ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

ვაჟა ჩალაური

ინფორმაციული უსაფრთხოების ანალიზი უმაღლეს საგანმანათლებლო სფეროში

ანალიზის შედეგები

ნაშრომი მაგისტრის ხარისხის მოსაპოვებლად

ხელმძღვანელი: ფიზ.მათ.კანდ: დავით ხაჩიძე

დავით აღნიაშვილი

ანოტაცია

ინფორმაციული ტექნოლოგიების განვითარების დონემ ხელი შეუწყო მის ყოველდღიურ გამოყენებადობას პირად ცხოვრებასა თუ სამუშაო გარემოში. ამასთან ერთად იმატა ინფორმაციაზე ხელმისაწვდომობამ. ინფორმაცია თანდათანობით გადავიდა ქაღალდიდან ელექტრონულ ფორმატში და საჭირო გახდა მისი სათანადოდ დაცვა.

ნაშრომში აღწერილია ყველა ის პრინციპები და მეთოდები რომელთა მიზანია ინფორმაციული უსაფრთხოების დონის განსაზღვრა, ანალიზი და გაუმჯობესება. ეს მეთოდები ძირითადად დაფუძნებულია ISO/IEC 27001 სტანდატზე.

ყველა დაწესებულება, ისევე როგორც უმაღლესი საგანმანათლებლო დგანან ისეთი საფრთხის წინაშე როგორიცაა ინფორმაციის არასანქცირებული გაჟონვა, ჰაკერული შეტევები, ფორსმაჟორული სიტუაციები და სხვა. აქედან გამომდინარე აუცილებელია ინფორმაციული უსაფრთხოების მაღალი დონის არსებობა რაც მოიცავს მთელ რიგ პროცესებს: რისკების შეფასებას, პასუხისმგებლობების გადანაწილებას, გასატარებელ აქტივებს, პერიოდულად ამ ციკლის გამეორებას და ა.შ. სწორედ ამიტომ საჭიროა საუნივერსიტეტო პროცესების მართვის სისტემის გაუმჯობესება უმაღლეს სასწავლო დაწესებულებებშიც.

კვლევის ობიექტისთვის შეირჩა თბილისის ივ. ჯავახიშვილის სახელობის სახელმწიფო უნივერსიტეტი. კვლევის ძირითად მიზანს წარმოადგენს თსუ-ში ინფორმაციული უსაფრთხოების მართვის სპეციალური სტრუქტურის მოდელის დანერგვა.

კვლევისა და ანალიზის ძირითად კომპონენტებს იყო რისკების შეფასება, მართვა და მისი ანალიზი. რისკი არის იმ შედეგის დადგომის ალბათობა, რომელიც წარმოადგენს გადახრას დაგეგმილი/მოსალოდნელი შედეგიდან და უარყოფითად მოქმედებს დაწესებულების მიზნების მიღწევაზე. ხოლო რისკის მართვა

წარმოადგენს ერთიან, უწყვეტ და განვითარებად პროცესს, რომელშიც თავისი უფლებამოსილების ფარგლებში მონაწილეობას იღებს დაწესებულების თითოეული თანამშრომელი. რაც შეეხება რისკის ანალიზს იგი შეიძლება განხორციელდეს სხვადასხვა გზით, თუმცა იგი ძირითადად კლასიფიცირდება შემდეგნაირად: 1.რაოდენობრივი. 2.ხარისხობრივი. 3კომბინირებული.

ნებისმიერი ეს რისკი ეკუთვნის აქტივს ან აქტივთა ჯგუფს რომელზეც პასუხისმგებელია ერთი ან რამოდენიმე პიროვნება. აქტივი არის ნებისმიერი რამ, რაც ფასეულია ორგანიზაციისთვის და ამდენად მოითხოვს დაცვას. აქტივების იდენტიფიცირებისათვის უნდა გვახსოვდეს, რომ ინფორმაციული სისტემა არ შედგება მხოლოდ აპარატურისა და კომპიუტერული პროგრამებისგან.

Annotation

IT development level has contributed to its applicability in everyday life and in his work environment . In addition, the increased availability of information . Information gradually moved from paper to electronic format and had to be properly protected .

The paper describes the principles and methods aimed at determining the level of information security , analysis and improvement . These methods are based on ISO / IEC 27001 standards for .

All of the facility , as well as higher education are facing the threat of such an unauthorized leak of information , hacking, and other emergency situations . It is therefore necessary to include a number of high-level information security processes : risk assessment , distribution of responsibilities , to be taken assets , periodically repeating this cycle , etc. That is why it is necessary to improve the university management system of higher education institutions .

Iv been selected for the research facility . Javakhishvili State University . The main objective of the TSU special structure model of information security management .

Research and analysis of the main components of the risk assessment , management, and analysis . The risk is the likelihood of the outcome , which represents the deviation of the planned / expected result and a negative impact on the institution's goals .

While risk management is a single , continuous and developing process , which takes part in the establishment of each employee within its authority . As for the risk analysis it can be implemented in different ways , but it is mainly classified as follows : 1.raodenobrivi . 2.khariskhobrivi . 3 combined .

It belongs to the risk of any asset or group of assets which is responsible for one or several persons . Asset is anything that has value to the organization and therefore requires protection . Identify the assets to remember that the information system does not only consist of hardware and computer programs .

სარჩევი

1. შესავალი

აღნიშნული დოკუმენტი წარმოადგენს სახელმძღვანელოს ინფორმაციული უსაფრთხოების გაუმჯობესებას უმაღლეს საგანმანათლებლო სფეროში და ძირითადად ემყარება ISO/IEC 27001 სტანდარტში აღწერილ პრინციპებს, რომლებიც მიზნად ისახავენ დაწესებულებასა თუ ორგანიზაციაში უსაფრთხოების დონის განსაზღვრას, ანალიზსა და გაუმჯობესებას. აღწერილი მეთოდები მორგებადია ყველა ტიპის ორგანიზაციისთვის (მაგ. კომერციული საწარმოები, სახელმწიფო უწყებები, არასამთავრობო ორგანიზაციები და სხვა.), რომლებიც გეგმავენ იმ რისკების მართვას, რომლებმაც შეიძლება მოახდინონ ორგანიზაციის ინფორმაციული უსაფრთხოების კომპრომენტირება.

ინფორმაციული ტექნოლოგიების განვითარების დონემ ხელი შეუწყო მის ყოველდღიურ გამოყენებადობას პირად ცხოვრებასა თუ სამუშაო გარემოში. ამასთან ერთად იმატა ინფორმაციაზე ხელმისაწვდომობამ. ინფორმაცია თანდათანობით გადავიდა ქაღალდიდან ელექტრონულ ფორმატში და საჭირო გახდა მისი სათანადოდ დაცვა.

დღესდღეისობით ინფორმაციული სისტემები საგანმანათლებლო სტრუქტურის განუყოფელი ნაწილია. მისი წარმატებული მუშაობა დიდ ზეგავლენას ახდენს უნივერსიტეტის იმიჯსა, სასწავლო პროცესსა თუ მის რეპუტაციაზე. ორგანიზაცია ვალდებულია დაიცვას და სათანადოდ მართოს მის მფლობელობაში არსებული ინფორმაცია თუ აქტივები.

