ივ.ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

მარინა მერებაშვილი

ინფორმაციული უსაფრთხოების ანალიზი უმაღლეს საგანმანათლებლო სფეროში ანალიზის მეთოდების შერჩევა

ინფორმაციული ტექნოლოგიები
ნაშრომი შესრულბულია ინფორმაციული ტექნოლოგიების მაგისტრის ხარისხის მოსაპოვებლად

ხელმძღვანელები: ფიზ.მათ.კანდ.დავით ხაჩიძე
ირაკლი გაგოშიძე

თბილისი 2015

ანოტაცია

დღევანდელ დღეს ინფორმაციული სისტემა გახდა აუცილებელი კომპონენტი უნივერსიტეტის საქმიანობის ყველა სფეროსა და დონეზე: მართვაში, შესრულებაში, სწავლებაში. .უმაღლესი სასწავლებლის ავტომატიზებული სისტემის ძირითადი მიზანია როგორც მართვის ეფექტურობის, განათლების, სამეცნიერი საქმიანობისა და მომსახურების მიწოდების ხარისხის გაზრდა, ასევე არაგონივრული გადაწყვეტილების მიღების რისკისა არასაჭირო ხარჯების თავიდან აცილებისათვის.

უმაღლესი სასწავლებელი არის ორგანიზაციული სტრუქტურა, სადაც პროცესების ცვალებადობის უწყვეტი რეჟიმია. ამის გამო პროგრამები საჭიროებენ მუდმივ განახლებას. ინფორმაციული სისტემა ავტომატიზებას უკეთებს უმაღლესი სასწავლებლის ინოვაციურ საქმიანობას – რაც უფრო მეტი სფეროს ავტომატიზება ხდება, მით უფრო რთულდება ინფორმაციული სისტემის მოდიფიცირება, განვითარება და უსაფრთხოების უზრუნველყოფა.

მაღალი ტექნოლოგიების სფეროში დანაშაულების ზრდამ განაპირობა მოთხოვნები სასწავლო დაწესებულების გამოთვლითი ქსელების რესურსების დაცვის კუთხით. აქტუალური გახდა საკუთარი უსაფრთხოების სისტემის შექმნის აუცილებლობა, რაც გულისხმობს სამართლებრივ-ნორმატიული ბაზის არსებობას, უსაფრთხოების კონცეფციის ფორმირებას, სპეციალური ღონისძიებების შემუშავებას, უსაფრთხოების მიზნით პროცედურების დაგეგმვას, პროექტირებას, ინფორმაციის დასაცავი ტექნიკური საშუალებების რეალიზებას. ყველა ზემოთ ჩამოთვლილი სისტემური კომპონტები განსაზღვრავს უნივერსიტეში ინფორმაციული უსაფრთხოების დაცვის ერთიან პოლიტიკას. საგანმანათლებლო დაწესებულებებში ინფორმაციის დაცვის სპეციფიკა მდგომარეობს იმაში, რომ უმაღლესი სასწავლებებლი საჯარო დაწესებულებაა მუდმივად ცვალებადი აუდიტორიითა და „დამწყები კიბერ კრიმინალების“ აქტიური ზრდით.

ჩატარებულმა კვლევებმა აჩვენა, რომ ჯერ კიდევ ბოლომდე არ არის შესწავლილი და დადგენილი ის სტანდარტები, რომლებიც სრულად უზრუნველყოფს ინფორმაციის უსაფრთხოებას. ინფორმაციის უსაფრთხოების საკითხები სულ უფრო და უფრო

აქტუალური ხდება თითქმის ყველა თანამედროვე ორგანიზაციისთვის. ამის გამო, ორგანიზაციები ხშირად ქირაობენ სპეციალურ კომპანიებს/სპეციალისტებს თავიანთი ორგანიზაციების უსაფრთხოების შემოწმების მიზნით. გარკვეული ტიპის დაწესებულებებს, მაგალითად სააქციო საზოგადოებებს, ხშირ შემთხვევაში, მთელი რიგი განყოფილებები აქვთ დაკომპლექტებული პროფესიონალებით, რომლებიც უზრუნველყოფენ უსაფრთხოების ნორმების, ჩარჩოების გამართვას და მათ სრულფასოვან ფუნქციონირებას. დღეისათვის ეს სფერო ჯერ კიდევ განვითარების ეტაპზეა და საგრძნობი პოპულაროობით განსაკუთრებით დიდ ორგანიზაციებში სარგებლობს.

ნაშრომის პირველ თავში განხილულია ინფორმაციული სისტემის სტრუქტურა და მისი უსაფრთხოება, სისტემის მოდულები, ინფრასტრუქტურის სქემა. მეორე და მესამე თავში საუბარია ინფორმაციული უსაფრთხოების მოთხოვნებზე, მათ ძირითად წყაროებზე და ორგანიზაციაში ინფორმაციული უსაფრთხოების რისკებზე. რაც შეეხება მეოთხე თავს, იქ განხილულია ინფორმაციული უსაფრთხოების პოლიტიკა და მენეჯმენტის როლი და პასუხისმგებლობა. მეხუთე და მეექვსე თავებში ჩამოყალიბებულია ინფორმაციული უსაფრთხოების შეფასების მიზანი, შეფასების მაჩვენებლები და გადაწყვეტილების კრიტერიუმები, ინფორმაციული უსაფრთხოების მართვის სისტემის ეფექტიანობის საზომები.მეშვიდე თავში საუბარია მონაცემების ანალიზზე და შეფასების შედეგებზე. და ბოლოს, ნაშრომში ჩამოყალიბებულია ის მარტივი მეთოდი, რომლის მიხედვითაც შესაძლებელია უნივერსიტეტში ინფორმაციული უსაფრთხოების შეფასება.

Abstract

Nowadays IT systems have become an essential component of the life of any university, an essential component for its management as well as a tool for educational processes. The aim of IT system nowadays is not only to ensure efficiency of university management and assure high quality of educational process but to support scientific research and to minimize the risk of taking unreasonable decisions and avoiding extra costs.

An institution of higher education is an organizational structure with everchanging work flows. This is why it is necessary to constantly renew programs. IT facilitates to the innovations made at any University. Moreover, the more sophisticated the processes at a university evolve the more sophisticated are the required IT systems.

High-technology growth requirements of an educational institution network computing resources protection. Current became a necessity for the security system, which implies the existence of the legal and normative basis, the formation of a new security concept, special measures for the development of safety procedures for planning, design, implementation of technical means to protect the information. All of the above information security at the University System kompontebi define common policy. Educational institutions in the information security specificity lies in the fact that a public institution of higher sastsavlebebli auditoriita constantly changing and "novice cyber criminals" active growth.

Studies have shown that still has not been studied and established standards, which will ensure full security of information. Information security issues are becoming more and more relevant in almost every modern organization. Because of this, organizations often hire special companies / specialists in order to check the security of their organizations. Certain types of institutions, such as joint stock companies, in most cases, a number of departments are staffed by professionals who provide security norms, limits on their full functioning. Today, the field is still in the development stage and enjoys considerable popularity, especially in large organizations.

The first chapter of the thesis deals with the structure and the information system security, system modules, infrastructure scheme. The second and third chapters deals with information security requirements, and their main sources of information security risks. As for

the fourth yourself, there is considered an information security policy and management roles and responsibilities. The fifth and sixth chapters of the goal set out in the Information Security, performance and decision criteria, the information security management system efficiency measures. The seventh chapter deals with the analysis of data and evaluation of results. Finally, this paper sets out a simple method, which is available at the university's information security evaluation.

შინაარსი

შესავალი

სამუშაოს აქტუალობა. საბაზრო ურთიერთობების განვითარებამ, უმაღლესი განათლების სფეროში წარმოშვა კონკურენცია უმაღლეს სასწავლებლებს შორის საგანმანათლებლო მომსახურებაზე. განათლების ხარისხი წარმოადგენს მნიშვნელოვან მახასიათებელს, რომელიც განსაზღვრას უმაღლესი სასწავლებლის კონკურენტუნარიანობას. განათლების ხარისხის ამაღლების ამოცანა მჭიდროდ არის დაკავშირებული საგანმანათლებლო პროცესების და უმაღლესი სასწავლებლის რესურსების ეფექტურ მართვასთან. ამ ამოცანების გადაწყვეტა შეუძლებელია მართვის კომპლექსური ინფორმაციული სისტემის გამოყენების გარეშე. უმაღლესი სასწავლებელი - ეს არის ფუნქციების კრებული გადანაწილებული სასწავლებლის ქვედანაყოფებს შორის. ქვედანაყოფის თანამშრომელი თავის სამუშაოს შესრულებისას უშუალოდ მონაწილეობს უმაღლეს სასწავლო დაწესებულების ინფორმაციულ პროცესებში, რომელიც საჭიროებს შესაბამისი დონის ინფორმაციულ უსაფრთხოებას.

ინფორმაცია ისეთივე არსებითი აქტივია, როგორც საქმიანობის მართვის სხვა მნიშვნელოვანი აქტივები და მას შესაბამისი დაცვა სჭირდება. ეს საკითხი განსაკუთრებით აქტუალური ხდება ურთიერთდამოკიდებულ და დაკავშირებულ გარემოში, რასაც შედეგად მოსდევს სისუსტეებისა და საფრთხეების მზარდი რაოდენობის მიმართ ინფორმაციის დაუცველობა.

ინფორმაცია შესაძლოა არსებობდეს მრავალი ფორმით. იგი შეიძლება იყოს ქაღალდზე, ელექტრონული ფოსტის მეშვეობით ან სხვა საშუალებებით გადაცემული, ფილმებში ნაჩვენები, ან საუბრისას ნათქვამი. რა ფორმითაც არ უნდა არსებობდეს, ან რა საშუალებებითაც არ უნდა ხდებოდეს მისი გადაცემა, ინფორამცია ყოველთვის უნდა იყოს შესაბამისად დაცული . თუმცა, ინფორმაციის უმეტესობა დღეისათვის, ნაწილობრივ მაინც, საინფორმაციო ტექნოლოგიებითაა (IT) შექმნილი, შენახული, ტრანსპორტირებული ან გადამუშავებული და შესაბამისად, საჭიროა IT ლანდშაფტის სათანადო დაცვა. ქვეყანაში მიმდინარე რეფორმების ფონზე არსებული მუდმივად ცვალებადი გარემო გავლენას ახდენს ორგანიზაციების მუშაობის ეფექტიანობაზე და დგება ადაპტაციის საჭიროება. ცვლილებების გატარება დაკავშირებულია

ორგანიზაციულ განვითარებასთან, თუმცა, აუცილებელია შესაბამისი ღონისძიებების გატარება, რათა თავიდან იქნეს აცილებული უარყოფითი ეფექტი – „გვერდითი მოვლენები“.

საგანმანათლებლო დაწესებულებები, მათი ინფორმაციული სისტემები და ქსელები უშუალოდ დგანან ისეთი საფრთხეების პირისპირ, როგორებიცაა კომპიუტერული თაღლითობა, შპიონაჟი, საბოტაჟი, ვანდალიზმი, ხანძარი ან წყალდიდობა. მავნე კოდის შემცველი პროგრამები, კომპიუტერული ჰაკეროზა, კომპიუტერულ პროგრამაზე თავდასხმა მომხმარებლისთვის სერვისის შეფერხებით მიწოდების მიზნით უფრო და უფრო დახვეწილი ხერხებით ხორციელდება. და ასეთი ქმედებებიდან გამოწვეული ზარალი სულ უფრო იზრდება.

უსაფრთხოება არ არის უცვლელი მდგომარეობა, რომელიც მიიღწევა ერთხელ და შემდეგ არასდროს იცვლება. ყოველი დაწესებულება ექვემდებარება მუდმივ დინამიკურ ცვლილებებს. შესამჩნევ ცვლილებებთან (რომელიც დაკავშირებული ბიზნესპროცესების სპეციალიზებული ამოცანების, ინფრასტრუქტურის, ორგანიზა-ციული სტრუქტურების IT-ის და საინფორმაციო უსაფრთხოების ცვლილებებთან) ერთად იცვლება გარე პირობები, როგორიცაა სამართლებრივი ან ხელშეკრულებით გათვალისწინებული მოთხოვნები, ასევე რადიკალურად შეიძლება შეიცვალოს არსებული ინფორმაციის ან საკომუნიკაციო ტექნოლოგიებიც. აქედან გამომდინარე, აუცილებელია უსაფრთხოების აქტიური მართვა, რათა შენარჩუნდეს უსაფრთხოების მიღწეული დონე.

