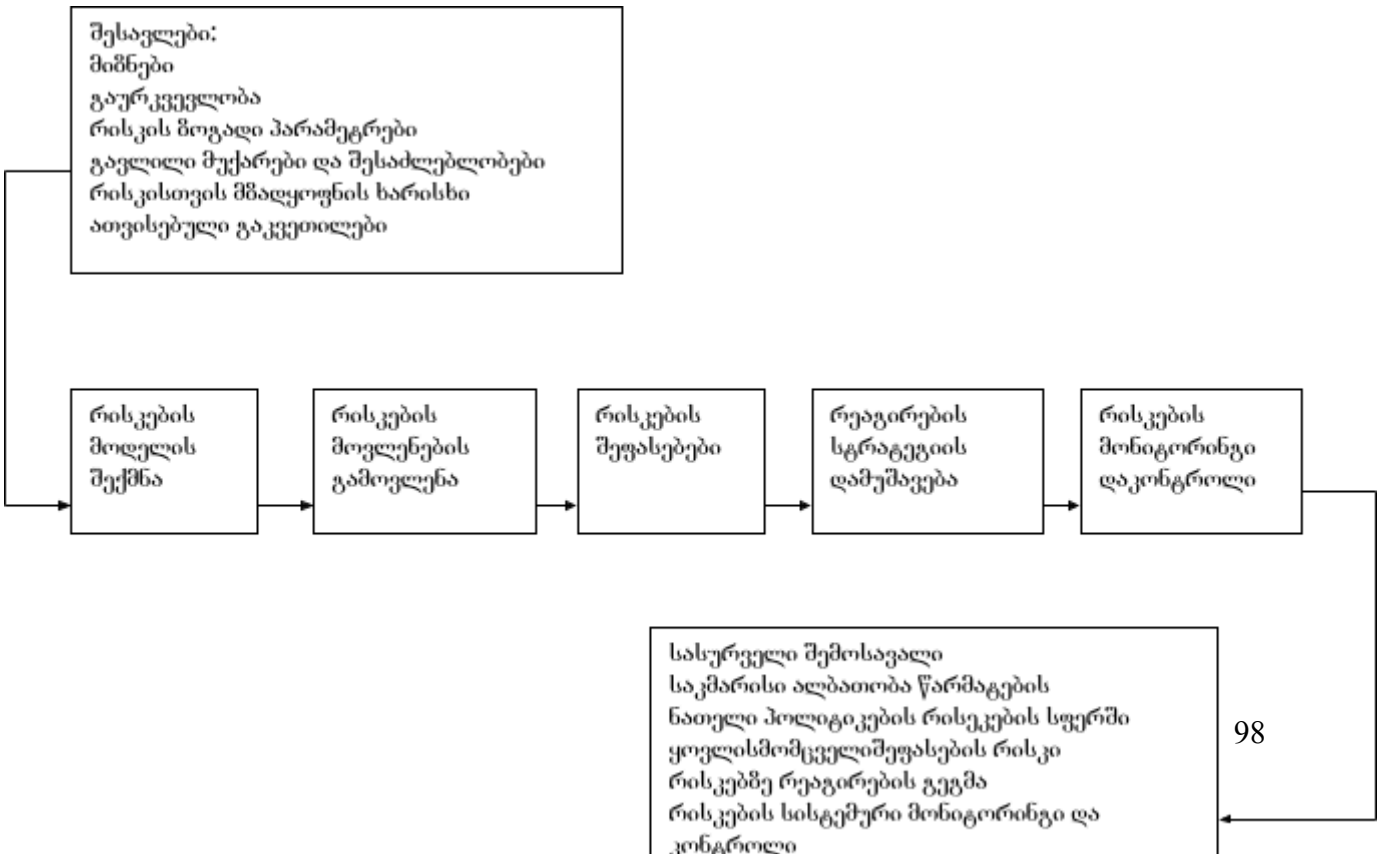
მიწოდება“, რამდენსაც მისი პერსონალი ვალდებულია თვალყური მიადევნოს ქვესადგურებისდაცვის სისტემებს და აკონტროლოს დაშვება მის ტერიტორიაზე.

ასეთ ზომებს რისკების მართვაში მოაქვს ფინანსურისარგებელი, რამდენადაც თანდათან მცირდება სადაზღვევო გადარიცხვების მოცულობა და ყველაზე მთავარი, ამცყრებს UI რეპუტაციული რისკების ალბათობას. საბოლოდკი, ყველა ჩამოთვლილი რგოლების გათვალისწინებას მივყავართ ERM დიდ ეფექტურობასთან.

სტრატეგიული მომსახურების დანაყოფი ყოველწლიურად ამზადებს ორ ანგარიშს: ერთს ოქტომბერში – მიმოხილვა, კომპანიის მიმდინარე წლის რისკების შეფასებით, რომელიც გამოიყენება ხელმძღვანელობის მიერ მომდევნო წლის რისკმენეჯმენტის სტრატეგიის კორექტირებისთვის და მაისში – მიმდინარე მდგომარეობის შესამოწმებლად. ეს დოკუმენტები შეიცავს რაოდენობრივ და ხარისხობრივ მონაცემებს კომპანიის ყველა რისკებისსა და მათი მართვის სტრუტეგიების შესახებ. ასევე ის აღწერს ცვლილებებს რეგულირებაში (ახელმწიფო და ფედერალურ) საგადასახადო კოდექსში, კანონმდებლობასა და იმ დარგში, რომელსაც შეუძლია გავლენა მოახდინონ კომპანიის ბიზნესზე.

ბ) რისკების მართვის პროცესი

რისკების მართვა – ყოველი თანამშრომლის ამოცანაა, და არა მარტო აუდიტორების. რისკები ახდენს გავლენას აქციონერულ ღირებულებაზე და არა მხოლოდ ორგანიზაციის შიდა პროცესებზე: რისკების მართვის პროცესი ნაჩვენებია ნახ. 7–ზე .