ინფორმაცია წარმოადგენს აქტივს, რომელსაც მსგავსად ორგანიზაციის სხვა ბიზნეს მნიშვნელობის მქონე აქტივებისა, გააჩნია სასიცოცხლო მნიშვნელობა ორგანიზაციის ბიზნეს საქმიანობისთვის და იგი შეიძლება წარმოდგენილ იქნას სხვადასხვა ფორმით: ინფორმაცია შეიძლება იყოს ბეჭდვითი, დაწერილი ფურცელზე, შენახული ელექტრონულად, გადაცემული ვერბალურად და ა.შ.

ძირითადად ინფორმაცია მიიღება, ინახება, მუშავდება და გადაიცემა ინტენსიურ-ტექნოლოგიური საინფორმაციაო სისტემების საშუალებით, როგორებიცაა: პერსონალური და სუპერ კომპიუტერები, მობილური მოყობილობები, სატელეკომუნიკაციო სისტემები და სხვა. ორგანიზაციები პირდაპირ დამოკიდებულნი არიან აღნიშნულ ტექნოლოგიებზე, რომლებიც უზრუნველყოფენ ბიზნეს ფუნქციისა და მისიის წარმატებით განხორციელებას.

ინფორმაციულ სისტემებზე ზეგავლენას ახდენს სხვადასხვა ტიპის სერიოზული საფრთხე, რომლებმაც შეიძლება უარყოფითი ზეგავლენა მოახდინონ ორგანიზაციის საოპერაციო გარემოზე (მაგ. მისია, ფუნქცია, იმიჯი და/ან რეპუტაცია), ორგანიზაციის აქტივებსა თუ ინდივიდებზე სხვადასხვა ფართოდ გავრცელებული სისუსტეების გამოყენებით, რომლებიც არღვევენ აღნიშნულ ინფორმაციულ სისტემებში მიღებული, შენახული, დამუშავებული თუ გადაცემული ინფორმაციის კონფიდენციალურობას, მთლიანობასა თუ ხელმისაწვდომობას. ინფორმაციული სისტემების საფრთხეებს მიეკუთვნება: მიზანმიმართული შეტევები, გარემოსდაცვითი ხასიათის დარღვევები, ადამიანური / მანქანური შეცდომები და სხვა, რომლებიც საბოლოოდ დიდ ან საერთოდ გამოუსწორებელ ზიანს აყენებენ ორგანიზაციას.

ინფორმაციული უსაფრთხოების რისკი ნიშნავს, რომ პოტენციური საფრთხე, არსებული სისუსტეების გამოყენებით, ზიანს მიაყენებს აქტივს ან აქტივთა ჯგუფს და საბოლოოდ მთლიანად ორგანიზაციას.

ორგანიზაციაში შეიძლება არსებობდეს მრავალი სახის რისკი: საინვესტიციო, ბიუჯეტური, სამართლებრივი და სხვა. ინფორმაციული უსაფრთხოების რისკი წარმოადგენს ორგანიზაციაში არსებული რისკების ერთ-ერთ კომპონენტს, რომლის მართვასაც გააჩნია არსებითი მნიშვნელობა.

დადგენილია რომ ინფორმაციული უსაფრთხოების სტანდარტების ძირითადი ნაწილი მიღებულია საუკეთესო გამოცდილების პრაქტიკიდან(best practice) ამიტომაც მისი კონკრეტული საზომი ეტალონი არ არსებობს. არსებობს მრავალი სახის სტანდარტი და სრულ უსაფრთხოებას ვერც ერთი სტანდარტი ვერ უზრუნველყოფს თუმცა მათი გამოყენებით მნიშვნელოვნად უმჯობესდება უსაფრთხოების დონე. სწორედ ამიტომ ეს სფერო დღესდღეისობითაც განვითარების გზაზე დგას.

ინფორმაციული უსაფრთხოება საქართველოში დანერგილია ძირითადად მსხვილ კომპანიებში რომელთა დანაკარგმაც შეიძლება ათეულობით მილიონსაც კი გადააჭარბოს. მეორეს მხრივ მსხვილი კომპანიები ავალდებულებენ მის დაქვემდებარებაში მყოფ ორგანიზაციებს გაიზიარონ მათი პოლიტიკა. გარდა ამისა საჯარო სამსახურების დიდ ნაწილს კანონი პირდაპირ ავალდებულებს დანერგოს კონკრეტული სტანდარტი, ხოლო დანარჩენ კომპანიებსა, ორგანიზაციებსა თუ სასწავლო, საგანმანათლებლო სტრუქტურებში ინფორმაციული უსაფრთხოება არ არის დანერგილი.

საერთო ჯამში, ჩვენ ვცხოვრობთ და ვმუშაობთ ისეთ მსოფლიოში, სადაც საზოგადოებისთვის და გარემოსთვის რისკი ჩვეული რამაა. ერთის მხრივ, არ არსებობს ცნება 100% უსაფრთხო და შესაბამისად არ შეგვიძლია ვიყოთ თვითდაჯერებულნი: „მე ეს არასდროს დამემართება“. მეორეს მხრივ, გაუმართლებელია თუ ვიცხოვრებთ მუდმივი შიშით. ჩვენ უნდა შეგვეძლოს დაბალანსებული და გონივრული ზომების მიღება, ფასეული აქტივების დასაცავად. ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი ებრძვის გაურკვეველი და მოულოდნელი საფრთხეების წარმოქმნისგან, რაც გვეხმარება ვმართოთ, ვაკონტროლოთ და დავიცვათ ორგანიზაცია შესაძლო საფრთხეებისგან.

2. აქტუალურობა

უმაღლესი სასწავლებლების განვითარებამ და გამრავლებამ წარმოშვა კონკურენცია მომსახურების ხარისხზე. განათლების მიღების დონე ყველაზე მნიშვნელოვანი კონპონენტია საგანმანათლებლო სფეროში. განათლების მიღების ხარისხი პირდაპირპროპორციულადაა დამოკიდებული ამავე ორგანიზაციის რესურსების ეფექტურ მართვასთან. ინფორმაციულ ტექნოლოგიებს ერთ-ერთი წამყვანი როლი აკისრია სასწავლო პროცესების მართვაში.
მისი გამართული მუშაობა პირდაპირ აისახება მიღებულ განათლებასა და უნივერსიტეტის რეპუტაციაზე.

ორგანიზაციას გააჩნია უამრავი აქტივი და აქედან ყველაზე მნიშვნელოვანია ინფორმაცია. მას შესაბამისი გაფრთხილება და დაცვა სჭირდება. ინფორმაცია შეიძლება მრავალი ფორმით იყოს წარმოდგენილი, მაგალითად: დოკუმენტირებული, ელექტრონულ ფორმატში წარმოდგენილი, ვიდეო რგოლით გადმოცემული ანდა საუბრისას გავრცელებული. როგორი სტრუქტურაც არ უნდა ქონდეს მას, უნდა ხდებოდეს მისი სათანადოდ დაცვა.