ორგანიზაცია საჭიროებს მართვის სისტემაში დროული და საჭირო ცვლილებების განხორციელებას, რაც ასრულებს ინდიკატორის როლს პერსონალის პროდუქტიულობის ზრდის და საგანმანათლებლო დაწესებულების პროგრესული განვითარებისა და გარდაქმნის პროცესში.

ზემოაღნიშნულიდან გამომდინარე, **კვლევის მიზანს** წარმოადგენს საუნივერსიტეტო პროცესების მართვის სისტემის ინფორმაციული უსაფრთხოება. კერძოდ, გამოავლინოს უმაღლესი საგანმანათლებლო დაწესებულებების (თსუ-ს მაგალითზე) შედეგის მიღწევაში ინფორმაციული უსაფრთხოების არსებული ხარვეზები, ამ ხარვეზების მიზეზები და განსაზღვროს, რა უნდა გაკეთდეს ხარვეზების

გამოსასწორებლად. ანალიზს შეუძლია გამოავლინოს შედეგის მიღწევაში არსებული ხარვეზები/ხელისშემშლელი ფაქტორები ორგანიზაციულ დონეზე, პროცესების დონეზე, დეპარტამენტის/განყოფილებების ან ინდივიდის დონეზე.

სამაგისტრო ნაშრომში დასახული ძირითადი მიზნის მიღწევისათვის გადაწყვეტილია შემდეგი ამოცანები:

1. ინფორმაციული უსაფრთხოების მოთხოვნების დონის შეფასება.
2. რისკის დონის განსაზღვრა და მისი ანალიზი.
3. ინფორმაციული უსაფრთხოების პოლიტიკის ჩამოყალიბება.
4. ინფორმაციული უსაფრთხოების დონის განსაზღვრის მეთოდის შემუშავება უნივერსიტეტის მიზნების და რესურსების გათვალისწინებით,

კვლევის ობიექტი. კვლევის ობიექტს წარმოადგენს თბილისის სახელმწიფო უნივერსიტეტში საუნივერსიტეტო პროცესების მართვის ავტომატიზებული სისტემა და მისი უსაფრთხოების დონის ანალიზის მეთოდების შერჩევა. ნაშრომში გამოყენებულია სისტემური ანალიზის მეთოდები, მონაცემთა ბაზის ორგანიზების მეთოდები.

სამუშაოს სამეცნიერო სიახლეს წარმოადგენს:

თსუ-ში ინფორმაციული უსაფრთხოების მართვის სპეციალური სტრუქტურის მოდელის ჩამოყალიბება. თუმცა, გამომდინარე იქიდან, რომ თავდაპირველ ეტაპზე, ისევ და ისევ არსებული რესურსების კვალდაკვალ, ეს შეიძლება გარკვეულწილად დიდ ხარჯებთან იყოს დაკავშირებული, შესაძლებელია შემუშავებული იქნას ალტერნატიული ვარიანტიც, რაც გულისხმობს არსებული ფინანსური და ადამიანური რესურსების გამოყენებას პასუხისმგებლობისა და ფუნქციების განსხვავებული გადანაწილების ხარჯზე.

თავი 1. ინფორმაციული სისტემის სტრუქტურა და მისი უსაფრთხოება

უნივერსიტეტის მენეჯმენტის ძირითად მიმართულებაზე დაყრდნობით საუნივერსიტეტო ინტეგრირებული ინფორმაციული კომპლექსი უზრუნველყოფს ინფორმაციულ მხარდაჭერას და სასწავლო პროცესების ოპერატიული მართვის ავტომატიზაციას ფაკულტეტებზე და კათედრებზე. ის უზრუნველყოფს სტუდენტთა კონტიგენტის, სტუდენტების მხრიდან სასწავლო პროგრამის მეთვალყურეობის და სასწავლო მიღწევების მონიტორინგს, სასწავლო გეგმების ფორმირების, სასწავლო დატვირთვების დაანგარიშების, აუცილებელი დოკუმენტების ფორმირების, ოპერატიული და ანალიტიკური ინფორმაციული მოთხოვნების დამუშავების მომსახურებას.

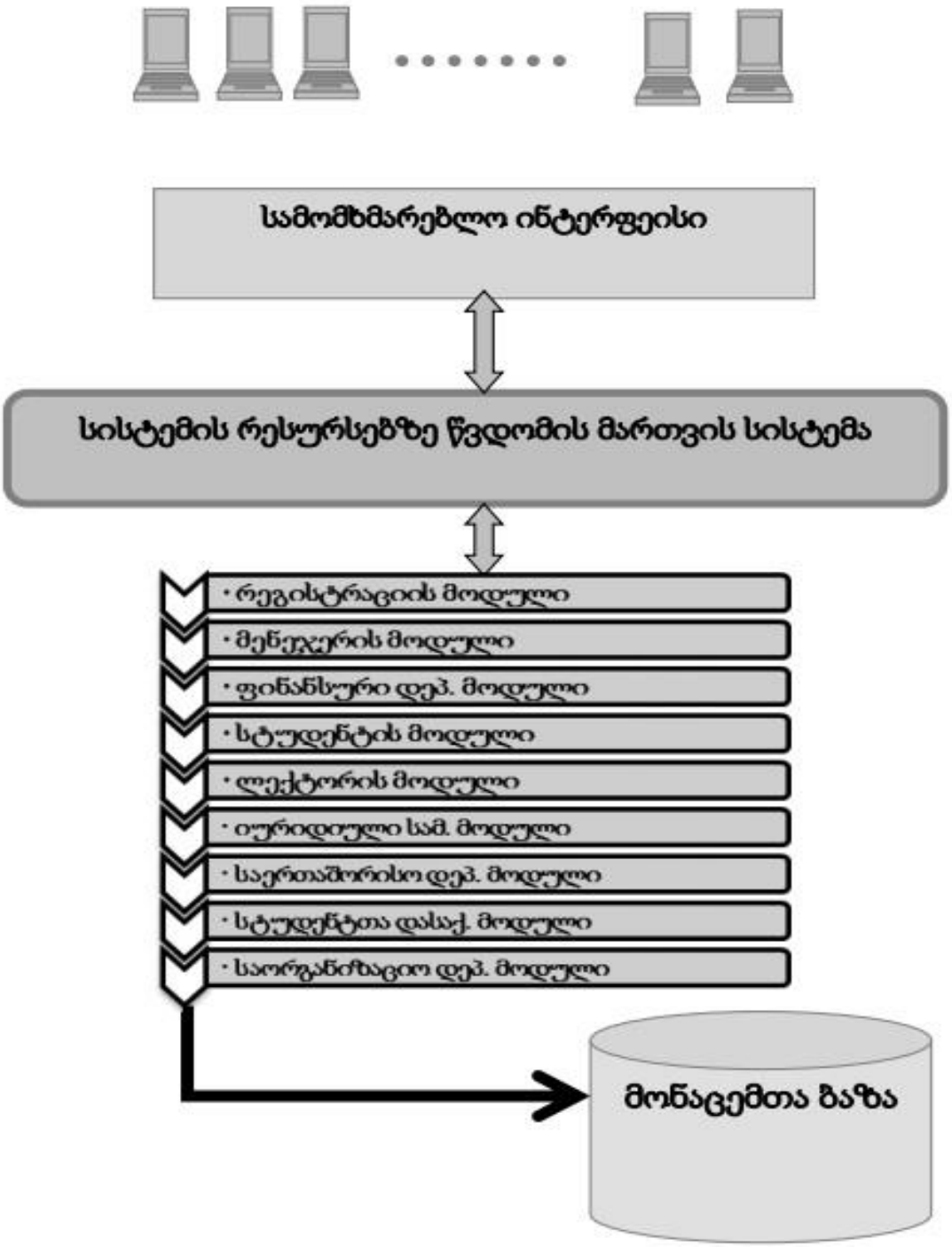
მთავარი იდეა, რომელიც განსაზღვრავს უნივერსიტეტის მართვის ინფორმატიზაციის პრინციპებს და ტექნოლოგიას, წარმოადგენს ერთიანი ინფორმაციული გარემოს შექმნა, რომელიც აერთიანებს ყველა ინფორმაციულ რესურს ცენტრალიზებულ მართველობაში და ფლობს მარტივ და ეფექტურ მექანიზმებს, რომლებიც უზრუნველყოფენ მოხმარების უფლებას საჭირო ინფორმაციის გამოყენებაზე. ტექნიკურად ინტეგრაცია მიიღწევა ერთიანი ინფორმაციული საცავის შექმნით, რომელიც ინახავს სხვადასხვა სახის მონაცემებს. მონაცემები საცავში განთავსებამდე გადის აუცილებელ ანალიზს და კლასიფიკაციას, რომელიც საშუალებას გვაძლევა თავიდან ავიცილოთ არასასურველი დუბლირება, რაც უზრუნველყოფს შენახული ინფორმაციის სანდოობის მაღალ დონეს.

სისტემა შედგება შემდეგი მოდულებისაგან:

- რეგისტრაციის;
- მენეჯერის ვირტუალური პორტალის;
- ფინანსური;
- სტუდენტისათვის ვირტუალური პორტალის;
- ლექტორისთვის ვირტუალური პორტალის;
- იურიდიული სამსახურის;
- საერთაშორისო ურთიერთობების;

- სტუდენტთა დასაქმების;
- საორგნიზაცო დეპარტამენტის;

ინფორმაციული სისტემის სტრუქტურა



მონაცემთა ბაზების მართვის სისტემის ამორჩევა წარმოადგენს ერთ- ერთ მთავარ ეტაპს ავტომატიზებული სისტემის შექმნის დროს. ამორჩეული სისტემის რესურსებზე წვდომის მართვის სისტემა სამომხმარებლო ინტერფეისი სისტემის მომხმარებელი მონაცემთა ბაზა 28 პროგრამული პაკეტი უნდა აკმაყოფილებდეს როგორც მიმდინარე, ისე უმაღლესი სასწავლებლის სამომავლო მოთხოვნებს. ამავე დროს, უნდა გავითვალისწინოთ დამუშავების ხარჯები, აუცილებელი პროგრამული უზრუნველყოფის პარამეტრების მორგება და ასევე პერსონალის სწავლება. მონაცემთა ბაზების მართვის სისტემის ამორჩევისას ყველაზე სწორი მიდგომა ეფუძნება იმის შეფასებას, თუ არსებული სისტემებიდან, რომელი აკმაყოფილებს ინფორმაციულის სისტემის მიმართ წაყენებულ მოთხოვნებს.

არსებობს მონაცემთა ბაზების სამართავი სისტემის ამორჩევის რამდენიმე კრიტერიუმი:

- მონაცემთა მოდელირება;
- არქიტექტურის თავისებურებები და ფუნქციონალური შესაძლებ-
- ლობები, სისტემის მუშაობის კონტროლი;
- პროგრამების დამუშავების თავისებურებები;
- მწარმოებლურობა;
- საიმედოობა;
- სამუშაო გარემოს მოთხოვნები;
- შერეული კრიტერიუმები;

აღნიშნული კრიტერიუმების ანალიზი საშუალებას იძლევა კონკრეტული პროექტისთვის რაციონალურად ამოვირჩიოთ შესაფერისი სისტემა. ჩამოთვლილი კრიტერიებს შეუძლიათ ამოცანის მაშტაბის გარკვევა და მისი ადეკვატურად გადაწყვეტა.

თანამედროვე პირობებში სასწავლო პროცესის ინფორმაციული რესურსების მართვის ეფექტური მექანიზმების შექმნა, შეუძლებელია ინფორმაციული უსაფრთხოების სამეცნიერო დასაბუთების და დაბალანსებული პოლიტიკის პრაქტიკულად განხორციინფორმაციული სისტემის უსაფრთხოების ქვეშ იგულისხმება, სისტემის დაცვა, მისი ნორმალური პროცესის ფუნქციონირებაში შემთხვევითი და

მიზანმიმართული ჩარევისაგან, ინფორმაციის მოპარვის მცდელობისაგან, მისი კომპონენტების მოდიფიცირებისა ან ფიზიკური განადგურებისაგან, ანუ ის არის ინფორმაციულ სისტემაზე სხვა და სხვა საგანგაშო ზემოქმედების განეიტრალების შესაძლებლობაელების გარეშე.