ნახ. 7 რისკების მართვის პროცესები

UI– ში, აღნიშნული პროცესი, გახდა საფუძველი ყველა ღონისძიებისთვის, რომლებიც დაკავშირებულიარისკებთან – სტრატეგიული დაგეგმვიდან–ცალკეულ პროექტებამდე. ოღონდ მიზანი მდგომარეობს არა იმაში, რომ მოშორებული იქნას ყველა რისკი, არამედ იმაში, რომ მოხდეს მათი ეფექტური მართვა. რისკები შეიძლება დაიყოს დადებით და უარყოფით რისკებად (რისკი მუქარები და რისკი შესაძლებლობები). გამოყენებული შესაძლებლობა სავსებით შესაძლებლია იქცეს მუქარად. მაგალითად, ელექტრონული ქსელების გაცვეთილი მოწყობილობების დროულადშეცვლის ხელიდან გაშვებულმა შესაძლებლობა, შეიძლებ გახდეს მიზეზი მსხვილი ავარიისა, რომლის შედეგების აღმოფხვრა იქნება ძნელი და ძვირადღირებული.

უმთავრესი პოსტულატი მდგომარეობს იმაში, რომ ნებისმიერი მენეჯერი უნდა იყოს რისკმენეჯერიც. ამრიგად ყველა ხელმძღვანელი ვალდებულია:

- ესმოდეს რა შედეგები მოყვება სხვადასხვა მოვლენებს, რისკების თვალსაზრისით, როგორია მათი წარმოშობის ალბათობა, უსაფრთხოების რა ზომები შეიძლება იქნას მიღებული;
- გამოიყენოს კომპანიის რესურსები რისკების მონიტორინგისა და დაცვის ორგანიზაციებისთვის.
- დაიცვას, რისკების მართვის დისციპლინა და შიდა პროცედურები რათა ორგანიზაციას ჰქონდეს შესაძლებლობა მიაღწიოს დაგეგმილ მაჩვენებლებს ყოველი დანაყოფის დონეზე.

ცხრილში მოცემულია რისკები, რომელთა მართვაც უკვე შედიოდა შესაბამისი მენეჯერების პასუხისმგებლობის ზონაში, ოღონდ რისკების მართვა ხორციელდება დამოუკიდებლად და არაკომფორმატიზებულად. ახალმა პროცესმა წარმოადგინა ინსტრუმენტებისთანმიმდევრობითი ნაკრები და ერთიანი ტექნოლოგია,

რომლებიც საშუალებას იძლევა უფრო ეფექტურად გამოვლინდეს, შეფასდეს, დოკუმენტირებულ იქნას და გაკონტროლდეს მთელი ორგანიზაციის მასშტაბით.

პასუხისმგებელ პირებს მოეთხოვება:

- გამოიყენოს რისკების მართვის სისტემა თავისი ამოცანებისთვის მიმდინარე წელს;
- ჩამოაყალიბონ კრიტერიუმები, რომელთა გამოყენებაც შესაძლებელი იქნება მთელი კომპანიის მასშტაბით, მაგალითისთვის რისკის ღირებულების გაანგარიშების ხერხი;
- დააფიქსიროს მიმდინარე წლის პროცესების ნებისმიერი გათვალისწინებები, განსაკუთრებით გამოყენებული შესაძლებლობების და მუქარების, რომელთა თავიდან აცილებაც მოხერხდაფულადი ეკვივალენტი;
- გამოიყენოს მიმდინარე წლის მეტრიკები მომავალი წლის მიზნების დასაძლევად.

ცხრილი .1

№	რისკის ზონები	რისკი, რომელიც უნდა იმართოს
1	საიმედოობა	ტრამვები, ავარიები
2	უსაფრთხოება	დანაშაულები, ხანძრები
3	ბიზნესის უწყვეტობა	მოღვაწეობის წყვეტები (შეწყვეტები) შეჩერებები
4	IT – ინფრასტრუქტურა	მსხვილი უწესრიგობები IT – ში
5	სტიქიური უბედურება	მსხვილი უწესრიგობები ელექტრონულ ქსელებში
6	სასამართლო სარჩელები	დაზღვეული რისკები
7	ელექტრონული ქსელების საზოგადოებრივი ზედამხედველობის დეპარტამენტის ჩინოვნიკის ანგარიში	კლიენტების საჩივრების რიცხვის ზრდა
8	სტრატეგიული დაგეგმვა	სტრატეგიული მუქარები და შესაძლებლობები
9	პროექტების მართვა	რისკები, რომლებიც დაკავშირებული არიან ორგანიზაციის პროექტების პორთფელებთან
10	პროცესები ოპტიმიზაცია	პროცესული მუქარები და შესაძლობები

11	გარემომცველი გარემო	
12	საქმის წარმოება	დოკუმენტაციის დაკარგვა
13	შიდა განაწესი	თაღლითობები და რეპუტაციული რისკები
14	ამონაგები	მოხმარებული ელექტროენერგიის ანგარიშების გადახდისაგან თავის არიდება

გ) რისკების უწყვეტი მართვა და ანგარიშგება

რისკების მართვის სისტემის დანერგვა ხდება ეტაპობრივად. რისკების შესახებ წლიურ ანგარიშში მოცემულია სტრატეგიული რისკებისსურათი, რომლებიც გამოვლენილი იქნა ხელმძღვანელობის მიერ იმ მონაცემების საფუძველზე, რომლებიც მიღებული იქნა მენეჯერების მიერ (რისკის ტიპი, მისი ალბათობა, ორგანიზაციის მზადყოფნის ხარისხი).