ყველა დაწესებულება, ისევე როგორც უმაღლესი საგანმანათლებლო დგანან ისეთი საფრთხის წინაშე როგორიცაა ინფორმაციის არასანქცირებული გაჟონვა, ჰაკერული შეტევები, ფორსმაჟორული სიტუაციები და სხვა. აქედან გამომდინარე აუცილებელია ინფორმაციული უსაფრთხოების მაღალი დონის არსებობა რაც მოიცავს მთელ რიგ პროცესებს: რისკების შეფასებას, პასუხისმგებლობების გადანაწილებას, გასატარებელ აქტივებს, პერიოდულად ამ ციკლის გამეორებას და ა.შ.

ინფორმაციული უსაფრთხოების რისკების მართვა უნდა იყოს უწყვეტი პროცესი. პროცესმა უნდა დაადგინოს ორგანიზაციული გარემო, შეაფასოს რისკები და გადაჭრას რისკები რისკებთან მობყრობის გეგმის მიხედვით რეკომენდაციების და გადაწყვეტილებების დასანერგად. რისკების დასაშვებ დონეზე დაყვანისათვის რისკების მართვა აანალიზებს რეაგირების არქონის შემთხვევაში შესაძლო უარყოფით მოვლენებს და განსაზღვრავს სამოქმედო გეგმას.

ინფორმაციული უსაფრთხოების რისკების მართვამ ხელი უნდა შეუწყოს:

- რისკების იდენტიფიცირებას;
- რისკების შეფასებას იმისდა მიხედვით, თუ რა შედეგები მოყვება მათ ბიზნესთან მიმართებაში და მათი ხდომილების ალბათობა;
- ამ რისკების დადგომის ალბათობას და მათ შესაძლო შედეგებს, მათ შესახებ ინფორმირებულობის არსებობას;
- რისკებთან მობყრობის პრიორიტეტულობის დადგენას;
- რისკების შემცირების შესახებ ქმედებების პრიორიტეტულობას;
- რისკების მართვასთან დაკავშირებული გადაწყვეტილებების მიღებაში ჩართული დაინტერესებული პირები და მათი ინფორმირებულობა რისკების მართვის სტატუსის შესახებ;
- რისკებთან მობყრობის მონიტორინგის ეფექტიანობას;
- რისკებისა და რისკების მართვის პროცესის რეგულარულ მონიტორინგსა და განხილვას;
- რისკების მართვისადმი მიდგომის გაუმჯობესების მიზნით საჭირო ინფორმაციის შეგროვებას;
- მენეჯერებისა და თანამშრომლების ინფორმირებულობას რისკებისა და მათი შემცირების შესახებ.

ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი შესაძლოა მიესადაგოს მთლიან ორგანიზაციას, ან მის ცალკეულ ნაწილს (მაგალითად: დეპარატმენტს, ფიზიკურ მდებარეობას, სერვისს), ნებისმიერ ინფორმაციულ სისტემას, კონტროლის მექანიზმების არსებულ ან დაგეგმილ ან სპეციფიკურ ასპექტებს (მაგალითად: ბიზნესის უწყვეტობის დაგეგმვა).

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

სამაგისტრო ნაშრომში დასახული ძირითადი მიზნის მიღწევისათვის გადაწყვეტილია შემდეგი ამოცანები:

1. ინფორმაციული უსაფრთხოების რისკების ანალიზი.
2. რისკების შეფასება
3. რისკის მართვა
4. პასუხისმგებლობების განაწილება
5. ინციდენტის ალბათობის შეფასება
6. გასატარებელი აქტივები უსაფრთხოების დონის გასაუმჯობესებლად
7. უსაფრთხოების ხანდაზმულობა
8. რეკომენდაციები და მისი ანალიზი

4.კვლევის ობიექტი. კვლევის ობიექტს წარმოადგენს თბილისის სახელმწიფო უნივერსიტეტში საუნივერსიტეტო პროცესების მართვის ავტომატიზებული სისტემა და მისი უსაფრთხოების დონის ანალიზის შედეგები. ანალიზი ჩაუტარდა თსუ-ს საგანმანათლებლო სტრუქტურას და შედეგები მოცემულია დანართი 1-ის სახით. სწორედ ამაზე დაყრდნობით დადგინდა კრიტიკული ადგილები და პრიორიტეტები რომელნიც საჭიროებენ გამოსწორებას მოკლე პერიოდში. ამიტომაც შევადგინეთ რეკომენდაციები რომლის გათვალისწინებითაც უნივერსიტეტი შეძლებს გააუმჯობესოს უსაფრთხოების დონე. ეს ასევე ხელს შეუწყობს უფრო ნათლად და კონკრეტულად გამოიკვეთოს ტექნიკური თუ პროგრამული ხარვეზები.

ასევე ძალიან მოქნილია მონიტორინგის თვალსაზრისით და ქმნის გარემოს რომელიც შეძლებს გამოკვეთოს სისტემაში არსებული სუსტი წერტილები. (თსუ-ს რეკომენდაციები და სამოქმედო გეგმა მოცემულია დანართი 2 სახით.)

5. 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. ერთადერთ მინუსად რაც შეიძლება ჩაითვალოს ამ მოდელის არის ის რომ პასუხისმგებლობის არეალი გაეზრდებათ თანამშრომლებსა თუ იმ პირებს რომელნიც პირდაპირ არიან დაკავშირებული უნივერსიტეტის სტრუქტურასა და სასწავლო პროცესებთან, მაგრამ ეს არაფრადაც შეიძლება ჩაითვალოს იმ დადებით მხარეებთან მიმართებაში რასაც ეს მოდელი მოუტანს სასწავლო გარემოს. დადებითი მხარეებია:

1. მინიმალური დანახარჯი.
2. პასუხისმგებლობების დადგენა
3. მონიტორინგის დაგეგმვა-გაუმჯობესება
4. ხარვეზებისა და ინციდენტების მკვეთრი შემცირება
5. ფორსმაჟორულ სიტუაციაში სამოქმედო გეგმა
6. ინციდენტების გადაჭრის ოპტიმალური გეგმა
7. ინფორმაციის დაკარგვის თავიდან აცილება
8. რეპუტაციის ამაღლება
9. საერთაშორისო სტანდარტებთან მიახლოება-დაკმაყოფილება
10. სამუშაო გარემოს გაუმჯობესება და სხვა.

6.ინფორმაციული უსაფრთხოების რისკების შეფასება

რისკი არის იმ შედეგის დადგომის ალბათობა, რომელიც წარმოადგენს გადახრას დაგეგმილი/მოსალოდნელი შედეგიდან და უარყოფითად მოქმედებს დაწესებულების მიზნების მიღწევაზე.

რისკი განისაზღვრება შემდეგი მახასიათებლების კომბინაციით:

ა) მოხდენის ალბათობა;

ბ) გავლენა (მოხდენის შემთხვევაში).