უმაღლეს სასწავლებელში ინახება და მუშავდება დიდი რაოდენობის სხვადასხვა მონაცემები, რომლებიც დაკავშირებულია არა მარტო სასწავლო პროცესის უწყვეტი რეჟიმის წარმართვასთან, არამედ სამეცნიერო- კვლევითი და კონსტრუქციული პროექტების განხორციელებასთან, სტუდენტებისა და პერსონალის პირადი მონაცემების დამუშავებასთან, ოფიციალური, კომერციული და კონფედენციალური ინფორმაციის შენახვასთან. მაღალი ტექნოლოგიების სფეროში დანაშაულების ზრდამ განაპირობა მოთხოვნები სასწავლო დაწესებულების გამოთვლითი ქსელების რესურსების დაცვის კუთხით. აქტუალური გახდა საკუთარი უსაფრთხოების სისტემის შექმნის აუცილებლობა, რაც გულისხმობს სამართლებრივ-ნორმატიული ბაზის არსებობას, უსაფრთხოების კონცეფციის ფორმირებას, სპეციალური ღონისძიებების შემუშავებას, უსაფრთხოების მიზნით პროცედურების დაგეგმვას, პროექტირებას, ინფორმაციის დასაცავი ტექნიკური საშუალებების რეალიზებას. ყველა ზემოთ ჩამოთვლილი სისტემური კომპონტები განსაზღვრავს უნივერსიტეში ინფორმაციული უსაფრთხოების დაცვის ერთიან პოლიტიკას. საგანმანათლებლო დაწესებულებებში ინფორმაციის დაცვის სპეციფიკა მდგომარეობს იმაში, რომ უმაღლესი სასწავლებებლი საჯარო დაწესებულებაა მუდმივად ცვალებადი აუდიტორიითა და „დამწყები კიბერ კრიმინალების“ აქტიური ზრდით. პოტენციური დამნაშავეების ძირითად ჯგუფს ქმნიან სტუდენტები, რომელთაგან ზოგიერთს გააჩნია ცოდნის საკმარისი დონე. 18-დან 23 - წლამდე ასაკი და ახალგაზრდული მაქსიმალიზმი უღვიძებს ასეთ ადამიანებს იამაყონ ცოდნით თავისი ჯგუფელების წინაშე-მოაწყონ ვირუსული ეპიდემია, მიიღონ 35 ადმინისტრაციული წვდომა და „დასაჯონ“ პედაგოგები, დაბლოკონ ინტერნეტში შესვლა და ა.შ

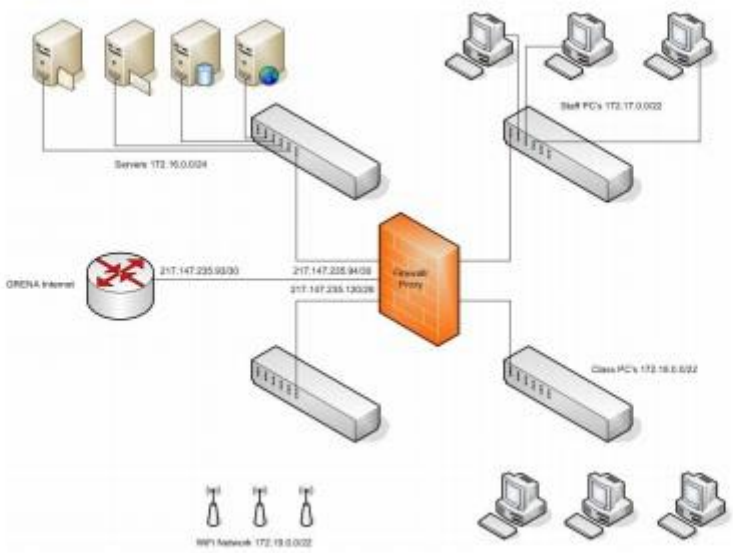
ინფორმაციული სისტემის უსაფრთხოების დაცვაზე მნიშვნელოვან გავლენას ახდენს: ინფორამციული გარემოს არქიტექტურა, ინფორმაციულ რესურსებზე ხელმისაწვდომობის უფლებების მართვა.

ინფორამციული გარემოს არქიტექტურის სტრუქტურა მოიცავს:

- ინფრასტრუქტურა
- საინფორმაციო რესურსები

ინფრასტრუქტურა - რომელიც უზრუნველყოფს სერვისების საიმედო, უსაფრთხო და 24 საათიან რეჟიმში ფუნქციონირებას და საინფორმაციო რესურსები - ნებისმიერ ადგილიდან და ნებისმიერ დროს უმაღლესი სასწავლებლის საინფორმაციო რესურსებთან მარტივ და საიმედო წვდომას.

ინფრასტრუქტურის სქემა



ინფორმაციული სისტემის უსაფრთხოების დაცვის ერთ-ერთ მნიშვნელოვან მეთოდს წარმოადგენს ინფორმაციულ რესურსებზე ხელმისაწვდომობის უფლებების მართვა. როგორც წესი, უმაღლეს სასწავლებელში გამოიყენება რამდენიმე პროგრამული პროდუქტი და ინფორმაციული სისტემები. თითოეულს გააჩნია რეგისტრაციის და უფლებების ადმინისტრიების საკუთარი სისტემა. ასეთი სისტემების მართვისთვის აუცილებელია ე.წ. ადმინისტრატორები, რომელთა ფუქნციაა მომხმარებლის კატეგორიისა და მათი უფლებების განსაზღვრა. უმაღლესი სასწავლებლის ინფორმაციულ სისტემაზე წვდომის უფლება ეძლევათ, როგორც თანამშრომლებს ასევე

სტუდენტებსა და ლექტორებს. მათი რაოდენობა მუდმივად ცვალებადია, შესაბამისად, იქმნება ინფორმაციულ რესურსებზე ხელმისაწვდომობის უფლებების მართვის ავტომატიზაციის აუცილებლობა.

ქსელის დაუცველობა „ხაკერს“ აძლევს პოტენციურ საშუალებას არასანქცირებული წვდომისა და ფალსიფიკაციის. უსაფრთხოების დასაცავად გამოყენებულია AAA (Authentication, Authorization, and Accounting) საშუალება, რომელიც ახორციელებს ქსელის მომხმარებლის აუტენტიფიკაციის, ავტორიზაციისა და აღრიცხვის შესაძლებლობას. AAA არქიტექტურის საშუალებით იზღუდება „ხაკერის“ შესაძლებლობები და კანონიერ მომხმარებელს ეძლევა რესურსებზე წვდომის საშუალება. მას გააჩნია მოდულური სტრუქტურა, რომელიც შედგება სამი კომპონენტისგან: 1. აუტენტიფიკაცია - ითხოვს პიროვნებისგან დამტკიცებას, რომ ის ნამდვილად წარმოადგენს ქსელის მომხმარებელს (მაგალითად: მომხმარებლის სახელის და პაროლის შეყვანა); 2. ავტორიზაცია - აუტენტიფიკაციის შემდეგ, ავტორიზაცია იღებს გადაწყვეტილებას თუ რომელ რესურსზე აქვს წვდომის უფლება მომხმარებელს და რომელი მოქმედებების შესრულებაა ნებადართული; 3. აღრიცხვა - აფიქსირებს ჩანაწერების სახით მომხმარებლის მონაცემბზე წვდომის დროსა და ინფორმაციას მისი ქმედებების შესახებ. უსაფრთხოების ინციდენტებს, მათ შორის ინფორმაციის გამჟღავნებას ან მანიპულირებას შეიძლება ჰქონდეს დამაზიანებელი შორსმიმავალი ზემოქმედების უნარი, ან აფერხებდეს ამოცანების შესრულებას, რაც შესაბამისად, იწვევს მაღალ ხარჯებს. ინფორმაციული უზრუნველყოფისთვის ხელმძღვანელობის დონეს აქვს დიდი პასუხისმგებლობა. ხელმძღვანელობის დონე აქტიურად უნდა აინიცირებდეს, მართავდეს და აკონტროლებდეს უსაფრთხოების პროცესს.

ამისთვის განიხილება შემდეგი ამოცანები:

1.მიღებულ უნდა იქნას ინფორმაციული უსაფრთხოების სტრატეგია და უსაფრთხოების მიზნები;

2. უსაფრთხოების რისკების გავლენა ბიზნესზე ან ამოცანების შესრულებაზე უნდა იქნას გამოკვლეული;

3. უნდა შეიქმნას ორგანიზაციული ჩარჩოს პირობები ინფორმაციული უსაფრთხოებითვის;

4. ინფორმაციული უსაფრთხოებითვის უნდა გამოიყოს საკმარისი რესურსები;

5. უსაფრთხოების სტრატეგია სისტემატურად უნდა მოწმდებოდეს და ტარდებოდეს მიზნის მიღწევის მონიტორინგი. გამოვლენილი ნაკლოვანებანი და შეცდომები უნდა გასწორდეს. ამისათვის უნდა შეიქმნას „ნოვატორული“ სამუშაო კლიმატი და ორგანიზაციის შიგნით მუდმივი სრულყოფის ნების დემონსტრირება;

6. თანამშრომლები მოტივირებული უნდა იყვნენ უსაფრთხოების საკითხებზე და ინფორმაციული უსაფრთხოება განიხილონ როგორც თავიანთი ამოცანების მნიშვნელოვანი ასპექტი. ამისათვის საჭიროა, სხვებთან ერთად, საკმარისი საინფორმაციო-საგანმანათლებლო ღონისძიებების შეთავაზება.

„საინფორმაციო სისტემების მენეჯმენტის საერთაშორისო გამოცდილება.“

მართვის არარსებობას, არაადეკვატური უსაფრთხოების სტრატეგიას ან არასწორ გადაწყვეტილებებს შეიძლება ჰქონდეს შორს მიმავალი უარყოფითი ეფექტები როგორც უსაფრთხოების ინციდენტებზე, ასევე ხელიდან გაშვებულ შესაძლებლობებსა და ცუდ ინვესტიციებზე.

სწორ და დროულ ინვესტიციებს ინფორმაციულ ინფორმაციულ უსაფრთხოებაში შეუძლია:

- ხელი შეუწყოს ხარჯების ეკონომიას , ხშირ შემთხვევაში - საშუალოვადიან პერსპექტივაშიც კი.
- მაღალი სამუშაო ხარისხი.
- კლიენტთა ნდობის ამაღლება.
- IT ლანდშაფტის ოპტიმიზაცია და ორგანიზაციული პროცესები,
- სინერგიული ეფექტების გამოყენება ინფორმაციული უსაფრთხოების მენეჯმენტის უკეთესი ინტეგრაციის საშუალებით არსებულ სტრუქტურებში.

თავი 2. ინფორმაციული უსაფრთხოების მოთხოვნები

გამომდინარე იქიდან, რომ სხვადასხვა დაწესებულებას აქვს სხვადასხვა საწყისი პირობები, უსაფრთხოების მოთხოვნები და ფინანსური საშუალებები განსხვავებულია. მცირე დაწესებულებები და კომპანიები არ უნდა შეშინდნენ, რადგან უსაფრთხოების პროცესის ხარჯები, როგორც წესი, ორგანიზაციის ზომებზეა დამოკიდებული. ამგვარად, ძალიან დიდ კომპანიაში, რომელსაც მრავალი განყოფილება და თანამშრომელი ჰყავს, ალბათ მოითხოვს უფრო ფორმალურ პროცესს და ზუსტად ამტკიცებს, თუ რომელი შიგა და გარე აუდიტებია საჭირო, ვინ ვისთანაა პასუხისმგებელი, ვინ ქმნის გადაწყვეტილებათა დოკუმენტებს, როდის იძლევა ხელმძღვანელობა უსაფრთხოების პროცესზე კონსულტაციას.

ინფრომაციული სისტემების გარკვეული რაოდენობა არ შეიცავს უსაფრთხოების მოთხოვნებს. უსაფრთხოება, რომელიც ტექნიკური საშუალებებით მიიღწევა, შეზღუდულია და მისი მხარდაჭერა უნდა მოხდეს შესაბამისი მენეჯმენტისა და პროცედურების მეშვეობით. სასურველი და საჭირო კონტროლის მექანიზმების გამოვლენა მოითხოვს ფრთხილ დაგეგმვას დეტალების გათვალისწინებით. ინფორმაციული უსაფრთხოების მართვა მოითხოვს ყველა თანამშრომლის თანამონაწილეობას. ამის გარდა, იგი შესაძლოა მოითხოვდეს დაინტერესებული წრეების, მომწოდებლების, მესამე მხარის, მომხმარებლების ან გარე მხარეების მონაწილეობას.შესაძლოა ასევე აუცილებელი გახდეს გარედან მოწვეული სპეციალისტის რჩევა.

როგორ ჩამოვაყალიბოთ ინფორმაციული უსაფრთხოების მოთხოვნები ?

მნიშვნლოვანია ის, რომ ორგანიზაციამ გამოავლინოს უსაფრთხოების საკუთარი მოთხოვნები. არსებობს უსაფრთხოების მოთხოვნების სამი ძირითადი წყარო:

1. პირველი წყარო არის ორგანიზაციისთვის რისკების შეფასება, რაც ასევე ითვალისწინებს ორგანიზაციის ბიზნესის სტრატეგიას და მიზნებს. რისკების შეფასების მეშვეობით გამოვლენილია საფრთხეები, რომლებიც ემუქრება აქტივებს, შეფასებულია სისუსტეები, მათი ხდომილების ალბათობა და მათი პოტენციური გავლენა.