რისკებზე წლიური ანგარიში და მის საფუძველზე ფორმირებულ რისკების გეგმებში ითვაალისწინებენ ამ ინფორმაციას და შემდეგ იყენებენ როგორც ბაზისს მთელი კომპანიის მასშტაბით პროექტების და ცალკეული ღონისძიებების წარმართვისთვის.

ყოველი მუშაკი ჩართული უნდა იყოს პროცესში. დამატებითი კომუნიკაციები ხორციელდება ხელმისაწვდომ გამოთვლებში და სპეციალურ ტრენინგებზე რისკმენეჯმენტში.

თითოეული თანამშრომლის წვლილი კომპანიის საერთო შედეგში.

ხორციელდება უმაღლესი რგოლის ხელმძღვანელების მიერ თავიანთი უშუალო ხელქვეითებისთვის. ცოდნის გადაცემისა ეს მნიშვნელოვანი სესხი განსაკუთრებით პერსონალის დაბერებით გათვალისწინებით – ერთ – ერთია სტრატეგიული რისკებიდან.

UI. მონაწილეობა წლიური ანგარიშის შედგენაში ასევე ხელს უწყობს თანამშრომლების ოპერაციულ გაცვლას.

UI დირექტორების საბჭო ადგენს ზღურბლურ მნიშვნელობებს მატერიალური რისკებისთვის, რომლის მიღწევისას მასვე უნდა მოხსენდეს დაუყოვნებლივ. ამ დროს რისკებს ახასიათებენ შემდეგნაირად:

- „ძალიან დიდი“ – ღირებულება, აჭარბებს 10 მილიონ დოლარს.
- „დიდი“ – ღირებულება შეადგენს 1 – დან 10 მლ. დოლარამდე.

● „საშუალო“ – ღირებულება შეადგენს 100 ათასიდან 1 მლ. დოლარამდე.

● „მცირე“ – ღირებულება ნაკლებია 100 ათას დოლარზე.

ანგარიშების მთელი სისტემა დაფუძნებულია ამ კლასიფიკაციაზე; რისკების ამაღლებასთან ერთად მაღლდება თანამშრომელთა დონე, რომლებიც დაკავებული არიან ამ რისკებით. მაგალითისთვის, ძალიან მაღალი რისკებითაა დაკავებულია დირექტორთა საბჭო, „დიდი“ რისკებით – დანაყოფების ხელმძღვანელები და ა. შ.

UI ცდილობს თავი აარიდოს პროექტებს, სადაც პოტენციური რისკები ვერ მართლდება მოსალოდნელი სარგებლებით. თუ წარმოიშობა გამონაკლისი ამ წესიდან, საჭიროა ზემდგომი ხელმძღვანელობის მოთმინება და სპეციალური ზედამხედველობა.

UI თანამშრომლები ამზადებენ შეფასების რისკის ანგარიშს 14 – ვე ძირითადი ზონების მიხედვით (იხ. ცხრილი), რომელიც განსახილველად წარედგინება უმაღლეს ხელმძღვანელობას.

ასეთი ანგარიში საშუალებას იძლევა გადაიხედოს არა მარტო ცალკეული პროექტების, არამედ კომპანიის რისკები მთლიანობაში.

ამრიგად, ასეთი ძალისხმევა საშუალებას იძლევა უფრო ნათლად მოხდეს რისკების ფორმულირება და უფრო წარმატებით მოხდეს მათთან ბრძოლა.

დ) რისკების მართვის ხარისხის უწყვეტი შეფასება

UI იყენებს დაბალანსებული მაჩვენბლების სისტემას და ზომავს რისკებს ორი ხერხით: თვალყურს ადევნებს რისკების მართვის მაჩვენებლებს და ბიზნესის აფექტურობის მაჩვენებლებს.

UI ეფუძნება შემდეგ პოსტულატებს:

· ფოკუსირება მოხდეს იმაზე, რაც მართლაც მნიშვნელოვანია კლიენტებისთვის, აქციონერებისა და რეგულატორებისთვის;

· გაიზომოს, რათა გაუმჯობესდეს. თანამშრომლებმა უნდა ჩამოაყალიბონ თუ რას გააკეთებენ ისინი რისკების მიმართებაში, რათა უსაფრთხო გახადონ ბიზნესი;

· არ უნდა გაიზომოს რისკი, მხოლოდ იმიტომ, რომ ის იზომებოდა წარსულში, ან იმიტომ, რომ ამის გაკეთება არაა რთული;

· არ იქნეს დავიწყებული რისკები, რომლებიც დაკავშირებულია კლიენტებთან და მომწოდებლებთან;

· გათვალისწინებულ იქნას, თუ როგორ შეიცვლება ადამიანების ქცევა დამატებითი მეტრიკების შემოღებისას.

· არ მოხდეს იმის დაშვება, რომ უკეთესი იყოს მტერი კარგი ან უფრო მარტივი.

პროცესის კარგი ორგანიზაცია ნიშნავს გათვალისწინებულ იქნას მოღვაწეობა კლიენტების, აქციონერების და მომწოდებლების და არა მარტო თვით ორგანიზაციის მოღვაწეობა.

აქვე მოგვყავს რამოდენიმე მეტრიკისმაგალითი, რომლებიც გამოიყენება UI– ის მიერ რისკების მართვის პროცესის ხარისხის კონტროლისთვის:

· ინფორმაციულობის დონე განისაზღვრება იმ რისკმენეჯერებისპროცენტებით, რომლებიც იყენებენ რისკების მართვის მეთოდიკას (გამოკვლევებით დაწყებული მიმდინარე ანგარიშების მომზადებით დამთავრებული);

· მიზნობრივი შედეგები განისაზღვრება ღირებულებით გამოყენებული შესაძლებლობებით და მუქარებით, რომელთა თავიდან აცილებაც მოხდა.