- მოხდენის ალბათობა არის კონკრეტული შედეგის დადგომის შესაძლებლობა, სადაც გასათვალისწინებელია შედეგის დადგომის სიხშირე.
- გავლენა არის მიღებული ეფექტი კონკრეტული შედეგის დადგომის შემთხვევაში. გავლენა ითვალისწინებს ოთხ ელემენტს:

o დრო

o ხარისხი

o სარგებელი

o ადამიანური და სხვა რესურსები

მოხდენის ალბათობისა და გავლენის კომბინაცია განსაზღვრავს კონკრეტული რისკის მნიშვნელობის დონეს და დაწესებულების მიზნებიდან გამომდინარე იძლევა პრიორიტეტების მიხედვით, რისკის დახარისხების საშუალებას. პირველ რიგში, უნდა განიხილებოდეს და იმართებოდეს რისკები, რომელთა მოხდენის ალბათობა და გავლენა ყველაზე მაღალია. რიგითობით ყოველი შემდეგი უნდა იყოს რისკი ნაკლები მოხდენის ალბათობითა და გავლენით. პრაქტიკაში ეს პროცესი გაცილებით რთულია, რადგან არსებობენ რისკები, რომელთა მოხდენის ალბათობა არის მაღალი, მაგრამ დაბალია გავლენა და/ან პირიქით. ასეთ შემთხვევებში უნდა განხორციელდეს რისკების პრიორიტეტებად დალაგება დაწესებულების მიზნებისა და ამოცანებიდან გამომდინარე, რათა არ მოხდეს შეცდომის დაშვება

ალბათობა	მაღალი	პრიორიტეტულია
გავლენა	მაღალი	
ალბათობა	მაღალი	რიგითობის განსაზღვრა უნდა მოხდეს დაწესებულების მიზნებიდან
გავლენა	დაბალი	და სტრატეგიიდან გამომდინარე
ალბათობა	დაბალი	რიგითობის განსაზღვრა უნდა მოხდეს დაწესებულების მიზნებიდან
გავლენა	მაღალი	და სტრატეგიიდან გამომდინარე
ალბათობა	დაბალი	ნაკლებად პრიორიტეტულია
გავლენა	დაბალი	

7. რისკის მართვა

რისკის მართვა წარმოადგენს რისკის განსაზღვრის, შეფასების, მონიტორინგის და რისკის მისაღებ დონეზე შენარჩუნების მიზნით საჭირო კონტროლის ღონისძიებების გატარების პროცესს, რომელიც გავლენას ახდენს დაწესებულების მიზნებისა და ამოცანების მიღწევაზე და გულისხმობს საჭირო ღონისძიებების განხორციელებას რისკის შემცირების მიზნით.

რისკის მართვა წარმოადგენს ერთიან, უწყვეტ და განვითარებად პროცესს, რომელშიც თავისი უფლებამოსილების ფარგლებში მონაწილეობას იღებს დაწესებულების თითოეული თანამშრომელი.

რისკის მართვა წარმოადგნეს დაწესებულების სტრატეგიული მართვის ერთ-ერთ მნიშვნელოვან კომპონენტს. რისკის მართვის მთავარი ამოცანაა მოახდინოს რისკების იდენტიფიკაცია და საპასუხო ღონისძიებების გატარება.

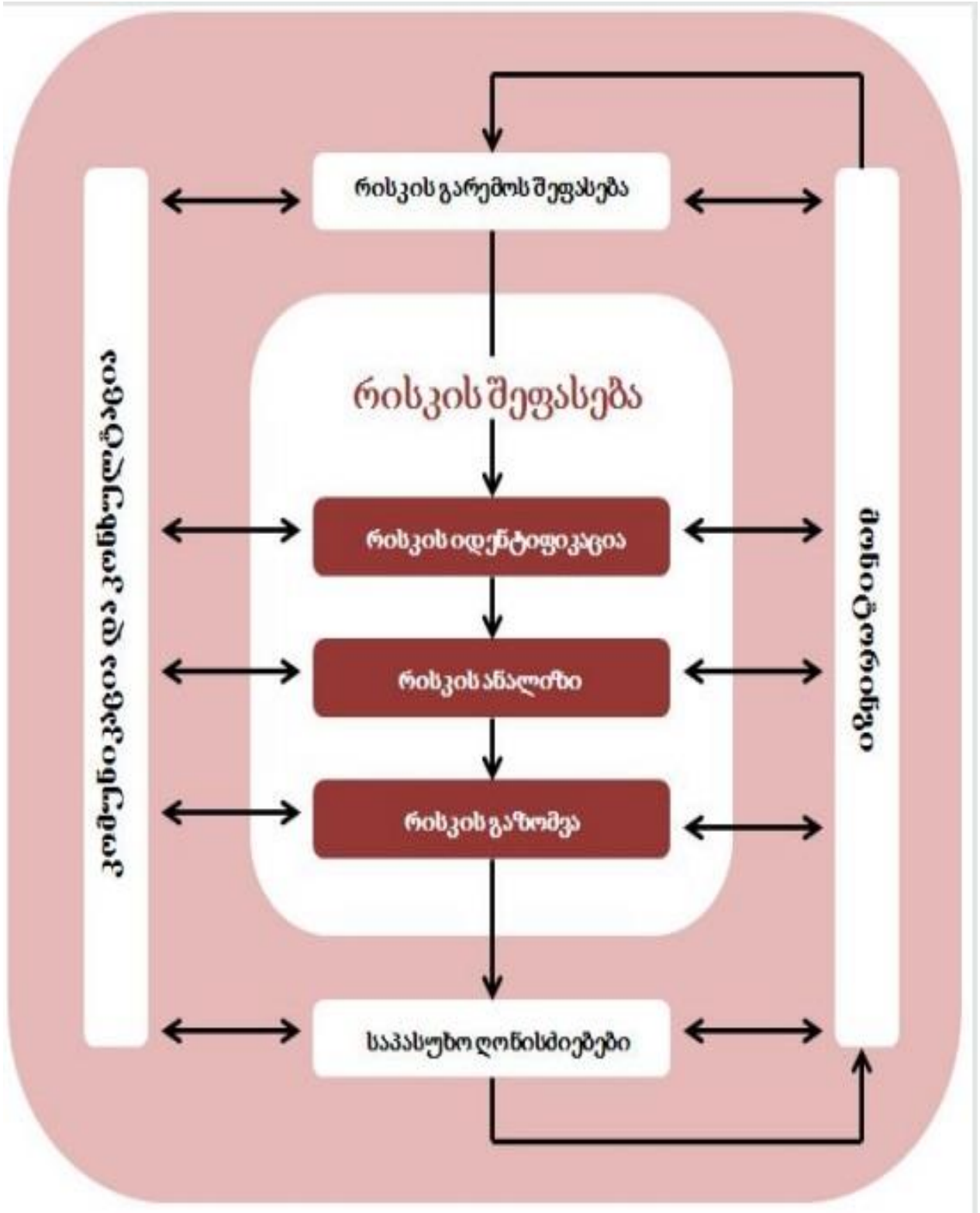
რისკის მართვის საშუალებით შესაძლებელია გამოვლენილ იქნეს პოტენციური დადებითი, თუ უარყოფითი ფაქტორები, რაც გავლენას ახდენს დაწესებულების საქმიანობაზე.რისკის მართვა მოიცავს პრაქტიკულად ყველა რისკს, რომელიც ეხება დაწესებულების საქმიანობას წარსულში, აწმყოსა და მომავალში.

