ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო
უნივერსიტეტი

ინფორმაციული უსაფრთხოების რისკების მართვა

ლევან ცხადაია

სამაგისტრო პროგრამა: ინფორმაციული ტექნოლოგიები

ნაშრომი შესრულებულია ინფორმაციული ტექნოლოგიების მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი: ტექ. მეცნ.კანდ. გელა ბესიაშვილი

თბილისი, 2014 წელი

სარჩევი

ანოტაცია

ნაშრომში განხილულია იმ რისკების მართვის მეთოდები, რომლებმაც შეიძლება მოახდინონ ორგანიზაციის ინფორმაციული უსაფრთხოების კომპრომენტირება. გაანალიზებულია ინფორმაციული უსაფრთხოების რისკების წარმოქმნის მიზეზები და მათი აღმოფხვრის / შემცირების გზები. ჩამოყალიბებულია ის თავისებურებები, რომელთა გათვალისწინებაც აუცილებელია ინფორმაციული უსაფრთხოების რისკების მართვის სისტემის ჩამოსაყალიბებლად.

შემუშავებულია რეკომენდაციები რომლებიც შეიცავენ ინფორმაციას ინფორმაციული უსაფრთხოების რისკების იდენტიფიცირების, შეფასების, მოპყრობისა და მიღების გზებისა და მეთოდების შესახებ. ინსტრუქცია პრაქტიკული დანიშნულებისაა და მისი გამოყენება შესაძლებელია ნებისმიერი ტიპის თუ ზომის ორგანიზაციაში.

ANNOTATION

The thesis discusses management methods of risks that could compromise the organization's information security. Causes of information security risks and further ways of elimination / reduction are analized. Sets out the characteristics that are necessary to take into account to establish information security risk management system.

Recommendations are included with information about the methods for information security risks identification, evaluation, treatment and acceptance. Given recommedations are intended for practical purposes and can be used in any organization redarding it’s type or size.

შესავალი

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.

ინფორმაციული უსაფრთხოების რისკების მართვა, როგორც მთლიანად რისკების მართვა, არ წარმოადგენს ზუსტ მეცნიერებას: იგი აერთიანებს იმ ხალხის ან ხალხთა ჯგუფის გადაწყვეტილებებს, რომლებიც პასუხისმგებელნი არიან ორგანიზაციის სტრატეგიულ დაგეგმვა, მმართველობასა და ყოველდღიურ ოპერირებაზე.

რისკების მართვა წარმოადგენს პროცესს, რომლის დროსაც ერთად სხდებიან ორგანიზაციის მთავარი წევრები და აანალიზებენ ყველა იმ პოტენციურ რისკს, რომელიც არსებობს ორგანიზაციაში. აღნიშნულ რისკებში განიხილება როგორც კრიტიკული, ასევე უმნიშვნელო რისკები: დაწყებული ხანძრიდან, დამთავრებული ბუნებრივ კატასტროფამდე, როგორიცაა მიწისძვრა.

იმისათვის, რომ წარმატებულად მოხერხდეს ორგანიზაციაში არსებული უსაფრთხოების რისკების მართვა, აუცილებელია ორგანიზაციის ლიდერებმა / აღმასრულებლებმა გაითავისონ და გახადონ რისკების მართვის პროცესი ორგანიზაციის მისიის / ბიზნეს გარემოს შემადგენელი ნაწილი. სწორედ ეს ზედა დონის მმართველობითი ორგანოები / აღმასრულებლები უზრუნველყოფენ რისკების მმართველობის პროცესისთვის საჭირო რესურსების გამოყოფას.