2. მეორე წყარო არის იურიდიული, კანონით დადგენილი, მარეგულირებელი და სახელშეკრულებო მოთხოვნები, რომლებიც ორგანიზაციამ, მისმა სავაჭრო პარტნიორმა, კონტრაქტორებმა და მომსახურების მომწოდებლებმა უნდა დააკმაყოფილონ, აგრეთვე გასათვალისწინებელია სოციალურ-კულტურული გარემო.

3. შემდეგი წყარო წარმოადგენს პრინციპების, მიზნებისა და ბიზნესის (საქმისწარმოების) მოთხოვნების ნაკრებს, რომელიც შემუშავებულია ორგანიზაციაში ოპერაციების მხარდამჭერი ინფორმაციის დამუშავებისთვის.

თავი 3. ინფორმაციული უსაფრთხოების რისკები

უსაფრთხოების რისკების შეფასება. უსაფრთხოების მოთხოვნების გამოვლენა ხდება უსაფრთხოების რისკების სისტემური და რეგულარული შეფასების მეშვეობით. კონტროლის მექანიზმების გამოყენების ხარჯები უნდა შეესაბამებოეს უსაფრთხოების გარღვევით გამოწვეულ უარყოფით შედეგებს. რისკების შეფასების შედეგები დახმარებას გაუწევს შესაბამისი მენეჯერული ქმედებების განსაზღვრას და გაძღოლას, ინფორმაციული უსაფრთხოების რისკების მართვის პრიორიტეტების დადგენას, აგრეთვე, გამოვლენილი რისკების საპასუხოდ დაცვის შერჩეული კონტროლის მექანიზმების დანერგვას. რისკების შეფასება პერიოდულად უნდა ხორციელდებოდეს, რათა ნებისმიერ ცვლილებაზე მოხდეს შესაბამისი რეაგირება , რამაც შესაძლოა გავლენა იქონიოს რისკების შეფასების შედეგებზე.

ორგანიზაციის მიზნებიდან გამომდინარე რისკის მიღების შესაბამისად, რიკსების შეფასების შედეგად უნდა გამოვლინდეს, რაოდენობრივად შეფასდეს და განისაზღვროს რისკების პრიორიტეტი.. შედგებმა უნდა განსაზღვროს მენეჯმენტის ის შესაძლო ქმედებები და პრიორიტეტები კონტროლის მექანიზმების დანერგვის პროცესში, რომლებმაც ორგანიზაცია ინფორმაციული უსაფრთხოების რისკებისგან უნდა დაიცვან. რიკსების შეფასების და კონტროლის პროცესი შესაძლოა განხორციელდეს რამდენჯერმე, რათა დაიცვას ორგანიზაციის სხვადასხვა მიმართულებები, ან საინფორმაციო სისტემები. რისკის შეფასება უნდა შეიცავდეს სისტემურ მიდგომას. საჭიროა ფასდებოდეს რისკის მაგნიტუდა (რისკების ანალიზი) და ხორციელდებოდეს მათი შედარება რისკების შეფასების კრიტერუმთან, რათა მოხდეს რისკის მნიშვნელოვნების დადგენა (რისკის დონის დადგენა).

რისკების შეფასებები უნდა ხორციელდებოდეს პერიოდულად, რათა შეფასების დროს აისახოს მომხდარი ცვლილებები. მაგალითად, უნდა შეფასდეს აქტივები, საფრთხეები, სისუსტეები, რისკის ზემოქმედება. უნდა დადგინდეს რისკის დონე იმ შემთხვევებისთვის, როდესაც ხორციელდება მნიშვნელოვანი ცვლილებები. რისკების შეფასება უნდა განხორციელდეს იმ მეთოდური მიდგომით, რომლებიც შედარებად შედეგებს იძლევა. ინფორმაცული უსაფრთხოების რისკის შეფასებას უნდა გააჩნდეს

მკაფიოდ დადგენილი ფარგლები, იმისათვის, რომ იყოს ეფექტიანი და ჰქონდეს კავშირი სხვა სფეროებში ჩატარებულ რისკების შეფასებებებთან(საჭიროების შემთხვევაში). რისკების შეფასება შეიძლება განხორციელდეს მთელი ორგანიზაციის მაშტაბით, მოიცავდეს ორგანიზაციის ნაწილს, ინდივიდუალურ საინფორმაციო სისტემას, კონკრეტული სისტემის კომპონენტებს, ან რომლიმე სერვისს. რისკების შეფასება საჭიროა ყველგან, სადაც ეს შესაძლებელია, პრაქტიკულია და გამოსადეგარია.

ინფორმაციული უსაფრთხოების რისკებთან მოპყრობა - რისკებთან მოპყრობის დაწყებამდე, ორგანიზაციამ უნდა განსაზღვროს რისკების მისაღებობის კრიტერიუმები. რისკი შეიძლება იყოს მიღებული, თუ, მაგალითად, მის მიერ მიყენებული პოტენციური ზარალი არის მცირე, ან მასთან მოპყრობის დანახრჯი არ არის მისაღები. ყოველი მსაგვსი გადაწყვეტულება უნდა იყოს აღწერილი და დოკუმენტირებული. თითოეული იდენტიფიცირებული რისკითვის, მათი შეფასების შესაბამისად უნდა განხორციელდეს გარკვეული რეაგირება.

რისკზე რეაგირება და მასთან მოპყრობა შესაძლოა მოიცავდეს შემდეგ ვარიანტებს:

- კონტროლის მექანიზმების დანერგვა რისკის შესამცირებლად;
- რისკის მიღება შეგნებულად და ობიექტურად, რაც ნათლად და ცალსახად შეესაბამება ორგანიზაციის პოლიტიკას, მიზნებს და რისკის მიღების კრიტერიუმს;
- რისკების თავიდან აცილება, მათი გამომწვევი მოვლენების არდაშვების შედეგად;
- რიკების გადაცემა ასოცირებული მხარეებისათვის, მაგალითად სადაზღვევო, სერვისების მომწოდებლი, ან სხვა ორგანიზაციებისთვის.

იმ რისკებისთვის, რომელთა მოპყრობის გადაწყვეტილება იქნა მიღებული, უნდა დაინრეგოს სათანადო კონტროლის მექნიზმები. ეს კონტროლის მექანიზმები უნდა შეირჩეს და დაინერგოს რისკების შეფასების მოთხოვნების შესაბამისად.

კონტროლის მექანიზმების შერჩევა - მას შემდეგ, რაც გამოვლინდება უსაფრთხოების მოთხოვნები და რისკები, ასევე მიღებული იქნება რისკებთან მოპყრობის შესახებ კონკრეტული გადაწყვეტილებები, უნდა მოხდეს კონტროლის შესაბამისი მექანიზმების შერჩევა და დანერგვა, რათა უზრუნველყოფილი იყოს რისკების შემცირება დასაშვებ,

მისაღებ დონემდე. კონტროლის მექანიზმების შერჩევა შესაძლოა მოხდეს მოცემული სტაბდარტიდან, ან კონტროლის მექანიზმების სხვა ნაკრებიდან, ან სრულიად ახალი კონტროლის მექანიზმების შემუშავებით, რაც ხელს შეუწყობს სასურველი მიზნების მიღწევას. უსაფრთხოების კონტროლის მექანიმზების შერჩევა დამოკიდებულია ორგანიზაციის მიერ განსაზღვრულ დასაშვები რისკების მიღების კრიტერიუმებზე, რისკებთან მოპყრობის სტრატეგიებზე და ზოგადად რისკების მართვისადმი ორგანიზაციის მიდგომაზე.

კონტროლის მექანიზმმა უნდა უზრუნველყოს რისკების მისაღებ დონეზე შემცირება და გათვალისწინოს შემდეგი:

- ეროვნული და საერთაშორისო საკონონმდებლო მოთხოვნები და რეგულაციები;
- ორგანიზაციული მიზნები;
- საოპერაციო მოთხოვნები;
- დანერგვისა და ფუნქციონირების ხარჯები, რაც დაკავშირებულია შესამცირებელ რისკებთან და არის ორგანიზაციის მოთხოვნების პროპორციული;
- უსაფრთხოების ჩავარდნებიდან გამომდინარე სავარაუდო ზიანის შესაბამისად კონტროლის მექანიზმების დანერგვისა და ფუნქციონირებისთვის ინვესტიციების დაბალანსების საჭიროება .

ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების გათვალისწინება აუცილებელია სისტემების და პროექტების მოთხოვნების ჩამოყალიბების და დიზაინის პროცესში. სხვაგვარად მოქცევამ შესაძლოა გამოიწვიოს პროექტის ღირებულების ზრდა, ან ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების გართულება ან/და შეუძლებლობა.

აუცილებელია აღინიშნოს, რომ ინფორმაციული უსაფრთხოების მიღწევ მხოლოდ კონტროლის მექანიზმების დანერგვით არ არის შესაძლებელი ა და აუცილებელია დამატებითი მმართველობითი ქმედებები: მონიტორინგი, განხილვა, ინფრომაციული უსაფრთხოების კონტროლის მექნიზმების ეფექტიანობის გაუმჯობესება ორგანიზაციის მიზნების მიღწევის მხარდასაჭერად.

თავი 4. ინფორმაციული უსაფრთხოების პოლიტიკა

4.1 ინფორმაციული უსაფრთხოების პოლიტიკის მიმოხილვა - მენეჯმენტმა უნდა ჩამოაყალიბოს პოლიტიკის ხედვა ბიზნეს-პროცესების მიზნებთან ერთად და წარმოაჩინოს ინფორმაციული უსაფრთხოებისთვის მხარდაჭერა და მზადყოფნა მისი დანერგვისთვის, რაც გამოიხატება ორგანიზაციაში ინფორმაციული უსაფრთხოების პოლიტიკის გამოცემითა და მხარდაჭერით. მისი მიზანია მენეჯმენტის მხრიდან ინფორმაციული უსაფრთხოების მართვა და მხარდაჭერა.

ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტი უნდა იყოს დამტკიცებული მენეჯმენტის მიერ, რის შემდეგაც უნდა გამოიცეს და მიეწოდოს ყველა თანამშრომელსა და დაკავშირებულ გარე მხარეს. იგი უნდა ასახავდეს მენეჯმენტის მზადყოფნას და დაადგინოს ორგანიზაციის მიდგომა ინფორმაციული უსაფრთხოების მართვისადმი. პოლიტიკის დოკუმენტი უნდა შეიცავდეს შემდეგი საკითხების ფორმულირებებს:

- ინფორმაციული უსაფრთხოების განმარტება, მისი მიზნები და ფარგლები, უსაფრთხოების, როგორც ინფორმაციის გაზიარების შუამავალი მექანიზმის (იხილეთ შესავალი) მნიშვნელოვნება;
- მენეჯმენტის მიზნების გაცხადება, ინფორმაციული უსაფრთხოების ამოცანებისა და პრინციპების მხარდაჭერა ბიზნესის (საქმიანობის ორგანიზების) სტრატეგიებსა და მიზნებთან ერთად;
- კონტროლის მიზნებისა და მექანიზმების ჩამოყალიბების ჩარჩოები, მათ შორის რისკების შეფასებისა და რისკების მართვის სტრუქტურა;
- უსაფრთხოების პოლიტიკის, პრინციპების, სტანდარტების და თავსებადობის მოთხოვნების მკაფიო განმარტება, რაც მოიცავს:
  - საკანონმდებლო, მარეგულირებელ და სახელშეკრულებო მოთხოვნებთან თავსებადობას;
  - უსაფრთხოების შესახებ სწავლების, ტრეინინგისა და ცნობიერების ამაღლების¬ მოთხოვნებს;
  - ბიზნეს-პროცესების უწყვეტობის მართვას;

- ინფორმაციული უსაფრთხოების პოლიტიკის დარღვევის უარყოფით შედეგებს;

- ინფორმაციული უსაფრთხოების მართვისთვის დადგენილი ძირითადი და სპეციფიკური პასხისმგებლობების განმარტება, მათ შორის ინფორმაციული უსაფრთხოების ინციდენტის შესახებ ანგარიშგება;
- პოლიტიკის მხარდამჭერი დოკუმენტაციის ჩამონათვალი, მაგალითად, უფრო დეტალური უსაფრთხოების პოლიტიკა და პროცედურები სპეციფიკური ინფორმაციული სისტემებისთვის ,ან უსაფრთხოების წესების მომხმარებლებისთვის.