ხელმძღვანელობა უზრუნველყოფს დაწესებულებაში რისკის მართვის გამართული სისტემის ჩამოყალიბებას და ფუნქციონირებას, ხოლო დაწესებულებაში შექმნილი შიდა აუდიტის სუბიექტის მოვალეობაა არსებული რისკის მართვის სისტემის შეფასება და მის გასაუმჯობესებლად შესაბამისი რეკომენდაციების გაცემა.

რისკის მართვა უნდა ატარებდეს პერმანენტულ ხასიათს და ხორციელდებოდეს დაწესებულების ხელმძღვანელის მიერ ყოველწლიურად დამტკიცებული რისკის მართვის სტრატეგიის შესაბამისად. რისკის მართვა ეხმარება და აძლიერებს დაწესებულებას, უზრუნველყოფს რა მისი ამოცანების ეფექტურად შესრულებას, მათ შორის:

- დაწესებულების ზოგადი მიმართულებების ჩამოყალიბებას, რომელიც საშუალებას იძლევა მომავალი საქმიანობა გამართული და კონტროლირებადი ფორმით წარიმართოს;
- რიგი პროცესების გაუმჯობესებას - გადაწყვეტილების მიღება, დაგეგმვა და პრიორიტეტების მინიჭება;
- დაწესებულებაში არსებული ქონებისა და რესურსების პროდუქტიული განაწილებისა და გამოყენების ხელშეწყობას;
- დაწესებულების რეპუტაციისა და აქტივების დაცვას და გაძლიერებას;
- ადამიანური რესურსებისა და ინსტიტუციონალური ცოდნის ბაზის განვითარებას და გაძლიერებას;
- ოპერაციების ოპტიმიზაციას და სხვ.

რისკის მართვის პროცესი არის კოორდინირებული და თანმიმდევრული უწყვეტი ქმედებების ერთობლიობა. მისი შემადგენელი ცალკეული ნაწილები დამოკიდებულია დაწესებულების სპეციფიკაზე, მის მიზნებსა და სტრატეგიაზე, თუმცა რისკის მართვის პროცესის ზოგადი სტრუქტურა ყველა დაწესებულებაში იდენტურია


რისკის გარემოს შეფასება
რისკის შეფასება
რისკის იდენტიფიკაცია
რისკის ანალიზი
რისკის გაზომვა
საპასუხო ღონისძიებები
კომუნიკაცია და კონსულტაცია
მონიტორინგი

8.რისკის ანალიზი

რისკის ანალიზი ხორციელდება იდენტიფიცირებული რისკების ალბათობისა და გავლენის შესწავლის მიხედვით, რათა განისაზღვროს, თუ როგორ უნდა იმართონ ისინი. შედეგად, რისკის ანალიზი გულისხმობს იმ ფაქტორების იდენტიფიკაციას, რომლებმაც შეიძლება გავლენა მოახდინონ რისკის მოხდენის ალბათობაზე და შედეგებზე.

საწყის ეტაპზე ხორციელდება წინასწარი ანალიზი, რომელიც გულისხმობს მსგავსი რისკების დაჯგუფებას, გაერთიანებას და დაბალი გავლენის მქონე რისკების გამორიცხვას (აღსანიშნავია, რომ გამორიცხვა არ გულისხმობს უგულებელყოფას, ვინაიდან მათი აღრიცხვა განხორციელდა რისკების იდენტიფიკაციის ეტაპზე.).

შემდეგი ეტაპია რისკის დონის განსაზღვრა მისი მასშტაბებიდან გამომდინარე. რისკის დონის განსაზღვრა ხდება არა მარტო რისკის მოხდენის ალბათობისა და გავლენის შესწავლით, არამედ ასევე ხდება რისკების ურთიერთდამოკიდებულებებისა და სხვა ფაქტორების გათვალისწინება.

რისკის დონე შესაძლებელია მისაღები იყოს დაწესებულებისთვის და მას რისკის მადა ეწოდება. შესაძლებელია ასევე მოხდეს არა რომელიმე კონკრეტული რისკის არამედ კომბინირებული რისკების განსაზღვრა.

რისკის ანალიზი შეიძლება განხორციელდეს სხვადასხვა გზით, რაც დამოკიდებულია კონკრეტულ რისკზე, ანალიზის მიზანზე, ხელმისაწვდომ ინფორმაციაზე, მონაცემებზე, რესურსებზე და სხვ.

რისკის ანალიზი შეიძლება იყოს:

- რაოდენობრივი
- ხარისხობრივი
- კომბინირებული

8.1 რაოდენობრივი ანალიზი

იმ შემთხვევაში როდესაც არსებობს რაოდენობრივი მონაცემები რისკის მოხდენის ალბათობის და გავლენის შესახებ, მაშინ საუკეთესო გზას წარმოადგენს რისკის რაოდენობრივი ანალიზის განხორციელება. არარაოდენობრივი შეფასება ნაკლებად

საიმედოა, განსაკუთრებით რისკის მოხდენის ალბათობის შეფასებისას.

რაოდენობრივი ანალიზის დროს შესაძლოა, გამოყენებული იქნას შემდეგი მეთოდები:

- ალბათობის ანალიზი
- გავლენის ანალიზი
- კომპიუტერული მოდელირება
- სტატისტიკური ანალიზი და სხვ.

8.2 ხარისხობრივი ანალიზი

ხარისხორივი ანალიზი ფართოდ არის გავრცელებული სახელმწიფო სექტორში, სადაც ანგარიშვალდებულების და საზოგადოებაზე გავლენის შედეგი მეტად მნიშვნელოვანია, რაც ხშირ შემთხვევაში შეუძლებელს, ან მეტად ხარჯიანს ხდის რისკების რაოდენობრივი სახით გამოსახვას. ასეთი ანალიზი ეყრდნობა სუბიექტურ შეფასებას და ასეთ დროს გადაწყვეტილებები მიიღება ხელმძღვანელთა გამოცდილების, ცოდნის, განსჯის და ინტუიციის საფუძველზე. ანალიზის ეს ტიპი სიტყვიერად აღწერს რისკის მოხდენის ალბათობას და გავლენის მასშტაბს.

ხარისხობრივი ანალიზი შეიძლება გამოყენებულ იქნას:

- როდესაც არ არსებობს რაოდენობრივი ანალიზისათვის აუცილებელი მონაცემები და რესურსი
- რისკების ანალიზის საწყის ეტაპზე, როგორც რისკის მოკვლევის საშუალება;
- როდესაც ამ ტიპის ანალიზი საკმარისია სათანადო ანალიზის განსახორციელებლად და გადაწყვეტილებების მისაღებად.