ორგანიზაციის მასშტაბით ინფორმაციული უსაფრთხოების რისკების წარმატებული მართვისთვის საჭიროა შემდეგი ძირითადი ელემენტები:

- ორგანიზაციის ლიდერებისთვის / აღმასრულებლებისთვის რისკების მართვის გარკვეული პასუხისმგებლობების მინიჭება;
- ორგანიზაციის ლიდერების / აღმასრულებლების მხრიდან მუდმივად საქმის ყურში ყოფნა, ორგანიზაციაში არსებული ინფორმაციული უსაფრთხოების რისკების შესახებ;
- ინფორმაციული უსაფრთხოების რისკების მმართველობის აუცილებლობის გათვითცნობიერება ორგანიზაციის მასშტაბით;
- ორგანიზაციის ლიდერებისთვის / აღმასრულებლებისთვის ანგარიშვალდებულების დაკისრება რისკების მართვის პროცესში მიღებულ გადაწყვეტილებებზე;
- ორგანიზაციის ლიდერების / აღმასრულებლების მხრიდან რისკების მმართველობის პროგრამის გაუმჯობესების / განახლების ხელშეწყობა.

აღნიშნული დოკუმენტი წარმოადგენს სახელმძღვანელოს ინფორმაციული უსაფრთხოების რისკების მმართველობისთვის და ძირითადად ემყარება ISO/IEC 27005 სტანდარტში აღწერილ პრინციპებს, რომლებიც მიზნად ისახავენ ინფორმაციული

უსაფრთხოების რისკების მმართველობის პროგრამის იმპლემენტაციას. 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 უსაფრთხოების რისკების მართვისადმი სისტემური მიდგომა აუცილებელია ორგანიზაციის საჭიროებების იდენტიფიცირებისათვის ინფორმაციული უსაფრთხოების მოთხოვნების თვალსაზრისით. ეს მიდგომა უნდა შეესაბამებოდეს ორგანიზაციულ გარემოს. უსაფრთხოების მიმართულებით გამოსაყენებელმა ძალისხმევებმა ეფექტურად და დროულად უნდა განახორციელონ საპასუხო ქმედებები. ინფორმაციული უსაფრთხოების რისკების მართვა უნდა იყოს ინფორმაციული უსაფრთხოების მართვის განუყოფელი ნაწილი.

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:

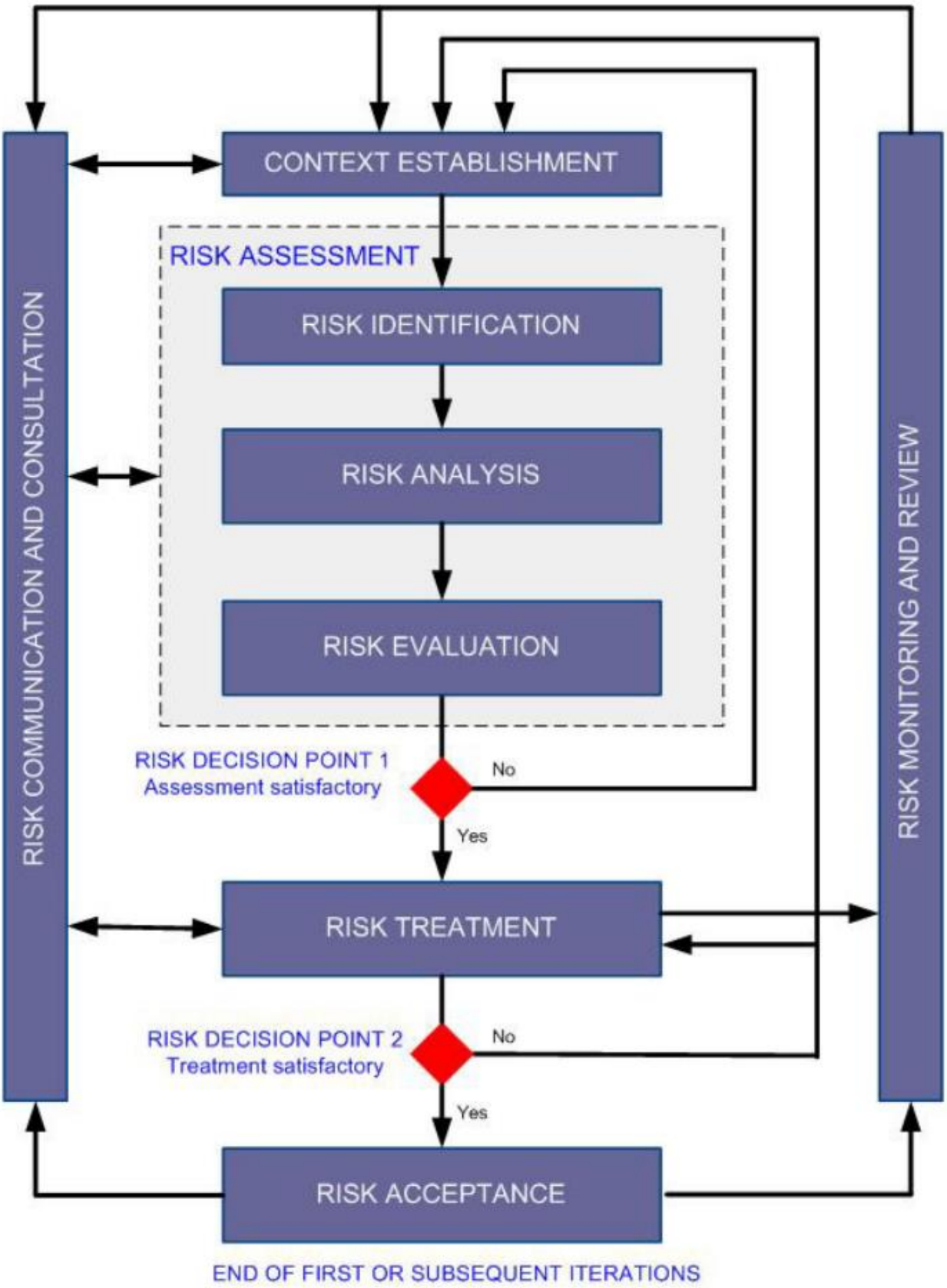
- რისკების იდენტიფიცირებას;
- რისკების შეფასებას იმისდა მიხედვით, თუ რა შედეგები მოყვება მათ ბიზნესთან მიმართებაში და მათი ხდომილების ალბათობა;
- ამ რისკების დადგომის ალბათობას და მათ შესაძლო შედეგებს, მათ შესახებ ინფორმირებულობის არსებობას;
- რისკებთან მობყრობის პრიორიტეტულობის დადგენას;
- რისკების 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).

1. ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის მიმოხილვა

ინფორმაციული უსაფრთხოების რისკები მართვის პროცესი შედგება შემდეგი პროცესებისგან: ორგანიზაციული გარემოს დადგენა, რისკების შეფასება, რისკებთან მობყრობა, რისკების მიღება, რისკების შესახებ ინფორმირება და რისკების მონიტორინგი და განხილვა.


CONTEXT ESTABLISHMENT
RISK ASSESSMENT
RISK IDENTIFICATION
RISK ANALYSIS
RISK EVALUATION
RISK DECISION POINT 1
Assessment satisfactory
No
Yes
RISK TREATMENT
RISK DECISION POINT 2
Treatment satisfactory
No
Yes
RISK ACCEPTANCE
RISK COMMUNICATION AND CONSULTATION
RISK MONITORING AND REVIEW
END OF FIRST OR SUBSEQUENT ITERATIONS

როგორც ნახაზი გვიჩვენებს, ინფორმაციული უსაფრთხოების მართვის პროცესი შეიძლება იყოს განმეორებადი ხასიათის რისკების შეფასებისა და/ ან რისკებთან მობყრობის ქმედებების თვალსაზრისით. რისკის შეფასების მართვის განმეორებადობამ შესაძლოა გააღრმავოს და უფრო დეტალური გახადოს შეფასება ყოველი შემდგომი ციკლისას. განმეორებადი ხასიათის მიდგომა წარმოადგენს საუკეთესო ბალანსს დროის დაზოგვასა და კონტროლის მექანიზმის იდენტიფიცირებას შორის, ამავდროულად უზრუნველყოფს მაღალი დონის რისკების შესაბამის შეფასებას.