ინფორმაციული უსაფრთხოების პოლიტიკა უნდა მიეწოდოს ორგანიზაციაში ყველა მომხმარებელს იმ ფორმით, რომელიც ხელმისაწვდომი და გასაგები იქნება სამიზნე აუდიტორიისთვის/მკითხველისთვის.იმ შემთხვევაში, თუ ინფორმაციული უსაფრთხოების პოლიტიკა უნდა მიეწოდოს ორგანიზაციის ფარგლებს გარეთ არსებულ მხარეებს, მაშინ ყურადღება უნდა გამახვილდეს (სენსიტიური) ინფორმაციის გაუმჟღავნებლობაზე.

4.2 მენეჯმენტის პასუხისმგებლობა

მენეჯმენტი პასუხისმგებელია ინფორმაციული უსაფრთხოების შეფასების პროგრამის ჩამოყალიბებაზე, რომელიც შეფასების საქმიანობაში მოიცავს შესაბამის დაინტერესებულ მხარეებს. მენეჯმენტმა უნდა გამოყოს რესურსები, რათა მოხდეს შეფასების ძირითადი ქმედებების მხარდაჭერა, როგორიცაა: მონაცემთა შეგროვება, ანალიზი, შენახვა, ანგარიშგება და გავრცელება. რესურსების განაწილება უნდა შეიცავდეს:

ა) ინფორმაციული უსაფრთხოების შეფასების პროგრამის ყველა ასპექტზე პასუხისმგებელ პირებს;

ბ) შესაბამის ფინანსურ მხარდაჭერას;

გ) შესაბამის ინფრასტრუქტურულ მხარდაჭერას, როგორიცაა ფიზიკური ინფრასტრუქტურა და შეფასების პროცესში გამოსაყენებელი ხელსაწყოები.

მენეჯმენტმა ასევე უნდა უზრუნველყოს ის , რომ ინფორმაციული უსაფრთხოების შეფასების პროგრამის ფარგლებშიმოხდეს დაინტერესებულ მხარეთათვის ტრენინგების ჩატარება მათი როლის და პასუხისმგებლობის შესაბამისად, რის შემდეგაც ისინი ხდებიან კვალიფიციურნი, რათა შეასრულონ მათზე დაკისრებული როლები და პასუხისმგებლობები.

<u>მენეჯმენტის ვალდებულებები შეგვიძლია ასე ჩამოვაყალიბოთ:</u>

- ჩამოაყალიბოს ინფორმაციული უსაფრთხოების შეფასების პროგრამის მიზნები;
- განსაზღვროს ინფორმაციული უსაფრთხოების შეფასების პროგრამის პოლიტიკა;
- ჩამოაყალიბოს ინფორმაციული უსაფრთხოების შეფასების პროგრამის როლები და პასუხისმგებლობა;
- უზრუნველყოს შეფასების პროცესი შესაბამისი რესურსებით, მათ შორის პერსონალით, დაფინანსებით, ხელსაწყოებით და ინფრასტრუქტურით;
- უზრუნველყოს, რომ ინფორმაციული უსაფრთხოების შეფასების პროგრამის მიზნები მიიღწევა;
- უზრუნველყოს, რომ მონაცემთა შეგროვების ხელსაწყოები და აღჭურვილობა გამოიყენება სწორად;
- შექმნას შეფასების მიზნები თითოეული შეფასების მოდელისთვის;
- უზრუნველყოს, რომ შეფასება აძლევს საკმარის ინფორმაციას შესაბამის დაინტერესებულ მხარეებს იუმს-ის ეფექტიანობის და გაუმჯობესების საჭიროებების თაობაზე და ფარავს მოქმედების არეალს, პოლიტიკას, მიზნებს, კონტროლებს, პროცესებს და პროცედურებს;
- უზრუნველყოს, რომ შეფასება აძლევს საკმარის ინფორმაციას შესაბამის დაინტერესებულ მხარეებს კონტროლების ან კონტროლთა ჯგუფის ეფექტიანობის და დანერგილი კონტროლების გაუმჯობესების საჭიროებების შესახებ.

შეფასების როლების და მოვალეობების შესაბამისი მინიჭებით მენეჯმენტმა უნდა უზრუნველყოს, რომ ინფორმაციის მფლობელები არ ახდენენ გავლენას შეფასების შედეგებზე ამის მიღწევა შესაძლებელია მოვალეობათა გამიჯვნით, ან თუ ეს შეუძლებელია, დეტალური დოკუმენტაციის გამოყენებით, რომლის მეშვეობით შესაძლებელია დამოუკიდებელი შემოწმება.

თავი 5. ინფორმაციული უსაფრთხოების შეფასება

5.1 შეფასების მიზანი.

ის შეიძლება ასე ჩამოვაყალიბოთ:

- ✓ დანერგილი კონტროლების ან კონტროლთა ჯგუფის ეფექტიანობის შეფასება.
- ✓ დანერგილი ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) ეფექტიანობის შეფასება.
- ✓ დადგენილი უსაფრთხოების მოთხოვნების დაკმაყოფილების დონის შემოწმება;
- ✓ ინფორმაციული უსაფრთხოების წარმადობის გაუმჯობესების ხელშეწყობა უმაღლესი სასწავლებლების რისკების ჭრილში;
- ✓ იუმს-თან დაკავშირებული მისაღები გადაწყვეტილებების და საჭირო გაუმჯობესების არგუმენტირების მიზნით მენეჯერული მიმოხილვის ხელშეწყობა.

შეფასების მიზნების ჩამოყალიბებისას უმაღლესმა სასწავლო დაწესებულებამ უნდა გააკეთოს შემდეგი დაშვებები:

- ინფორმაციული უსაფრთხოების როლი, სასწავლებლის ქმედებები და მათთან დაკავშირებული რისკები;
- შესაბამისი საკანონმდებლო, მარეგულირებელი და საკონტრაქტო მოთხოვნები;
- უნივერსიტეტის სტრუქტურა;
- ინფორმაციული უსაფრთხოების დანერგვის ხარჯები და სარგებელი;
- სასწავლებელში რისკების მიღების კრიტერიუმები;
- ალტერნატიული იუმს-ების შედარების აუცილებლობა.

უნდა შემუშავდეს და განხორციელდეს გაზომვის მეთოდები, რათა ინფორმაციული უსაფრთხოების მოდელის საფუძველზე მიიღოს განმეორებადი, ობიექტური და სასარგებლო შედეგები.

ინფორმაციული უსაფრთხოების შეფასების პროგრამა მოიცავს შემდეგ პროცესებს:

- საზომების შემუშავება.
- საზომების ფუნქციონირება.

- მონაცემთა ანალიზი და შეფასების შედეგების ანგარიშგება.
- ინფორმაციული უსაფრთხოების შეფასების პროგრამის შემოწმება და გაუმჯობესება.

ინფორმაციული უსაფრთხოების შეფასების პროგრამის მიერ შერჩეული და დანერგილი საზომები უშუალოდ უნდა იყოს იუმს-ის ფუნქციონირებასთან, სხვა საზომებთან, აგრეთვე სასწავლებელში მიმდინარე პროცესებთან დაკავშირებული. შეფასება შეიძლება ინტეგრირებული იყოს ჩვეულ საოპერაციო ქმედებებში, ან შესრულდეს იუმს-ის მიერ განსაზღვრულ პერიოდებში.

ჩამოვთვალოთ ინფორმაციული უსაფრთხოების შეფასების პროგრამის წარმატების რამდენიმე ფაქტორი, ესენია:

- მენეჯმენტის მზადყოფნა, რომელსაც მხარს უჭერს შესაბამისი რესურსები;
- იუმს-ის პროცესების და პროცედურების არსებობა;
- განმეორებადი პროცესი, რომელიც დროთა განმავლობაში მოიცავს მნიშვნელოვან მონაცემებს და აწარმოებს ანგარიშგებას საჭირო მიმართულებებით;
- იუმს-ის მიზნებიდან გამომდინარე რაოდენობრივი საზომები;
- შეფასებისათვის ადვილად მოსაპოვებელი მონაცემები;
- ინფორმაციული უსაფრთხოების შეფასების პროგრამის ეფექტიანობის შემოწმება და აღმოჩენილი გაუმჯობესებების დანერგვა;
- შეფასებისთვის საჭირო მონაცემების შეგროვება, მათი ანალიზი და ანგარიშგება;
- დაინტერესებული პირების მიერ შეფასების შედეგების გამოყენება, რათა იუმს-ში დაინერგოს გამოვლენილი გასუმჯობესებები, მათ შორის გავრცელების სფეროს, პოლიტიკების, მიზნების, კონტროლების, პროცესების და პროცედურების გათვალისწინებით;
- დაინტერესებული პირებისგან შეფასების შედეგების შესახებ უკუკავშირის მიღება;
- შეფასების შედეგების გამოყენებადობის შეფასება და გამოვლენილი გაუმჯობესებების ასახვა;

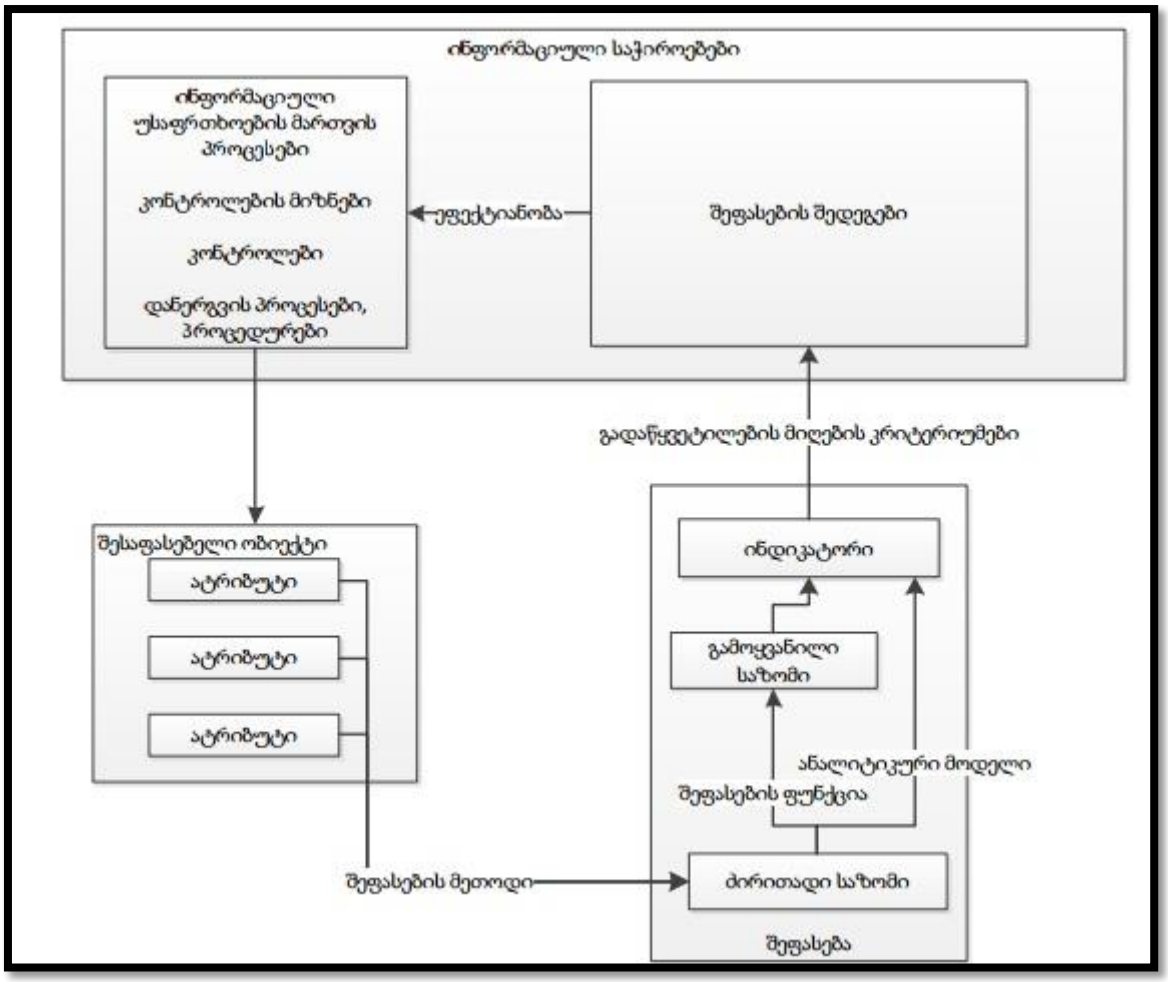
პროგრამის წარმატებით დანერგვას შეუძლია:

- საკანონმდებლო ან მარეგულირებელი მოთხოვნებისა და სახელშეკრულებო ვალდებულებებისადმი შესაბამისობის უზრუნველყოფა;
- ფარული ან უცნობი ინფორმაციული უსაფრთხოების საკითხების აღმოჩენის უზრუნველყოფა;
- მენეჯერული ანგარიშგების საჭიროებების ხელშეწყობა ისტორიული და მიმდინარე საქმიანობის შესახებ;
- გამოიყენებოდეს, როგორც ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის, იუმს-ის შიდა აუდიტის და მენეჯერული მიმოხილვების შემავალი რესურსები;

5.2 ინფორმაციული უსაფრთხოების შეფასების მოდელი

შეფასების მოდელი - ესაა სტრუქტურა, რომელიც აკავშირებს შესაფასებელი ობიექტებისათვის საჭირო ინფორმაციას მათ ატრიბუტებთან. შესაფასებელი ობიექტები შეიძლება მოიცავდეს დაგეგმილ ან დანერგილ პროცესებს, პროცედურებს, პროექტებს და რესურსებს. ინფორმაციული უსაფრთხოების შეფასების მოდელი აღწერს, თუ როგორ ხდება ატრიბუტების რაოდენობრივი შეფასება და ინდიკატორებად გარდაქმნა, რომლებიც გადაწყვეტილების მიღების საშუალებას იძლევა.