მიზნობრივი შედეგები განისაზღვრება იქ, სადაც შეუძლებელია შედეგები შეფასდეს ფულად გამოსახულებაში (კლიენტების რისკების შემცირება, მიღებული ჯილდოების რიცხვი და ა. შ.). შედეგები, ფულადი გამოსახულებით, მოიცავს ხარჯების ინვესტიციაზე (ROI) პროექტების პორთფელების მიხედვით, დაბრუნებულ ამონაგებს და დანაკარგების შემცირებას, რომლებიც განპირობებული იყო რისკებით.

რისკების მართვის ეს მიდგომა ეფუძნება პერსონალის ცოდნის მაღალ დონეს, მკაცრ ანგარიშგებასა და აქტიურ პოზიციებს რისკებთან მიმართებაში.

თავი 4. რეკომენდაციები პერსონალის შერჩევა-მიღების პროცესების ორგანიზებისა და შემდგომი მონიტორინგის საკითხებში

4.1. თანამშრომელთა როლი უსაფრთხოების პოლიტიკაში

უსაფრთხოება თანამედროვე ინფორმაციული ტექნოლოგიების სავანძო საკითხია. ინფორმაციული საცავების ზრდასთან ერთად, მატულობს მისი როლი და დაგეგმვის საჭიროება. სისტემების დაცვა და რისკების მინიმიზაცია კომპლექსური თემაა და მისი ცალკეული ასპექტის დამოუკიდებლად განხილვა ყოვლად დაუშვებელია. სწორედ ამიტომ, ორგანიზაციებში იქმნება უსაფრთხოების პოლიტიკა, რომელიც ყოველ მხრივ აანალიზებს მოსალოდნელ საფრთხეს და აწესებს რეგულაციებს მათ შესამცირებლად.

განვიხილოთ პერსონალის როლი ინფორმაციული უსაფრთხოების სფეროში.

პერსონალსა და ინფორმაციულ სისტემების უსაფრთხოებას შორის დამოკიდებულებაზე მრავალი შეხედულება არსებობს. ერთ-ერთი მათგანი ამ დამოკიდებულებას სამ ასპექტში განიხილავს – პროდუქტი, პროცესი და პანორამა. პირველ შემთხვევაში აქცენტი პროდუქტის ანუ ინფორმაციული სისტემის შემუშავებაზე კეთდება. აღნიშნული კომპონენტი მოიცავს სისტემის დაგეგმვასა და

შემუშავებას. ამასთანავე მოიაზრება, რომ უსაფრთხოების განმსაზღვრელი ძირითადი ფაქტორი, სწორედ თავად სისტემის ხარისხიანი არქიტექტურაა.

სისტემის უსაფრთხოებაში დიდ როლს თამაშობს დანერგვის პროცესი. იმპლემენტაცია მნიშვნელოვანი საფეხურია. საწყის შეცდომებზე რეაგირება დიდწილად განაპირობებს,ექსპულატაციის პერიოდში, სისტემის შემდგომ სტაბილურობას. ითვლება, რომ სისტემა, რომლის ფუნქციონირებისას მრავალი ინციდენტი ფიქსირდება დანერგვის ეტაპზე არასათანადოდ იყო დამუშავებული.

პანორამა, რისკის თავიდან ასაცილებელი ოპერაციების თავისებურებებს მოიცავს. გამომდინარე იქედან, რომ ინფორმაციული სისტემების უსაფრთხოება, როგორც წესი, არ წარმოადგენს ორგანიზაციის ძირითად საქმიანობას და რთულია მასზე ორიენტირება, ამიტომ აღნიშნული საკითხის ოპტიმალურად გასაკონტროლებლად, დიდი მნიშვნელობა ენიჭება თანამშრომელთა კონსოლიდაციას. აუცილებელია პერსონალი მოქმედებდეს შეთანხმებულად და აღიარებდეს უსაფრთხოების მნიშვნელობას. ამასთანავე რისკების ანალიზის სცენარების შემუშავებაში, გათვალისწინებული უნდა იქნას პერსონალის აზრი.

უსაფრთხოების სისტემაში, ტექნიკურ მაჩვენებლებთან და არსებულ კონცეფციებთან ერთად, მნიშვნელოვან როლს ასრულებს ადამიანური ფაქტორი. ამასთანავე, უდიდესი მნიშვნელობა აქვს პერსონალის მართვასა და მათთან დამოკიდებულებას.

მენეჯმენტის თანამედროვე კონცეფციების თანახმად, მენეჯერის ერთ-ერთ მთავარ ფუნქციას თანამშრომელთა სტიმულირება და მათთან ურთიერთობების რეგულირება წარმოადგენს.

ინფორმაციის მოსაპოვებლად ტექნიკური საშუალებების გამოყენება რთულ და გრძელვადიან გზას წარმოადგენს, უფრო იოლია იმ ადამიანის მოსყიდვა ან თუნდაც მისგან ინფორმაციის „მოპარვა“, ვისაც უკვე გააჩნია წვდომა საჭირო რესურსზე. დღეისათვის კიბერ შპიონაჟის დიდი ნაწილი სწორედ პერსონალის შეცდომებსა და მიკერძოებაზეა დამყარებული. ბოლო წლებში აქტუალური გახდა გამოთქმა – „დამნაშავეები კიბერ თავდასხმის წყალობით იპარავენ ინფორმაციას, პროფესიონალი დამნაშავეები კი იგივეს მხოლოდ შესაბამის ადამიანებთან საუბრით ახერხებენ“.