გავრცელებულ პრაქტიკას რისკის ანალიზის პროცესში წარმოადგენს რისკის მატრიცის შემუშავება, რაც გვაძლევს რისკის რანგირების და გამოვლენის საშუალებას. მატრიცა დგება რისკის ალბათობისა და გავლენის ურთიერთკავშირით, რის მიხედვითაც ვიღებთ რისკის რეიტინგს და ვახდენთ მის კატეგორიზაციას

ალბათობა	მაღალი	3	6	9
	საშუალო	2	4	6
	დაბალი	1	2	3
		დაბალი	საშუალო	მაღალი
		გავლენა		

სადაც:

მაღალი	• ფინანსური გავლენა არის მაღალი; • მნიშვნელოვანია გავლენა დაწესებულების სტრატეგიაზე და ოპერაციებზე; • მნიშვნელოვანია დაინტერესება მხარეების მიერ.
საშუალო	• ფინანსური გავლენა არის საშუალო; • ზომიერია გავლენა დაწესებულების სტრატეგიაზე და ოპერაციებზე; • ზომიერია დაინტერესება მხარეების მიერ.
დაბალი	• ფინანსური გავლენა არის დაბალი; • დაბალია გავლენა დაწესებულების სტრატეგიაზე და ოპერაციებზე; • დაბალია დაინტერესება მხარეების მიერ.

9.პასუხისმგებლობების განაწილება

აქტივი არის ნებისმიერი რამ, რაც ფასეულია ორგანიზაციისთვის და ამდენად მოითხოვს დაცვას. აქტივების იდენტიფიცირებისათვის უნდა გვახსოვდეს, რომ ინფორმაციული სისტემა არ შედგება მხოლოდ აპარატურისა და კომპიუტერული პროგრამებისგან.

აქტივების იდენტიფიკაცია უნდა შესრულდეს დეტალურობის გარკვეულ მისაღებ დონემდე, რაც განაპირობებს რისკების შეფასებისათვის საჭირო ინფორმაციის მოპოვებას. აქტივების იდენტიფიკაციისას გამოყენებული დეტალურობის დონე გავლენას ახდენს

რისკების შეფასებისას შეგროვილი ინფორმაციის მოცულობაზე. აღნიშნული დონე შეიძლება გაუმჯობესებული იქნას რისკების შეფასების შემდგომი ციკლის დროს.

ყოველი აქტივის იდენტიფიცირებისას აუცილებლად უნდა მოხდეს კონკრეტული აქტივის მფლობელის გამოვლენა, რათა დადგინდეს აქტივზე პასუხისმგებლობა და ანგარიშვალდებულება. აქტივის მფლობელს შესაძლოა არ გააჩნდეს საკუთრების უფლება კონკრეტულ აქტივზე, მაგრამ მას აქვს პასუხისმგებლობა მის წარმოებაზე, განვითარებაზე, მხარდაჭერაზე, გამოყენებასა და მის უსაფრთხოებაზე საჭიროების შემთხვევაში. აქტივის მფლობელი ხშირად არის სწორედ ის პირი, რომელიც განსაზღვრავს კონკრეტული აქტივის ფასეულობას ორგანიზაციისათვის.

ორგანიზაციის აქტივებზე განხორციელებული მეთვალყურეობის ჩარჩოები წარმოადგენს იმ არეალს, რომელიც განსაზღვრულია ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის წარმართვისათვის.

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.

მენეჯმენტის ვალდებულებები შეგვიძლია ასე ჩამოვაყალიბოთ:

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 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.

10.ინციდენტების ალბათობის შეფასება

ინციდენტის სცენარის იდენტიფიკაციის შემდეგ, აუცილებელია შეფასდეს ყოველი სცენარის ალაბთობა და გავლენა, რის დროსაც გამოყენებული უნდა იყოს როგორც ხარისხობრივი ასევე რაოდენობრივი შეფასების ტექნიკა. ასევე გათვალისწინებული უნდა იყოს თუ რამდენად ხშირად იჩენს თავს საფრთხე და რამდენად მარტივია სუსტი წერტილებით სარგებლობა, ასევე მხედველობაშია მისაღები:

- საფრთხის სტატისტიკა და ალბათობა;

- განზრახ წარმოშობილი საფრთხის წყაროებისთვის: მოტივაცია და შესაძლებლობა, რაც დროთა განმავლობაში იცვლება და ასევე შესაძლო თავდამსხმელების ხელთ არსებული რესურსები, ისევე როგორც აქტივების მნიშვნელოვნების მიმზიდველობისა და სუსტი წერტილების აღქმა შესაძლო თავდამსხმელის მიერ;
- შემთხვევითი საფრთხის წყაროებისთვის: გეოგრაფიული ფაქტორები, მაგალითად ქიმიურ ან ნავთობ ქარხნებთან სიახლოვე, ექსტრემალური მეტეოროლოგიური პირობების შესაძლებლობა, და ფაქტორები, რომლებმაც შესაძლოა გავლენა იქონიონ ადამიანურ შეცდომებსა და დანადგარების შეფერხებით ფუნქციონირებაზე;
- სუსტი წერტილები, როგორც ინდივიდუალური ასევე მათი ერთობლიობა;
- არსებული კონტროლის მექანიზმები და მათი ეფექტურობა სისუსტეების შემცირების თვალსაზრისით.

მაგალითად, ინფორმაციულ სისტემას შესაძლოა გააჩნდეს მომხმარებლის იდენტიფიკაციის შენიღბვის საფრთხის შემცველი სისუსტეები და რესურსების ბოროტად გამოყენების შესაძლებლობა. რესურსების ბოროტად გამოყენების ალბათობა არის დაბალი მნიშვნელობის, მიუხედავად მომხმარებლის აუტენტიფიკაციის არარსებობისა, რადგანაც რესურსების ბოროტად გამოყენების შესაძლებლობები შეზღუდულია.

სიზუსტის აუცილებლობიდან გამომდინარე, აქტივები შეიძლება დაჯგუფდეს, ან დაიყოს შემადგენელ ელემენტებად და სცენარები დაკავშირებული იყოს ამ ელემენტებთან.

10.1 რისკების მიახლოებითი შეფასება

რისკების მიახლოებითი შეფასება განაპირობებს რისკის ალბათობისა და მისი უარყოფითი შედეგების მნიშვნელობას. ეს მნიშვნელობა შეიძლება იყოს რაოდენობრივი ან ხარისხობრივი. რისკების მიახლოებითი შეფასება აერთიანებს და ეყრდნობა ალბათობასა და უარყოფით შედეგებს. დამატებით, იგი შეიძლება ითვალისწინებდეს ასევე გამართლებულ დანახარჯებს, დაინტერესებული პირების პრობლემებს, და სხვა ცვლადებს, რაც რისკების შეფასებითვის აუცილებელია. მიახლოებით შეფასებული რისკი წარმოადგენს ინციდენტის სცენარის და მისი უარყოფითი შედეგების ალბათობის კომბინაციას.