ინფორმაციული უსაფრთხოების შეფასების მოდელი ასე გამოიყურება



შეფასების მეთოდი არის ატრიბუტზე გარკვეული ოპერაციების ჩატარების თანმიმდევრობა რაოდენობრივი მახასიათებლის მიღების მიზნით, ხოლო ძირითადი საზომი - ესაა შესაფასებელი ობიექტისთვის შერჩეული ატრიბუტის შეფასების მეთოდის შედეგი. შესაფასებელ ობიექტს შესაძლოა გააჩნდეს ბევრი ატრიბუტი, რომლეთაგან მხოლოდ რამოდენიმეს გააჩნია ძრითად საზომად გამოსაყენებელი სასარგებლო მნიშვნელობები.

შეფასების მეთოდი გამოიყენება შესაფასებელი ობიექტის ატრიბუტების მიმართ. ობიექტის შეფასების მაგალითებად შეგვიძლია მოვიყვანოთ:

- იუმს-ში დანერგილი კონტროლების წარმადობა;
- კონტროლების მიერ დაცული ინფორმაციული აქტივების სტატუსი;

- იუმს-ში დანერგილი პროცესების წარმადობა;
- იუმს-ზე პასუხისმგებელი პერსონალის ქცევა;
- ინფორმაციულ უსაფრთხოებაზე პასუხისმგებელი ორგანიზაციული ქვედანაყოფების საქმიანობა;
- დაინტერესებულ პირთა კმაყოფილების ხარისხი.

შეფასების მეთოდი შესაძლოა გამოიყენებდეს შეფასების ობიექტებს ან ატრიბუტებს სხვადასხვა წყაროდან, ესენია:

- რისკის ანალიზი და რისკების შეფასების შედეგები;
- კითხვარები და პერსონალის გამოკითხვა;
- შიდა და გარე აუდიტის ანგარიშები;
- მოვლენების, ლოგების, სტატისტიკის და აუდიტისთვის საკონტროლო ჩანაწერები; ინციდენტის შესახებ ანგარიში, განსაკუთრებით ის, რომელიც აისახება შედეგში;
- ტესტირების შედეგები, მაგ. შეღწევადობის ტესტები, ადამიანური ფაქტორი (სოციალური ინჟინერია), შესაბამისობის ხელსაწყოები და უსაფრთხოების აუდიტის ხელსაწყოები;
- ჩანაწერები ორგანიზაციის ინფორმაციული უსაფრთხოების პროცედურებიდან და პოლიტიკებიდან, მაგალითად ინფრომაციული უსაფრთხოების ცნობადობის ტესტირების შედეგები.

ძირითადი საზომის არსი ვთქვით. არის ასევე წარმოებული საზომი, რომელიც წარმოადგენს ორი ან მეტი ძირითადი საზომის კომბინაციას. მოცემული ძირითადი საზომი შეიძლება გამოიყენებოდეს როგორც რამოდენიმე წარმოებული საზომის შემავალი რესურსი.გაზომვის ფუნქცია არის გარკვეული გამოთვლის მეთოდი, რომელიც ძირითად საზომებს გამოიყენებს წარმოებული საზომის მისაღებად. წარმოებული საზომის მასშტაბი და საზომი ერთეული დამოკიდებულია ძირითადი საზომების მასშტაბზე და საზომ ერთეულზე, რომელიც მის შემადგელობაში შედის, აგრეთვე ამ საზომების გამოყენების ხერხზე. გაზომვის ფუნქცია შეიძლება მოიცავდეს სხვადასხვა ტექნიკას, როგორიცაა ძირითადი საზომების გასაშუალოება, წონის გამოყენება, ან ხარისხობრივი კოეფიციენტების მინიჭება. გაზომვის ფუნქცია შეიძლება

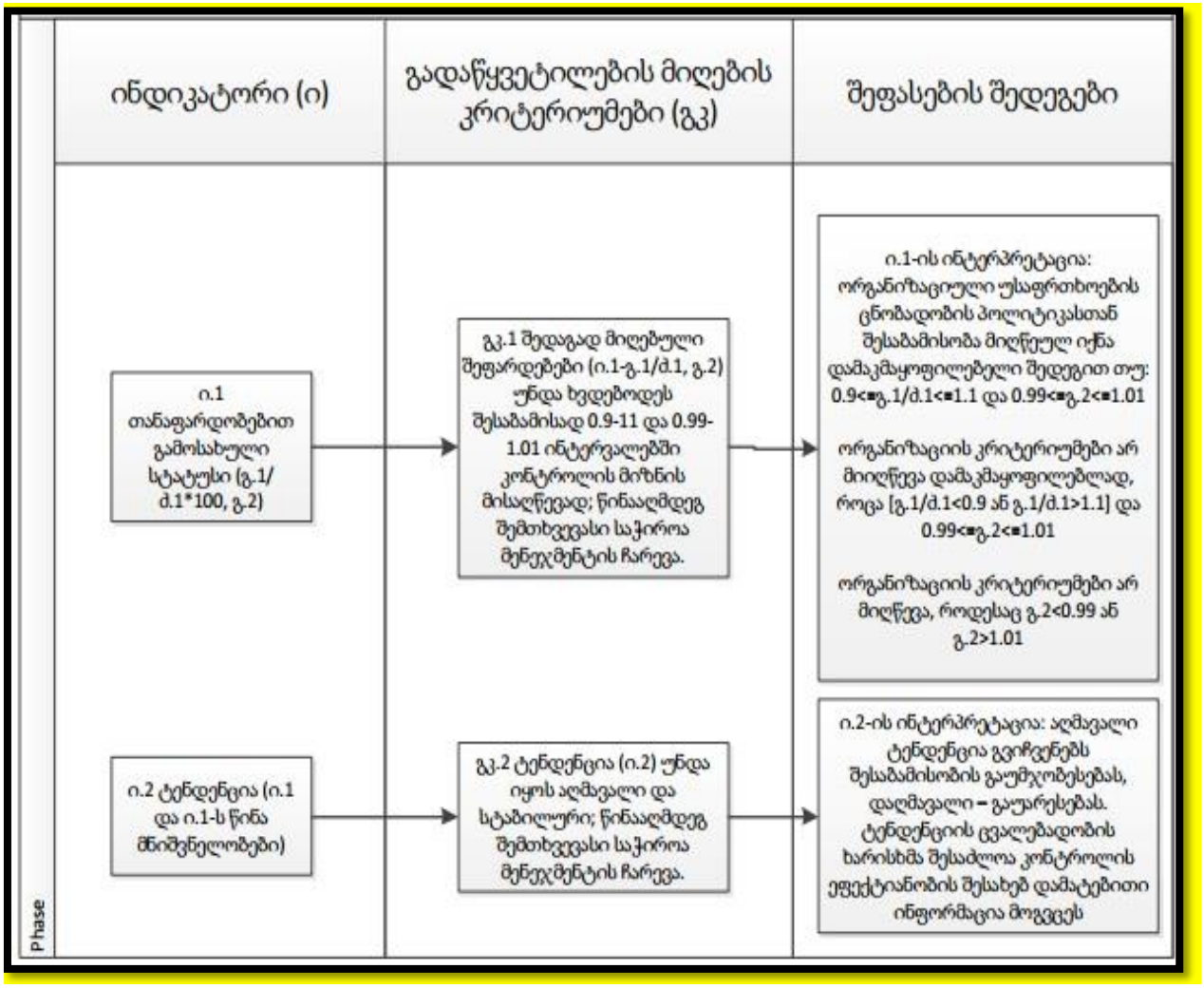
აერთიანებდეს ძირითად საზომებს სხვადასხვა მასშტაბით, როგორიცაა პროცენტები და ხარისხობრივი შეფასების შედეგები.

5.3 შეფასების მაჩვენებლები, შედეგები და გადაწყვეტილების კრიტერიუმები

მაჩვენებელი არის საზომი, რომელიც, ინფორმაციული საჭიროებიდან გამომდინარე, შეაფასებს ანალიტიკური მოდელის კონკრეტულ ატრიბუტს. მაჩვენებლები მიიღება ანალიტიკური მოდელის გამოყენებით ძირითად ან / და წარმოებულ საზომზე და მათი გადაწყვეტილების კრიტერიუმის მასშტაბი და გაზომვის მეთოდი გავლენას ახდენს მაჩვენებლების წარმოსაქმნელად გამოყენებულ ანალიტიკურ ტექნიკაზე. რაც შეეხება შეფასების შედეგებს, მას განაპირობებს შესაბამისი მაჩვენებლებით განსაზღვრული გადაწყვეტილების კრიტერიუმები და ითვალისწინებს იუმს-ის ეფექტიანობის შეფასების ზოგადი მიზნებს. გადაწყვეტილების კრიტერიუმები გასაზღვრავს შემდგომი გამოძიების აუცილებლობას ისევე, როგორც შეფასების შედეგების სანდოობას. გადაწყვეტილების კრიტერიუმები შეიძლება გამოყენებულ იქნას მთელ რიგ მაჩვენებლებზე, მაგალითად დროის სხვადასხვა მომენტში მიღებული მაჩვენებლების ტენდენციის ანალიზი. ობიექტებს წარმოადგენს ორგანიზაციის ან მისი ნაწილის წარმადობის დეტალური მახასიათებლები, რომლებიც მიიღება ინფორმაციული უსაფრთხოების მიზნებიდან, როგორებიცაა იუმს-ის გავრცელების სფერო და კონტროლის მიზნები, რომლებიც ჩამოყალიბებული და მიღწეული უნდა იქნას დასახული მიზნების მისაღწევად.

ცხრილის სახით შეგვიძლია ვნახოთ ინფორმაციული უსაფრთხოების მოდელის გამოყენების ელემენტების ურთიერთკავშირი, ანუ კავშირი მაჩვენებელს, გადაწყვეტილების კრიტერიუმებსა და შეფასების შედეგებს შორის.

შეფასების შედეგები და ანალიტიკური მოდელის მაგალითი



თავი 6. ინფორმაციული უსაფრთხოების მართვის სისტემის ეფექტიანობის საზომები და შეფასებების შემუშავება

გასატარებელ ღონისძიებათა კლასიფიკაცია. ინფორმაციული უსაფრთხოების მართვის სისტემის ეფექტიანობის საზომებისა და შეფასებების შამუშავებლად უნდა ჩამოყალიბდეს გასატარებელი ღონისძიებები და ეს ყველაფერი უნდა იყოს დოკუმენტირებული.

ამ გასატარებელ ღონისძიებათა შორის არის:

- შეფასების ფარგლების დადგენა.
- საჭირო ინფორმაციის განსაზღვრა.
- შესაფასებელი ობიექტის და მისი ატრიბუტების შერჩევა.
- შეფასების კონსტრუქციების შექმნა და გამოყენება.
- მონაცემთა შეგროვების, ანალიზის პროცესის და ხელსაწყოების ჩამოყალიბება.
- შეფასების მიდგომის დანერგვა და დოკუმენტირება.

შენიშვნა: ორგანიზაციამ უნდა გაითვალისწინოს ფინანსური, ადამიანური და ინფრასტრუქტურული რესურსები.

განვიხილოთ ზემოაღნიშნული გასატარებელი ღონისძიებები.