აღნიშნული პრობლემა მეტ აქტუალობას, არსებული ნორმებიდან თუ ხასიათიდან გამომდინარე, იძენს საქართველოში, ადამიანებს შორის ნებისმიერი თემა შეიძლება განიხილებოდეს. პიროვნებამ შესაძლოა საკუთარი ორგანიზაციის საიდუმლოება ოჯახის წევრებთან ან უარეს შემთხვევაში, მეგობრებთან საუბრის თემაც კი გახადოს. შესაბამისად მსმენელმა, თუ ის არაკეთილსინდისიერი ან თუნდაც დაინტერესებული მხარეა, შეიძლება მსგავსი დიალოგი სათავისოდ გამოიყენოს. ამ სიტუაციაში ორგანიზაციის თანამშრომელი ძალაუნებურად ხდება დანაშაულებრივი ჯგუფის წევრი.

კონფიდენციალობის დარღვევას ასევე შესაძლოა ჰქონდეს გამიზნული ხასიათი, მაგალითად, ქრთამის ან ნებისმიერისახით, თანამშრომლის გადაბირების შემთხვევაში, ორგანიზაციამშესაძლებელია მიიღოს ინფორმაცია კონკურენტის შესახებ.

კონფიდენციალურობის დაცვა და საკუთარი, თუ მომხმარებლას მონაცემების შენახვა, ნებისმიერი ორგანიზაციის ძირითადი საქმიანობის შემადგენელი ნაწილია, განსაკუთრებით მსხვილ კომპანიებში, სადაც კრიტიკული ინფორმაციის მოცულობა დიდია და რაც უფრო დიდია პერსონალის რიცხვი, მით მეტია ინფორმაციის „გაჟონვის“ , თუ დაზიანების საფრთხე.

უსაფრთხოებასთან დაკავშირებული პრობლემები თანამშრომლების შერჩევიდან იწყება. ყველა კომპანიას აქვს კადრების აყვანის საკუთარი პოლიტიკა. ის ითვალისწინებს კანდიდატთა განათლებას, მათ პიროვნულ უნარებსა თუ ათვისების უნარს, თუმცა იშვიათად თუ საიდუმლო ინფორმაციასთან დაკავშირებულ საკითხებისადმი შეხედულებებს.

მას შემდეგ, რაც ადამიანი ვაკანტურ პოზიციას დაიკავებს და საქმიანობის შესრულებას შეუდგება, მას როგორც წესი, აღარავინ აუხსნის, თუ რა მნიშვნელობა ენიჭება კონფიდენციალობის დაცვას და რა ზეგავლენას მოახდენს მათი დარღვევა ორგანიზაციის საქმიანობაზე. არსებული სტერეოტიპული მიდგომებიდან გამომდინარე, რატომღაც ითვლება, რომ ინფორმაციული უსაფრთხოების უზრუნველყოფა მთლიანად ინფორმაციული ტექნოლოგიების განყოფილებას ეკისრება, რაც მცდარ სტერეოტიპს წარმოადგენს.

IT დანაყოფი,ტექნიკურ დონეზე შიფრაციისა, თუ წვდომის კონტროლის საფუძველზე, უზრუნველყოფს უსაფრთხოებას, თუმცა ნებისმიერ დაშიფრულ, თუ

შეზღუდულ ინფორმაციას ჰყავს შიდა მომხმარებელი და კონტროლის განხორციელება აუცილებელია სწორედ მათზე- ინფორმაციის მომხმარებლებზე.

თითოეულ თანამშრომელს მკაფიოდ უნდა განემარტოს კონფიდენციალობის მნიშვნელობა და ინფორმაციის ის ნაწილი, რომლის სულ მცირე კომპონენტის ცვლილება/დაკარგვასაც კი შესაძლოა სავალალო შედეგები მოყვეს. აუცილებელია პერსონალი ხედავდეს საკუთარ როლს ორგანიზაციის საქმიანობაში, რაც მას ორგანიზაციული საქმიანობისადმი მეტად ერთგულს გახდის. მცირე კომპანიაში მსგავსი მიდგომების დანერგვის შემთხვევაში შესაძლოა სულაც არ გახდეს საჭირო ძვირადღირებული ტექნიკური საშუალებების შეძენა-მონტაჟი და უსაფრთხოების აქცენტები სრულად თანამშრომელთა კეთილსინდისიერებაზე იყოს აგებული.

ადამიანური ურთიერთობების რეგულირება შედარებით იოლია მცირე კომპანიებში. შედარებით მსხვილ დაწესებულებებში, რომლებიც ფილიალებისაგან და რამდენიმე ასეული თანამშრომლისგან შედგება, საქმე ცოტა რთულადაა. მსგავს ორგანზიაციებში შეუძლებელია თითოეულ თანამშრომელს ინდივიდუალურად აუხსნა მასზე დაკისრებული პასუხისმგებლობა და მოსთხოვო კონფიდენციალობის დაცვა. მიუხედავად იმისა, რომ ორგანიზაციისთვის კრიტიკული ინფორმაციის საიდუმლოდ შენახვაზე ყველა თანამშრომლის კონტრაქტშია მითითებული. კონფიდეციალობის რეგულირება კიდევ უფრო რთულდება თანამშრომლის კონკურენტფირმაში გადასვლის შემთხვევაში, ვერავინ ვერ გააკონტროლებს, რამდენად გასცემს ადამიანი წინა სამსახურიდან მოპოვებულ ინფორმაციას. უსაფრთხოება მხოლოდ ტექნიკურ საკითხს არ წარმოადგენს და მის მიმართ სისტემური მიდგომა სასიცოცხლოდ მნიშვნელოვანია.