10.2 რისკების დონის დადგენა

რისკების დონის დადგენასთან და მის კრიტერიუმებთან დაკავშირებული გადაწყვეტილებები მიღებული უნდა იქნას ჯერ კიდევ გარემოს განსაზღვის დროს. ეს გადაწყვეტილებები და გარემო ხელხლა უნდა იქნას გადახედილი უფრო დეტალურად იმ შემთხვევაში, როდესაც კონკრეტული რისკის იდენტიფიკაცია უფრო მეტ ინფორმაციას იძლევა. რისკების დონის დასადგენად ორგანიზაციამ უნდა შეადაროს მიახლოებით შეფასებული რისკი რისკების დონის დადგენის კრიტერიუმებთან. გადაწყვეტილებების მისაღებად გამოყენებული რისკების დონის დადგენის კრიტერიუმები შეთავსებადი უნდა იყოს ინფორმაციული უსაფრთხოების რისკების მართვის შიდა და გარე გარემოსთან და უნდა ითვალისწინებდეს ორგანიზაციისა და დაინტერესებული პირების მიზნებს და ა.შ. რისკების დონის დადგენის დროს მიღებული გადაწყვეტილებები ძირითადად ეფუძნება რისკების მისაღებ დონეს. თუმცაღა, უარყოფითი შედეგები, ალბათობა და სანდოობის ხარისხი რისკების იდენტიფიკაციისა და ანალიზის დროს ასევე უნდა იქნას გათვალისწინებული. მრავალი დაბალი ან საშუალო დონის რისკების გაერთიანებამ შეიძლება გამოიწვიოს უფრო მაღალი დონის ყოვლისმომცველი რისკები და საჭირო ხდება მათზე შესაბამისი რეაგირება.

განხილული უნდა იქნას ასევე:

- ინფორმაციული უსაფრთხოების მახასიათებლები: თუ ორგანიზაციისთვის ერთი რომელიმე კრიტერიუმი არ არის მნიშვნელოვანი (მაგალითად: კონფიდენციალურობის დაკარგვა), მაშინ ყველა ამ კრიტერიუმის შემცველი რისკი უმნიშვნელოა
- კონკრეტული აქტივის ან აქტივების ნაკრების მიერ უზრუნველყოფილი ბიზნეს-პროცესების ან ქმედებების მნიშვნელობა: თუ პროცესი განისაზღვრა როგორც დაბალი მნიშვნელობის მქონე, მაშინ მასთან დაკავშირებულ რისკებსაც შესაბამისად ნაკლები ყურადღება მიექცევა, შედარებით მაღალი დონის გავლენის მქონე რისკებთან.

რისკების დონის დადგენა ითვალისწინებს რისკების ანალიზისას გამოვლენილ რისკებს, რათა მიღებული იქნას გადაწყვეტილებები სამომავლო ქმედებების განსახორციელებლად. გადაწყვეტილებები უნდა შეიცავდეს:

- უნდა განხორციელედეს თუ არა ქმედება;
- რისკების თავიდან აცილების პრიორიტეტები რისკების დონეების გათვალისწინებით.

რისკების დონის დადგენის ეტაპზე ხელშეკრულებით გათვალისწინებული, იურიდიული და მარეგულირებელი მოთხოვნები არის ის ფაქტორები, რომლებიც მხედველობაში უნდა იქნას მიღებული მიახლოებით შეფასებულ რისკებთან ერთად.

11. უსაფრთხოების მოდელის ხანდაზმულობა

ნებისმიერ უსაფრთხოების სტანდარტსა თუ მოდელს გააჩნია პერიოდულობა რომლის ინტერვალშიც იგი უნდა გადაიხედოს და შესაბამისობის დადგენა მოხდეს ახლიდან. ამის გამომწვევი მიზეზებია:

1. ორგანიზაციაში ტექნიკური და აპარატურული ცვლილებები
2. ადამიანური რესურსები
3. პროგრამული განახლება
4. ტექნიკური განახლება
5. ორგანიზაციის გაფართოება
6. მოთხოვნების ცვალებადობა
7. ახალი აქტივების დამატება
8. და სხვა მრავალი გამოწვევები

საერთაშორისო სტატისტიკური მონაცემებით დადგენილია რომ ახალი კომპიუტერული ტექნიკა სტაბილურია როგორც ტექნიკურად ისე პროგრამულად 3 წლის მანძილზე. ასევე მათზე გავრცელებული სერთიფიკატებიც 3 წლის მერე გადაიხედება. ეს არ ეხება ნებისმიერ ტექნიკას არსებობს გამონაკლისებიც, თუმცა 3 წელი ოქროს შუალედაა მიჩნეული.

სწორედ ამიტომ თუ ეს მოდელი თბილისის სახელმწიფო უნივერსიტეტში დაინერგება, მისი ოპტიმიზაციის შემდეგ მაქსიმუმ 3 წელში უნდა მოხდეს შესაბამისობის დადგენა ისევ აკმაყოფილებს თუ არა ორგანიზაცია ამ მოდელს.

12.რეკომენდაციები და სამოქმედო გეგმა.

თბილისის ივ.ჯავახიშვილის სახელობის სახელმწიფო უნივერსიტეტში ჩატარებული ანალიზის საფუძველზე დადგინდა გასატარებელი აქტივები. ასევე გამოიკვეთა შესრულებისა და რისკის დონეები.

მენეჯმენტთან გასაუბრების საფუძველზე გადაწყდება გასატარებელი აქტივების თანმიმდევრულობა. ცხრილში მოყვანილია რეკომენდაციების მხოლოდ ფრაგმენტი ხოლო სრული ვერსია „დანართი 2“ სახითაა გადმოცემული.

ჩატარებული კვლევები და შედგენილი კითხვარი დანართი 1 სახით არის წარმოდგენილი მოცემულ ნაშრომში.