- **შეფასების ფარგლების დადგენა.** დაწესებულებაში, მისი შესაძლებლობებიდან და რესურსებიდან გამომდინარე, შეფასების ღონისძიებების საწყისი ფარგლები მოიცავს ისეთ ელემენტებს, როგორიც არის კონკრეტული კონტროლი, კონკრეტული კონტროლის მიერ დაცული ინფორმაციული აქტივები, მენეჯმენტის მიერ მინიჭებული უმაღლესი პრიორიტეტის მქონე ინფორმაციული უსაფრთხოების სპეციფიური ღონისძიებები. პირველყოვლისა, შეფასების ფარგლების დადგენისას უნდა დადგინდეს ყველა დაინტერესებული მხარე და მიიღონ მონაწილეობა. დაინტერესებული მხარეები

შეიძლება იყვნენ შიდა ან გარე ორგანიზაციული ერთეულები, მაგალითად, პროექტის მენეჯერები, საინფორმაციო სისტემის მენეჯერები ან ინფორმაციული უსაფრთხოების გადაწყვეტილების მიმღები პირები. ინდივიდუალური კონტროლების ან კონტროლთა ჯგუფის ეფექტიანობის კონკრეტული შეფასების შედეგები უნდა განისაზღვროს და ეცნობოს შესაბამის დაინტერესებულ მხარეებს. შეფასების შედეგებს უნდა მიენიჭოს პრიორიტეტი ინფორმაციის და მასთან დაკავშირებული ინფორმაციული უსაფრთხოების მიზნების მნიშვნელობიდან გამომდინარე.

- **საჭირო ინფორმაციის განსაზღვრა.** ინფორმაციული საჭიროებების განსაზღვრისათვის შესწავლილ უნდა იქნეს ინფორმაციული უსაფრთხოების მართვის სისტემის ისეთი პროცესები, როგორიცაა: იუმს-ის პოლიტიკა და ამოცანები, კონტროლის მიზნები და კონტროლები, იურიდიული, მარეგულირებელი, სახელშეკრულებო და ორგანიზაციული მოთხოვნები ინფორმაციული უსაფრთხოების უზრუნველყოფის კუთხით, ასევ ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის შედეგები. უნდა განხორციელდეს პრიორიტეტებზე დაყრდნობით აღმოჩენილი ინფორმაციული საჭიროებებისადმი პრიორიტეტის მინიჭება. ესენია: რისკის დამუშავების პრიორიტეტები, ორგანიზაციის შესაძლებლობები და რესურსები, დაინტერესებული მხარეების ინტერესები, ინფორმაციული უსაფრთხოების პოლიტიკა, სამართლებრივი, მარეგულირებელი და სახელშეკრულებო მოთხოვნების დასაკმაყოფილებლად საჭირო ინფორმაცია, ინფორმაციის ღირებულება და შეფასების ხარჯები. პრიორიტეტების მინიჭების შემდგომ უნდა მოხდეს შეფასების ღონისძიებებიდან ინფორმაციის ქვესიმრავლის არჩევა. და ბოლოს, დაინტერესებულ მხარეებთან შერჩეული ინფორმაციის აღწერა და შეტყობინება.
- **შესაფასებელი ობიექტის და მისი ატრიბუტების შერჩევა.** შესაფასებელ ობიექტს შესაძლოა რამდენიმე ატრიბუტი გააჩნდეს. შეფასებაში გამოყენებული ობიექტი და მისი ატრიბუტები უნდა შეირჩეს შესაბამისი ინფორმაციული საჭიროებების პრიორიტეტულობის მიხედვით. შერჩეული ატრიბუტების შეფასების მეთოდის გამოყენებით მიიღება ის მნიშვნელობები, რაც ძირითად საზომებს უნდა მიენიჭოს. ეს შერჩევა უზრუნველყოს იმას, რომ ძირითადი საზომი და შესაბამისი შეფასების მეთოდი იდენტიფიცირებადია და მიღებული მნიშვნელობების და შექმნილი საზომების

საფუძველზე, შესაძლებელია შემუშავდეს გონივრული, გამოყენებადი შეფასების შედეგები. შერჩეული ატრიბუტების მახასიათებლები განსაზღვრავს, თუ რა ტიპის შეფასების მეთოდები უნდა იქნას გამოყენებული, რათა ძირითად საზომებს მიენიჭოს მნიშვნელობები, ხარისხობრივი იქნება ეს თუ რაოდენობრივი. შესაფასებელი ობიექტების მაგალითებია:

- პროდუქტები და მომსახურება;
- პროცესები;
- აქტივები, როგორიცაა მოწყობილობები, პროგრამები და საინფორმაციო სისტემები;
- ორგანიზაციული ერთეული;
- გეოგრაფიული მდებარეობა;
- მესამე მხარის მიერ გაწეული მომსახურება;

იმისათვის, რომ შეფასებისათვის შეირჩეს შესაბამისი ატრიბუტი და ეფექტური გაზომვის მიზნით, განისაზღვროს მონაცემთა შესაბამისი რაოდენობა, ატრიბუტი უნდა იყოს განხილული. შერჩევა უნდა მოხდეს ძირითადი საზომის შესაბამისად. თუმცა, ეს არ უნდა ხორციელდებოდეს მხოლოდ ადვილად მოპოვებად მონაცემებზე ან ატრიბუტებზე, მიუხედავად იმისა, რომ ატრიბუტების შერჩევა უნდა ითვალისწინებდეს ატრიბუტების შეფასების სირთულის ხარისხს.

შეფასების კონსტრუქციების შექმნა. ძირითადი საზომების გამოვლენა მჭიდროდ არის დაკავშირებული შესაფასებელი ობიექტების და მათ ატრიბუტების გამოვლენასთან. საზომები განსაზღვრული უნდა იქნას ისე, რომ დაკმაყოფილდეს შერჩეული ინფორმაციული საჭიროება. შერჩეული საზომები უნდა ასახავდეს ინფორმაციული საჭიროების პრიორიტეტს. კრიტერიუმის მაგალითი, რომელიც შეიძლება გამოყენებული იქნას საზომების შერჩევისას, მოიცავს:

- მონაცემების შეგროვების სიმარტივე;
- ადამიანური რესურსების ხელმისაწვდომობა მონაცემთა შესაგროვებლად და სამართავად;
- სათანადო ხელსაწყოების ხელმისაწვდომობა;

- ძირითადი საზომის მიერ უზრუნველყოფილი პოტენციურად შესაბამისი ინდიკატორების რაოდენობა;
- ინტერპრეტაციის სიმარტივე;
- შეფასების შედეგების მომხმარებელთა რაოდენობა;
- საზომის ვარგისიანობის მტკიცებულება მიზნების ან ინფორმაციული საჭიროების დასაკმაყოფილებლად;
- შეგროვების, მართვის და მონაცემთა ანალიზის ხარჯები.

ყოველი ძირითადი საზომისათვის უნდა განისაზღვროს შეფასების მეთოდი, რომელიც ახდენს ობიექტის რაოდენობრივ შეფასებას. ამ დროს ხდება ატრიბუტების გარდაქმნა მნიშვნელობებად, რომლებიც ენიჭება ძირითად საზომებს. შეფასების მეთოდები შეიძლება იყოს სუბიექტური ან ობიექტური. შეფასების მეთოდი ატრიბუტებს გადააქცევს მნიშვნელობებად შესაბამისი შკალის გამოყენებით.

შეფასების კონსტრუქცია სულ ცოტა უნდა შეიცავდეს შემდეგი სახის ინფორმაციას:

- შეფასების მიზანი;
- კონტროლების, კონტროლთა ჯგუფების და იუმს-ის შესაფასებელი პროცესის მისაღწევი
- მიზნები;
- შეფასების ობიექტი;
- შესაგროვებელი და გამოსაყენებელი მონაცემები;
- მონაცემთა შეგროვების და ანალიზის პროცესები;
- შეფასების შედეგების ანგარიშის პროცესი, მათ შორის ანგარიშგების ფორმატები;
- შესაბამისი დაინტერესებული პირების როლები და პასუხისმგებლობები;
- შეფასების მიმოხილვის ციკლი, რომელიც უზრუნველყოფს შეფასების კონსტრუქციების
- გონივრულობას ინფორმაციულ საჭიროებებთან მიმართებაში.

თითოეული წარმოებული საზომისთვის უნდა განისაზღვროს შეფასების ფუნქცია, რათა ძირითადი საზომისთვის მინიჭებული მნიშვნელობები გარდაქმნას წარმოებული საზომის მნიშვნელობებად. შეფასების ფუნქცია შეიძლება მოიცავდეს

სხვადასხვა ტექნიკას, როგორიცაა ძირითადი საზომის ყველა მნიშვნელობის გასაშუალოება, წონების გამოყენება, ან ხარისხობრივი კოეფიციენტების მიყენება. შეფასების ფუნქციას შეუძლია გააერთიანოს ძირითადი საზომების მნიშვნელობები სხვადასხვა შკალების გამოყენებით, როგორებიცაა, მაგალითად პროცენტული ან ხარისხობრივი შეფასების შედეგი.

მონაცემთა შეგროვების, ანალიზის პროცესის და ხელსაწყოების ჩამოყალიბება. მონაცემთა შეგროვების და ანალიზის პროცედურები, აგრეთვე შეფასების შედეგების ანგარიშგების პროცესები მნიშვნელოვანი საფეხურია. უნდა ჩამოყალიბდეს დამხმარე ხელსაწყოები, შეფასების მოწყობილობები და ტექნოლოგიები, რაც ხელს უწყობს ქვემოთ ჩამოთვლილ ქმედებებს:

- <u>მონაცემთა შეგროვება, მათ შორის მონაცემთა შენახვის და შემოწმების საშუალებებს.</u>

  მონაცემთა შეგროვება, შენახვა და შემოწმება მოიცავს შემდეგს:

- დროის თანაბარ მონაკვეთებში მონაცემთა შეგროვება განსაზღვრული შეფასების მეთოდის გამოყენებით;
- მონაცემთა შეგროვების დოკუმენტირება, მათ შორის:
  - მონაცემთა შეგროვების თარიღი, დრო და ადგილმდებარეობა;
  - ინფორმაციის შემგროვებელი;
  - ინფრომაციის მფლობელი;
  - მონაცემთა შეგროვების პროცესში მომხდარი ინციდენტები, რომელიც სასარგებლო შეიძლება იყოს;
  - მონაცემთა შემოწმებისა და შეფასებისათვის საჭირო ინფორმაცია;
- მონაცემთა შერჩევის კრიტერიუმების და შეფასების კონსტრუქციების შემოწმების კრიტერიუმების მიმართ შეგროვებული მონაცემების გადამოწმება. დაგროვილი მონაცემები და ნებისმიერი კონტექსტური ინფორმაცია უნდა გაერთიანდეს და შენახული იქნას მონაცემთა ანალიზისათვის გამოყენებადი სახით.

პროცედურებმა უნდა განსაზღვრონ თუ როგორ უნდა ხდებოდეს მონაცემთა შეგროვება შეფასების მეთოდის, შეფასების ფუნქციის და ანალიტიკური მოდელის მეშვეობით, ისევე როგორც, როგორ და სად უნდა ხდებოდეს მათი შენახვა სხვა

შესაბამის ინფორმაციასთან ერთად, რომელიც აუცილებელია მონაცემთა გასაგებად და შესამოწმებლად. მონაცემთა შემოწმება შესაძლოა შესრულდეს სიის მიხედვით მონაცემთა გადამოწმებით, რომელიც შექმილია მონაცემთა დაკარგვის შემცირების მიზნით და ყოველი საზომისადმი მინიჭებული მნ.იშვნელობის შესამოწმებლად. აქვე უნდა აღინიშნოს, რომ საზომისადმი მინიჭებული მნიშვნელობების შემოწმება მჭიდრო კავშირშია შეფასების მეთოდების დადასტურებასთან.

- შეფასების შედეგების ანალიზსა და ანგარიშგებას. პროცედურემბა უნდა განსაზღვროს მონაცემთა ანალიზის ტექნიკები, სიხშირე, ფორმატი და მეთოდები შეფასების შედეგების აგნარიშგებისათვის. უნდა განისაზღვროს ის საჭირო ხელსაწყოები, რომელიც ახდენს მონაცემთა ანალიზს.

ანგარიშგების ფორმატების მაგალითები შეგვიძლია ასე წარმოვადგინოთ:

- შედეგების ცხრილი, რომელიც გვაძლევს სტრატეგიულ ინფორმაციას მაღალი დონის ინდიკატორების გამოყენებით;
- მენეჯერულ და საოპერაციო ცხრილებს, რომლებიიც ნაკლებადაა ორიენტირებული სტრატეგიულ მიზნებზე და უფრო დაკავშირებულია გარკვეული კონტროლების და პროცესების ეფექტიანობასთან;
- მარტივი და სტატიკური ანგარიშები, მაგალითად: მოცემული დროის მონაკვეთისთვის საზომთა სია, უფრო თანამედროვე ჯვარედინი ანგარიშები ჩაშენებული დაჯგუფებით, ნამატი ჯამი და დინამიური კავშირები. საუკეთესო ანაგრიშები მარტივად უნდა აღიქმებოდეს მომხმარებლის მხრიდან;
- მონაცემთა მაჩვენებელი, რომელიც ასახავს დინამიურ მონაცემებს, მათ შორის შეტყობინებებს, დამატებით გრაფიკულ ელემენტებს და საბოლოო წერტილებს .