4.2. რეკომენდაციები პერსონალის შერჩევა- მიღებისმეთოდებისა და ინსტრუქციების საჯარო სექტორში დანერგვის საკითხებში

დაწესებულება მუდმივად უნდა ზრუნავდეს კადრების გეგმიური და არაგეგმიური დენადობით გამოწვეული დეფიციტის დასაფარად. აღნიშნული პრობლემების გადაწყვეტისთვის დაწესებულებისა და ადამიანური რესურსების

მართვის ქვედანაყოფი მუდმივად უნდა იყოს საქმის კურსში ქვეყნის შრომითი რესურსების ბაზარზე არსებული მდგომარეობის შესახებ. გარდა ამისა, ახალგაზრდა კადრების მოზიდვის მიზნით, ქვედანაყოფის ერთერთ თანამშრომელს მუდმივი კავშირი უნდა ჰქონდეს უმაღლეს სასწავლებლებთან, რომლებშიც ხდება შესაბამისი კვალიფიკაციის სპეციალისტების მომზადება. მას, აგრეთვე, უნდა ჰქონდეს ინფორმაცია დაწესებულებისთვის საჭირო სფეროში კვალიფიკაციის ამაღლების შესახებ. განსაკუთრებით ეს ეხება პირებს, რომლებმაც საზღვარგარეთ მიიღეს ცოდნა და გამოცდილება.

უკანასკნელ წლებში დამკვიდრდა უმაღლესი სასწავლებლის დამამთავრებელი კურსის სტუდენტებისა და კურსდამთავრებულთათვის სახელმწიფო დაწესებულებებში სასწავლო პრაქტიკისა და სტაჟირების მოწყობა, რაც საჯარო სამსახურში ახალგაზრდა პერსპექტიული სპეციალისტების მოზიდვის ერთერთი საშუალებაა.მიზანშეწონილია, დაწესებულებას ჰქონდეს ოფიციალური ხელშეკრულება შესაბამის უმაღლეს სასწავლებლებთან სტუდენტების სასწავლო პრაქტიკისა და სტაჟირების მოწყობის შესახებ.

ვაკანტურ თანამდებობაზე თანამშრომლების მიღება- დაგეგმვის პროცესზე პასუხისმგებელი მენეჯერი უნდა დარწმუნდეს, რომ ვაკანტური თანამდებობის აღწერა, განსაკუთრებით საკვალიფიკაციო მოთხოვნები, ზუსტად შეესაბამებოდეს არსებულ მოთხოვნებს. საჭიროების შემთხვევაში თანამდებობის აღწერაში შეტანილი უნდა იქნას სათანადო ცვლილებები. შემდეგ მენეჯერმა უნდა განიხილოს და გაესაუბროს ყველა თანამშრომელს, ვისაც შესაძლებელია ჰქონდეს ამ თანამდებობის დაკავების სურვილი და, ამავე დროს, აკმაყოფილებდეს ვაკანტური თანამდებობის მიმართ წაყენებულ მოთხოვნებს, რადგან ზოგჯერ მიზანშეწონილია შიდა რესურსის გამოყენება. ეს განსაკუთრებით მნიშვნელოვანია იმ შემთხვევაში, როდესაც დაგეგმილია შტატების შემცირება.

არსებული კანონმდებლობის თანახმად საჯარო მოსამსახურეების სამსახურში მიღება ძირითადად კონკურსის შედეგად შერჩევის საფუძველზე ხდება. კონკურსს ატარებს დაწესებულების საკონკურსო-საატესტაციო კომისია. კონკურსის ჩატარების ზოგადი წესი და პირობები განსაზღვრულია„საჯარო სამსახურის შესახებ“ საქართველოს კანონის 29-36[4]-ე მუხლებით და საქართველოს პრეზიდენტის 2009 წლის 5 თებერვლის #46 ბრძანებულებით

„საჯარო თანამდებობათა დასაკავებელი კონკურსის ჩატარების წესის დამტკიცების შესახებ“ დამტკიცებულ წესით. საჯარო სამსახურის თითოეულ დაწესებულებას თავისი სპეციფიკის გათვალისწინებით დამტკიცებული უნდა ჰქონდეს საკონკურსო-საატესტაციო კომისიის დებულება და კონკურსისა და ატესტაციის ჩატარების პირობები. ამ დოკუმენტის შესაბამისად შესაძლებელია ცალკეული კონკურსის ჩატარების წინ დაწესებულების ხელმძღვანელის ბრძანებით ან საკონკურსო-საატესტაციო კომისიის გადაწყვეტილებით განისაზღვროს ამ კონკრეტულიკონკურსის მოწყობის პირობები, რომელიც არ უნდა ეწინააღმდეგებოდეს არც ერთ ზემოაღნიშნულ მოთხოვნებს. საკონკურსო-საატესტაციო კომისიას. „საჯარო სამსახურის შესახებ“ საქართველოს კანონის 36^2-ე მუხლის პირველი პუნქტის თანახმად, ადგილობრივი თვითმმართველობის ორგანოს გარდა, კომისიის თავმჯდომარეს ნიშნავს საჯარო სამსახურის ბიუროს უფროსი. იგივე მუხლის მე-2 პუნქტის თანახმად, თავმჯდომარედ, როგორც წესი, ინიშნება დაწესებულების ხელმძღვანელი ან მისი მოადგილე. იგივე კანონის 36^3-ე მუხლის პირველი პუნქტის თანახმად კომისიის წევრთა რაოდენობასა და შემადგენლობას განსაზღვრავს კომისიის თავმჯდომარე და ხშირად წევრების ძირითადი ნაწილიც ორგანიზაციის ხელმძღვანელი მუშაკები არიან. მათი დრო შეზღუდულია და თავის ძირითად საქმიანობასთან ერთად უჭირთ კონკურსის მოწყობის პროცესშიმაქსიმალური ჩაერთვა, რამაც შესაძლოა ნეგატიური გავლენა იქონიოს კონკურსის პროცესზე. ეს გარემოება გათვალისწინებული უნდა იყოს კომისიის შემადგენლობის შერჩევისას. რეკომენდებულია კომისია შედგებოდეს 5-7 წევრისგან და მის შემადგენლობაში აუცილებლად იყოს კონკურსის პირობებით გათვალისწინებული პროცედურის ჩატარების სპეციალისტი. კარგი იქნება, თუ იგი წინასწარ მოამზადებს კომისიის წევრებს კონკურსის მოწყობის სპეციფიკურ საკითხებში. აუცილებლობის შემთხვევაში კომისიამ შესაძლებელია თავის სხდომაზე მოიწვიოს პირი, რომელიც დაეხმარება მას ობიექტური გადაწყვეტილების მიღებაში. თუ ამის საჭიროება არსებობს, შესაძლებელია შეიქმნას კომისიის სპეციალიზებული შემადგენლობა, როგორც ეს გათვალისწინებულია „საჯარო სამსახურის შესახებ“ საქართველოს კანონის 36^1-ე მუხლის მე-3 პუნქტსა და 36^2-ე მუხლის მე-4 პუნქტებში.