აღწერილობა	შესრულების დონე	გასატარებელი აქტივები
ინფორმაციული უსაფრთხოების უნდა იმართებოდეს და პასუხისმგებლობა გამოყოფილი უნდა იყოს თსუ-ს უსაფრთხოების პოლიტიკისა და უსაფრთხოების მართვის პრინციპების შესაბამისად.	არ აკმაყოფილებს	უსაფრთხოების პოლიტიკისა პროცედურების შექმნა-დანერგვა
ყველა თანამშრომელი ვალდებულია ხელი მოაწეროს შესაბამის გაუმჟღავნებლობის შეთანხმებას (მაგალითად, როგორც მათი შრომითი ხელშეკრულების ნაწილი) როგორც ეს განსაზღვრულია ადამიანური რესურსების მიერ. დამატებითი ვალდებულებები	არ აკმაყოფილებს	თანამშრომლების მიერ უსაფრთხოების პოლიტიკის აღიარება და ხელმოწერით დადასტურება
კონფიდენციალურობის ვალდებულებები ისე უნდა ჩამოყალიბდეს, რომ ისინი ძალაში დარჩეს მას შემდეგაც, რაც მოხდება თანამშრომელთა გათავისუფლება ან სხვა შეთანხმების საფუძველზე, თუ სავალდებულო ადგილობრივი კანონმდებლობის შესაბამისად სხვაგვარად არ არის განსაზღვრული.	არ აკმაყოფილებს	დოკუმენტის შექმნა, თანამშრომლის მიერ აღიარება და ხელმოწერა
გაუმჟღავნებლობის შესახებ ხელშეკრულებებით გათვალისწინებული მოთხოვნები პერიოდულად უნდა გადაიხედოს და როდესაც ცვლილებები განხორციელდება, რა გავლენას მოახდენს ამ მოთხოვნებზე.	არ აკმაყოფილებს	გაუმჟღავნებლობის დოკუმენტის შექმნა
არ აქვს მნიშვნელობა ინფორმაციის დამუშავება ან მართვა ხორციელდება შიდა თუ გარე ჯგუფების მიერ, ინფორმაციის დაცვის დონე არ უნდა იყოს დაბალი.	არ აკმაყოფილებს	პოლიტიკისა პროცედურების შექმნა-დანერგვა

თსუ-მ ყოველთვის უნდა ჩაატაროს აუდიტი, რომელიც დაკავშირებულია თსუ-ს მომწოდებლებისა და საქვუწყებო მომწოდებლების მიერ განხორციელებულ სამუშაოებთან.	არ აკმაყოფილებს	აუდიტის პროცესის დანერგვა
აქტივების საკუთრება და მასთან დაკავშირებული პროცესები უნდა იყოს დოკუმენტირებული.	ნაწილობრივ აკმაყოფილებს	აქტივების მფლობელების დოკუმენტირება
ინფორმაციის უსაფრთხოება კლასიფიცირდება ბიზნესის, იურიდიული და სახელშეკრულებო მოთხოვნების შესაბამისად.	არ აკმაყოფილებს	სტანდარტებთან და რეგულაციებთან თავსებადობადობის დადასტურება
ინფორმაციის კლასიფიკაცია არის უსაფრთხოების დონის გადაწყვეტილება ინფორმაციის შექმნის ან იმპორტის დროს.ეს გადაწყვეტილება რეგულარულად უნდა გადაიხედოს და შესაბამისად, შეიცვალოს.	ნაწილობრივ აკმაყოფილებს	კლასიფიკაციის სტანტარტიზაცია
კონფიდენციალურობის კლასიფიკაცია უნდა განხორციელდეს არაავტორიზებული პირის მიერ პოტენციური საფრთხის შექმნის საფუძველზე.კონფიდენციალურობის კლასებია: საიდუმლო, კონფიდენციალური, შიდა და საჯარო.	ნაწილობრივ აკმაყოფილებს	კლასიფიკაციის სტანტარტიზაცია
მთლიანობის კლასიფიკაცია უნდა განხორციელდეს პოტენციური ზიანის საფუძველზე იმ შემთხვევაში, თუ ეს ინფორმაცია არასრულია, დაზიანებული ან დაკარგული.	ნაწილობრივ აკმაყოფილებს	კლასიფიკაციის სტანტარტიზაცია
ხელმისაწვდომობის კლასიფიკაცია უნდა განხორციელდეს პოტენციური საფრთხის საფუძველზე იმ შემთხვევაში, როდესაც ინფორმაცია ან ფუნქცია არ არის ხელმისაწვდომი ავტორიზებული პირისათვის, როცა მას ეს ჭირდება	ნაწილობრივ აკმაყოფილებს	კლასიფიკაციის სტანტარტიზაცია
ინფორმაციული აქტივები ფიზიკურ და ელექტრონულ ფორმატში უნდა შეფასდეს.	ნაწილობრივ აკმაყოფილებს	კლასიფიკაციის სტანტარტიზაცია
ინფორმაციის ყველა მომხმარებელმა უნდა დაცვას გადაწყვეტილი კლასიფიკაციის მოდელი და შესაბამისად, იმოქმედოს ჩამოყალიბებული შიდა ინსტრუქციების მიხედვით.	ნაწილობრივ აკმაყოფილებს	კლასიფიკაციის სტანტარტიზაცია
ასახული უნდა იყოს ინფორმაციის მფლობელის სახელი, წინააღმდეგ შემთხვევაში არ იქნება მითითებული მომხმარებლები.	ნაწილობრივ აკმაყოფილებს	დოკუმენტირება

13.დასკვნა

მოპოვებული მონაცემებისა და ჩატარებული კვლევების საფუძველზე შეიძლება ჩამოვაყალიბოთ შემდეგი:

1. თბილისის ივ. ჯავახიშვილის სახელობის სახელმწიფო უნივერსიტეტში უსაფრთხოების დონე საშუალოა. იგი ჯერ ჯეროზით არ საჭიროებს ISO 27001 საერთაშორისო სტანდარტის დანერგვას თუმცა ჩვენს მიერ მიღებული მოდელის დანერგვა მკვეთრად გააუმჯობესებს უსაფრთხოების დონეს.
2. უნივერსიტეტში არსებული ტექნიკა და პროგრამული უზრუნველყოფა აკმაყოფილებს თანამედროვე სტანდარტებს. მას ესაჭიროება სათანადო დაცვა და გაფრთხილება.
3. ინფორმაციის უსაფრთხოების სისტემა თანხვედრაში უნდა იყოს საკანონმდებლო, მარეგულირებელ და სახელშეკრულებლო ვალდებულებებთან.
4. სახელმწიფო უნივერსიტეტი წამყვანი ობიექტია საქართველოს საგანმანათლებლო სისტემაში და მისთვის რეპუტაცია გადამწყვეტ აქტივს წარმოადგენს.
5. ყველაზე დიდი ხარვეზი ინფორმაციულ უსაფრთხოებაში რაც გამოიკვეთა უნივერსიტეტთან მიმართებაში არის დოკუმენტირების ნაკლებობა. კერძოდ როლები არის გადანაწილებული აქტივებიც განსაზღვრულია მაგრამ არის დოკუმენტირების დეფიციტი.
6. უნივერსიტეტი საჭიროებს მონიტორინგისა და ლოგირების საფუძვლიან დანერგვას
7. აღნიშნული მოდელი მკვეთრად შეამცირებს ინციდენტების რაოდენობას და საშუალებას მიცემს სპეციალისტებს ადვილად აღმოაჩინონ და აღმოფხვრან იგი.
8. სახელმწიფო უნივერსიტეტს გააჩნია ყველა ის რესურსი რაც საჭიროა ამ მოდელის დასანერგად, ასე რომ დანერგვის ფინანსური ღირებულება თითქმის ნულის ტოლი იქნება.

14. გამოყენებული ლიტერატურა

ISO/IEC 27001 – INFORMATION SECURITY MANAGEMENT

NIST 800-39 – MANAGIN INFORMATION SECURITY RISK

COSO – RISK ASSESSMENT IN PRACTISE