შეფასების მიდგომის დანერგვა და დოკუმენტირება.

შეფასების დანერგვის გეგმა უნდა მოიცავდეს მინიმუმ შემდეგს:

- ორგანიზაციაში ინფორმაციული უსაფრთხოების შეფასების პროგრამის დანერგვას;
- შეფასების მახასიათებლებს:
  - ორგანიზაციის შეფასების ზოგადი კონსტრუქცია;

- ორგანიზაციის შეფასების კონკრეტული კონსტრუქციები;
- მონაცემთა შეგროვების და მონაცემთა ანალიზის დიაპაზონისა და პროცედურების განსაზღვრა;

- შეფასების ქმედებების შესრულების გეგმა-გრაფიკი;
- ჩანაწერები, რომელიც შეიქმნება შეფასების შედეგად, მათ შორის დაგროვილი მონაცემები და ანალიზის შესახებ ჩანაწერები;
- მენეჯმენტისათვის და დაინტერესებული მხარეებისათვის შეფასების შედეგების საანგარიშო ფორმატები.

შეფასებისადმი ზოგადი მიდგომა უნდა იყოს დოკუმენტირებული დანერგვის გეგმაში.

თავი 7. მონაცემების ანალიზი და შეფასების შედეგები

დაგროვილი მონაცემები უნდა გაანალიზდეს და მოხდეს მათი გამოყენება გადაწყვეტილების მიღების კრიტერიუმების შესამუშავებლად. შესაძლებელია მონაცემთა აგრეგირება, გარდაქმნა და კოდირების შეცვლა ანალიზის დაწყებამდე. ამ ეტაპზე ხდება მონაცემთა დამუშავება ინდიკატორების მისაღებად. შესაძლოა სხვადასხვა ანალიზის ტექნიკის გამოყენება. ანალიზის სიღრმე უნდა განისაზღვრებოდეს მონაცემების მახასიათებლებით და ინფორმაციული საჭიროებით. შედეგების ანალიტიკოსი, იგივე კომუნიკატორი უნდა აყალიბებდეს გარკვეულ საწყის დასკვნებს შედეგებიდან გამომდინარე. მაგრამ, რადგან კომუნიკატორი შესაძლოა არ იყოს ტექნიკურ და მენეჯერულ პროცესებში ჩართული, ეს დასკვნები უნდა გადაიხედოს დაინტერესებული პირების მიერ. ყველა ინტერპრეტაცია უნდა ითვალისწინებდეს შეფასების კონტექსტს. მონაცემთა ანალიზმა უნდა აღმოაჩინოს დანერგილი იუმს-ის, კონტროლების ან კონტროლთა ჯგუფის ხარვეზები მოსალოდნელ და რეალურ შეფასების შედეგებს შორის. აღმოჩენილი ხარვეზები მიუთითებს დანერგილი იუმს-ის გაუმჯობესების საჭიროებას, მასშტაბის, პოლიტიკების, მიზნების, კონტროლების, პროცესების და პროცედურების ჩათვლით.

იმისათვის, რათა გამოვლინდეს შეუსაბამობა ან არაეფექტიან წარმადობა, უნდა ჩამოყალიბდეს და მოხდეს ინდიკატორების კლასიფიცირება შემდეგნაირად:

- დანერგვა, ფუნქციონირება და კონტროლების ან იუმს-ის პროცესების მართვის რისკების დამუშავების გეგმის ჩავარდნა (მაგ: საფრთხეების მიერ კონტროლების და იუმს-ის პროცესების გვერდის აქცევა)
- რისკების შეფასების წარუმატებლობა:
  - კონტროლები ან იუმს-ის პროცესები არის არაეფექტური, იმიტომ რომ არასაკმარისია მოსალოდნელი საფრთხეებისათვის (მაგ: საფრთხეების მოლოდინის არაჯეროვნად შეფასება) ან ახალი საფრთხეებისათვის წინააღმდეგობის გასაწევად;
  - კონტროლები ან იუმს-ის პროცესები არ დაინერგა აღმოუჩენელი საფრთხეების გამო.

შეფასების შედეგების ანგარიშები დაინტერესებულ მხარეებისთვის უნდა მომზადდეს შესაბამისი ანგარიშგების ფორმატის გამოყენებით, ინფორმაციული უსაფრთხოების შეფასების პროგრამის დანერგვის შესაბამისად. ანალიზის შედეგები განხილული უდნა იქნას შესაბამისი დაინტერესებული მხარეების მიერ მონაცემთა სათანადოდ გაგების მიზნით. მონაცემთა ანალიზის შედეგები უნდა იყოს დოკუმენტირებული დაინტერესებული მხარეების ინფრომირებისათვის.

ის, თუ როგორ მოხდება ინფორმაციული უსაფრთხოების შეფასების შედეგების მიწოდება, ეს უნდა განსაზღვროს ინფრომაციის მიმწოდებელმა. მაგალითად, ისეთი ტიპის ინფორმაცია, როგორიცაა:

- ✓ შეფასების რომელი შედეგების ანგარიში უნდა გავრცელდეს შიგნით ან გარეთ;
- ✓ ყოველი დაინტერესებული მხარის შესაბამისი საზომების სია;
- ✓ შეფასების სპეციფიური შედეგების მიწოდება ყოველი ჯგუფისთვის სპეციფიკურ ფორმატში;
- ✓ დაინტერესებული მხარეებისგან უკუკავშირის მიღების საშუალება, რომელიც გამოიყენება შეფასების შედეგების სარგებლიანობის ხარისხის და ინფორმაციული უსაფრთხოების შეფასების პროგრამის ეფექტიანობის დასადგენად;

<u>შეფასების შედეგები უნდა მიეწოდოს შიდა დაინტერესებულ მხარეებს, მათ შორის:</u>

- შესაფასებელ კლიენტებს
- ინფრომაციის მფლობელებს
- ინფორმაციული უსაფრთხოების რისკების მართვაზე პასუხისმგებელ პერსონალს, განსაკუთრებით სადაც რისკების შეფასების ხარვეზებია აღმოჩენილი;
- გაუმჯობესების საჭიროების მქონე არეებზე პასუხისმგებელ პერსონალს.

დაწესებულებას, ზოგიერთ შემთხვევაში, შეიძლება მოეთხოვებოდეს გარე დაინტერესებული მხარეებისათვისაც ინფორმაციის მიწოდება. სასურველია, რომ გარეთ გამავალი შეფასების ანგარიში შეიცავდეს მხოლოდ გარე მოხმარებისათვის განკუთვნილ მონაცემებს და გამოქვეყნებამდე დასტურდებოდეს მენეჯმენტის და შესაბამისი დაინტერესებული მხარეების მიერ.

დასკვნა

თეორიული მონაცემებისა და ჩატარებული კვლევის საფუძველზე შეიძლება ჩამოვაყალიბოთ შემდეგი:

1. არსებული ცვალებადი და კონკურენტული გარემოს პირობებში, დაწესებულებაში აუცილებელია ინფორმაციული უსაფრთხოების სისტემის დანერგვა, თუცა აქვე უნდა ავღნიშნოთ, რომ პირობები და შესაძლებლობები, რესურსები განსხვავებულია. შესაბამისად, უნდა მოხდეს ყოველივე ზემოაღნიშნულის იდენტიფიცირება და შესაბამისი მიდგომის განსაზღვრა.
2. ინფორმაციული უსაფრთხოების სისტემა შესაბამისობაში უნდა იყოს საკანონმდებლო, მარეგულირებელ მოთხოვნებსა და სახელშეკრულებო ვალდებულებებთან.
3. ინფორმაციული უსაფრთხოების შეფასებისას, მნიშვნელოვანია ის ფაქტორი, რომ შეფასებისათვის საჭირო მონაცემები იყოს ადვილად მოსაპოვებელი.
4. ინფორმაციული უსაფრთხოების სისტემის დანერგვაში უმნიშვნელოვანესია მენეჯმენტის როლი, ხოლო რაც შეეხება პასუხისმგებლობას, ის უნდა განისაზღვროს ყველა დონეზე.
5. დაწესებულებამ დროის გარკვეულ ინტერვალში უნდა შეაფასოს დანერგილი ინფორმაციული უსაფრთხოების შეფასების პროგრამის ეფექტიანობა იმისათვის, რომ დარწმუნდეს, რამდენად ეფექტურია შეფასების შედეგები, რამდენად სრულდება გეგმა, უნდა დარწმუნდეს ასევე, გარემოს ცვლილებების (მაგ. მოთხოვნები, კანონმდებლობა, ან ტექნოლოგია) გათვალისწინების უზრუნველყოფაში. მან ასევე, უნდა შეაფასოს მიღებული შეფასების შედეგების გამოყენებადობა შესაბამისი ინფორმაციული საჭიროებების უზრუნველსაყოფად.
6. დაწესებულების მიზნების გათვალისწინებით, ინფორმაციული უსაფრთხოების შეფასების პროგრამის ეფექტიანობის შეფასების კრიტერიუმები უნდა განისაზღვროს ინფორმაციული უსაფრთხოების შეფასების პროგრამის დანერგვის დასაწყისში.

7. დაწესებულებამ უნდა აწარმოოს თავისი ინფორმაციული უსაფრთხოების შეფასების პროგრამის ზედამხედველობა, უნდა გამოავლინოს ინფომაციული უსაფრთხოების შეფასების პროგრამის გაუმჯობესების პოტენციური საჭიროებები, როგორიცაა: გამოუსადეგარი შეფასების კონსტრუქციების გადახედვა-ამოღება და ინფორმაციული უსაფრთხოების შეფასების პროგრამისათვის რესურსების გადანაწილება.
8. დაწესებულებამ უნდა უზრუნველყოს შესაბამისი დაინტერესებული მხარეების მიერ საჭირო გაუმჯობესებების გამოვლენა ინფორმაციული უსაფრთხოების შეფასების პროგრამის ფარგლებში. გამოვლენილი გაუმჯობესებები, რათქმაუნდა, უნდა დადასტურდეს მენეჯმენტის მიერ. დამტკიცებული გეგმა უნდა იყოს დოკუმენტირებული და მიეწოდოს შესაბამის დაინტერესებულ მხარეებს. ორგანიზაციამ უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების შეფასების პროგრამის დამტკიცებული გაუმჯობესებების გეგმიური დანერგვა.
9. უმაღლესი საგანმანათლებლო სფეროს სპეციფიკის გათვალისწინებით, შემუშავებული იქნა სპეციალური კითხვარი, რომელიც გამოავლენს თბილისის სახელმწიფო უნივერსიტეტში არსებული ინფორმაციული უსაფრთხოების დონეს და გამოვლინდება რამდენად საჭიროებს, უნივერსიტეტის მიზნებიდან გამომდინარე, არსებული სისტემა ცვლილების განხორციელებას. თუ საჭიროებს, რამდენად არსებობს ამის რესურსი და თუ არა, მაშინ რა შეიძლება იყოს ალტერნატიული გზა. გადაწყვეტილების მიღების კრიტერიუმები იქნება:
    - ✓ წითელი - ჩარევა აუცილებელია, უნდა ჩატარდეს გამომწვევი მიზეზების ანალიზი, რათა დადგინდეს შეუსაბამობისა და არაჯეროვნად შესრულების მიზეზები.
    - ✓ ყვითელი - ინდიკატორზე უნდა განხორციელდეს დაკვირვება, რათა არ გადაიზარდოს წითელში.
    - ✓ მწვანე - არანაირი ქმედება არაა საჭირო

    (იხ.დანართი - Excel ფაილი)

გამოყენებული ლიტერატურა

1. ISO/IEC 27001 – INFORMATION SECURITY MANAGEMENT
2. NIST 800-39 – MANAGIN INFORMATION SECURITY RISK
3. COSO – RISK ASSESSMENT IN PRACTISE
4. ISO/IEC 27005: 2008 – INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - INFORMATION SECURITY RISK MANAGEMENT
5. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - SPECIAL PUBLICATION 800-39 – MANAGIN INFORMATION SECURITY RISK
6. SANS INSTITUTE – INFOSEC READING ROOM - INFORMATION RISK & RISK MANAGEMENT.