4.3. რეკომენდაციები ვაკანსიაზე კანდიდატთა შერჩევის ძირითადი კომპეტენციების განსაზღვრისა და პროცესების შემდგომი მონიტორინგის საკითხებში

იმ სამუშაოთა შესასრულებლად, რომელსაც ახალი თანამშრომელი უნდა მოერგოს,ვაკანტური პოზიციისადმი ძირითადი მოთხოვნების განსაზღვრისას მნიშვნელოვანია, რომ ჩამოყალიბდესყველაზე რელევანტური და მნიშვნელოვანი კომპეტენციების ნუსხა. ამ ჩამონათვალის ჩამოყალიბება/შემოწმება შესაძლებელია შესასრულებელ სამუშაოთა ანალიზის საფუძველზე. ანალიზის შედეგად განისაზღვრება ძირითადი კომპეტენციები, რომელთა მიხედვით უნდა მოხდეს საუკეთესო კანდიდატის შერჩევა.

სამუშაოთა უმრავლესობისთვის, საკმარისია ქვემოთმოყვანილი კომპეტენციებიდან ექვსამდე კომპეტენციის შერჩევა:

1 გადაწყვეტილების მიღება და მოქმედების ინიცირება;
2 მართვა და გედამხედველობა;
3 ადამიანებთან მუშაობა;
4 პრინციპებისა და ღირებულებების დაცვა;
5 ურთიერთობების დამყარება და კონტაქტების მართვა;
6 სხვათა დარწმუნება და გეგავლენა;
7 ინფორმაციის წარდგენა და გადაცემა.
8 წერა და ანგარიშგება;
9 ტექნიკური საშუალებების გამოყენება;
10 კრიტიკული და ანალიტიკური აზროვნება;
11 სწავლა და კვლევა;
12 შემოქმედებითობა და ინოვაცია;
13 სტრატეგიებისა და კონცეფციების შემუშავება;
14 დაგეგმვა და ორგანიზება.
15 შედეგების მიღწევა.
16 ინსტრუქციებისა და პროცედურების დაცვა.

17 ადაპტაცია და ცვლილებებზე რეაგირება.

18 გეწოლის მიმართ მდგრადობა.

19 სამუშაო მიზნების მიღწევაზე ორიენტირება.

დასკვნა

სადისერტაციო ნაშრომში, „პერსონალის მიღება-დაგეგმვის რისკების მართვის სისტემა, საჯარო სექტორის მაგალითზე“, ჩატარებული კვლევებისა და ანალიზის საფუძველზე, შემუშავებულია კონკრეტული რეკომენდაციები და შესაბამისი დასკვნები, კერძოდ:

1. გაანალიზებულია, ორგანიზაციაში კადრების შერჩევისა და ვაკანსიების შევსების პროცესების ორგანიზებისა და მართვის თანამედროვე მეთოდები,მიდგომები და შემუშავებულია შესაბამისი რეკომენდაციები;
2. შემუშავებულია, რისკების მართვის ისეთი სისტემა, რომელშიც გათვალისწინებულია ინფორმაციული უსაფრთხოება;
3. ფართოდ არის გაშუქებული მუშაკზე ობიექტური და დაცული ინფორმაციის მოპოვების, გადამუშავებისა და შენახვის საკითხები, რაც შემდგომი შესაძლებელია გამოყენებულ იქნას, როგორც კადრების ოპტიმალური შერჩევის, ასევე მისი ეფექტიანი მართვის პროცესებში;.
4. გაანალიზებულია ორგანიზაციაში პერსონალის მიღება-დაგეგმვის პროცესში გასაუბრება- გამოკითხვის მეთოდის გამოყენების შედეგები და გამოვლენილია მისი დადებითი და უარყოფითი მხარეები;
5. გაანალიზებულია საჯარო სექტორში პერსონალის შერჩევის, ვაკანსიების შევსების, თანამშრომელთა დასჯისა და განთავისუფლების, წახალისებისა და პრემირების, კონკურსების ორგანიზებისა და მართვის საკანონმდებლო დოკუმენტები, მითითებები და სხვა ნორმატიული აქტები.

6. ნაშრომში, პერსონალის ანკეტირების მონაცემთა ბაზების, ინფორმაციული უსაფრთხოების უზრუნველყოფისა და რისკების მართვის სისტემების ფორმირებისთვის გამოყენებულია პროგრამული ენა ექსელი, რომელიც შედარებით მარტივი და ადვილად აღქმადი საშუალებაა, მაგრამ ის სრულად აკმაყოდილებს დისერტაციის ფარგლებში დასახული ამოცანების ეფექტიან გადაწყვეტასთან დაკავშირებულ მოთხოვნებს;
7. საკადრო კომისიისთვის შემუშავებულია რეკომენდაციები, რომლის მიხედვით;ობიექტური საკადრო მონაცემების, საქმიანი და მორალური თვისებების, პროფესიული ცოდნისა და უნარების, სამუშაო კარიერისა და სხვა, პიროვნების დამახასიათებელი, სპეციფიური ელემენტების გამოყენებით,უნდა აიგოს სამუშაო ადგილებისა და თანამშრომლთა კრებსითი მოდელი:
8. ნაშრომში, მუხლობრივად არის გაანალიზებული, საჯარო სამსახურის შესახებ“ საქართველოს კანონის 29-36^4-ე მუხლები და საქართველოს პრეზიდენტის 2009 წლის 5 თებერვლის #46 ბრძანებულება „საჯარო თანამდებობათა დასაკავებელი კონკურსის ჩატარების წესის დამტკიცების შესახებ“ და მიღებულია კონკრეტული რეკომენდაციები საკონკურსო კომისიის შემადგენლობის შესახებ;
9. მიღებულია რეკომენდაციები კომპეტენციებზე ორიენტირებული გასაუბრების ჩატარების სპეციალიზირებული კომისიის შესახებ, როგორც ეს გათვალისწინებულია „საჯარო სამსახურის შესახებ“ საქართველოს კანონის 36^1-ე მუხლის მე-3 პუნქტისა და 36^2-ე მუხლის მე-4 პუნქტის. ინსტრუქციაში;
10. რეკომენდირებულია, საუკეთესო კანდიდატის შესარჩევად, შეიქმნას ყველაზე რელევანტური და მნიშვნელოვანი კომპეტენციათა ნუსხა, მათ შორის; გადაწყვეტილების მიღება და მოქმედების ინიცირება, მართვა და ზედამხედველობა, პრინციპებისა და ღირებულებების დაცვა, ურთიერთობების დამყარება და კონტაქტების მართვა, ინფორმაციის წარდგენა და გადაცემა და სხვ. სავარაუდოდ, ცხრამეტი კომპეტენციიდან ექვსამდე კომპეტენციის შერჩევა, საკმარისი იქნება უმრავლესი ორგანიზაციების მოთხოვნების დასაკმაყოფილებლად;

11. გაანალიზებულია რისკების მართვის მეთოდოლოგიის ძირითადი პრინციპები და მექანიზმები, შეფასებულია საფრთხეები და მათთან ბრძოლის ხერხები თავისი დადებითი და უარყოფითი მხარეებით.

გამოყენებული ლიტერატურა:

1. ორგანიზაციის შრომითი რესურსების მართვა როგორც მართვის საინფორმაციო სისტემის ინფორმაციული უზრუნველყოფის აუცილებელი პირობა, სტუ-ს,სტუდენტთა 81-ე ღია საერთაშორისო სამეცნიერო კონფერენცია 2014. ხ. ქორთიაშვილი, გ.მაისურაძე, ნ. წიკლაური
2. პერსონალის მართვის მეთოდები, სტუ, შრომათა კრებული N3 (497),2015. ხ. ქორთიაშვილი
3. რისკების მართვა, საერთაშორისო პერიოდული სამეცნიერო ჟურნალი „ინტელექტი“, N3(59),2017. ხ.ქორთიაშვილი, გ. დალაქიშვილი.
4. სოციალური ქსელი - პერსონალის შერჩევის ერთ-ერთი წყარო, სტუ, შრომები: N2(24)2017. ხ.ქორთიაშვილი, გ. მაისურაძე
5. პერსონალის შერჩევის თანამედროვე მეთოდები, სტუ, შრომები: N2(24)2017. ხ.ქორთიაშვილი
6. We Make Operating System Reliable and Secure?Andrew S. Tanenbaum, Jorrit N. Herder, Herbert Bos, Vrije Universiteit, Amsterdam, Computer (IEEE Computer Soviety, v.39, #5, May 2006)
7. ჩოგოვაძე გ. გოგიჩაიშვილი. გ.სურგულაძე. გ. შეროზია. თ.შონია მართვის ავტომატიზებული სისტემების დაპროექტება და აგება. – თბილისი, გამომცემლობა “ტექნიკური უნივერსიტეტი”.
8. სურგულაძე გ.შონია ო.ყვავაძე ლ. მონაცემთა განაწილებული ბაზების მართვის სისტემები (MS Access, SQL server, Oracl, Inter base, JDBC) - თბილისი გამომცემლობა “ტექნიკური უნივერსიტეტი”. 2005.
9. Worlfwita Quarterly Enterprise Networks Tracker-ის მონაცმების მიხედვით - http://www.idc.com
10. სურგულაძე გ. ველეკინგი. ჰ.თოფურია ნ. განაწილებული ოფის–სისტემების მონაცემთა ბაზების დაპროექტება და რეალიზაცია UML ტექნოლოგიით– თბილისი, გამომცემლობა “ტექნიკური უნივერსიტეტი”. 2004.

11. კუციავა ვ.კაცაძე გ.დიაკონიძე გ. ინფორმაციის დაცვა/დამხმარე სახელმძღვანელო –თბილისი, გამომცემლობა “ტექნიკური უნივერსიტეტი”. 2005.
12. https://www.hr-director.ru/article/63204-ekd-sotsialnye-seti-v-rekrutinge-alternativa-ili-dopolnenie
13. https://www.hr-director.ru/article/63103-metody-nayma-personala
14. https://www.mediascope.ru/node/1093 Transactions
15. https://www.e-xecutive.ru/career/hr-management/1984154-10-i-odin-sovet-po-podb-oru-personala-v-sotsialnyh-setyah
16. Егоршин А.П. (2003). Основы управления персоналом: уч.пособие для вузов – Н. Новгород: НИМБ
17. Модели и методы управления персоналом: Рос-Британское учю пособие /под ред. Е.Б. Моргунова – М.: ЗАО Бизнес-школа, Интел-Синтез, 2001
18. http://upravlencam.ru/page82/page86/index.html

..