პირველ რიგში უნდა დადგინდეს გარემო. შემდგომ კი უნდა მოხდეს რისკის შეფასება. თუ ამ ქმედებების შემდეგ ხელთ გვექნება საკმარისი ინფორმაცია იმისათვის, რომ რისკები დაყვანილი იქნას დასაშვებ დონემდე, მაშინ შეიძლება ჩაითვალოს, რომ დავალება შესრულებულია და შემდგომი ეტაპი უკვე არის რისკებთან მობყრობა. არასაკმარისი ინფორმაციის არსებობის შემთხვევაში ადგილი ექნება რისკის შეფასების შემდგომ ციკლს (გარემოს გადახედვის ჩათვლით) (მაგალითად: რისკების შეფასების, მნიშვნელოვნების დადგენის კრიტერიუმები, რისკებზე თანხმობის კრიტერიუმები ან ზემოქმედების კრიტერიუმები), რაც სავარაუდოდ ვრცელდება მთლიანი ფარგლების კონკრეტულ ნაწილზე.

რისკებთან მობყრობის ეფექტიანობა დამოკიდებულია რისკის შეფასების შედეგებზე. შესაძლებელია რისკებთან მობყრობამ მაშინვე არ უზრუნველყოს მოცემული რისკის დასაშვები დონე. ასეთ შემთხვევაში შესაძლოა საჭირო გახდეს რისკების განმეორებითი შეფასება გარემოს განსაზღვრის შეცვლილი პარამეტრებით (მაგალითად: რისკების შეფასება, რისკების მიღება ან რისკების გავლენის კრიტერიუმები), რომლის თანმხლები პროცესი არის რისკებთან შემდგომი მობყრობა.

რისკების მიღებამ უნდა უზრუნველყოს რეაგირების გარეშე დარჩენილ რისკზე ცალსახა თანხმობა ორგანიზაციის მენეჯერების მხრიდან. ეს მომენტი განსაკუთრებით მნიშვნელოვანია ისეთ დროს, როდესაც კონტროლის მექანიზმის დანერგვა უგულვებელყოფილია ან გადადებულია, მაგალითად ხარჯების მიზეზით.

ინფორმაციული უსაფრთხოების რისკების მართვის მთელი პროცესის განმავლობაში მნიშვნელოვანია, რომ არსებობდეს კომუნიკაცია რისკებსა და მათთან მობყრობას შორის, ასევე შესაბამის მენეჯერებსა და საოპერაციო თანამშრომლებს შორის. რისკთან მობყრობამდე კი ძალზე მნიშვნელოვანია ინფორმაცია იდენტიფიცირებული რისკის შესახებ, რათა მოხდეს ინციდენტის მართვა, რამაც შესაძლოა ხელი შეუწყოს პოტენციური ზიანის შემცირებას.

მენეჯრებისა და თანამშრომლების ინფორმირებულობა ორგანიზაციის რისკების შესახებ, რისკების და პრობლემური საკითხების შემცირების კონტროლის მექანიზმის შესახებ ხელს უწყობს ინციდენტების და მოულოდნელი შემთხვევების ეფექტურ აღმოფხვრას. ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის თითოეული ქმედების დეტალური შედეგი და ასევე რისკების შესახებ გადაწყვეტილების მიღების შედეგი უნდა იყოს დოკუმენტირებული.

2. **გარემოს განსაზღვრა**

ინფორმაციული უსაფრთხოების რისკების მართვის გარემო უნდა იქნას განსაზღვრული, რაც თავისთავად მოიცავს საჭირო კრიტერიუმების დადგენას ინფორმაციული უსაფრთხოების რისკების მართვის თვალსაზრისით, გამოყენების სფეროსა და ჩარჩოების განსაზღვრას და შესაბამისი ორგანიზაციული სტრუქტურის შექმნას, რომელიც განახორციელებს ინფორმაციული უსაფრთხოების რისკების მართვას.

ინფორმაციული უსაფრთხოების რისკების მართვის მიზნის განსაზღვრა არის არსებითი მომენტი, რადგანაც იგი ზეგავლენას ახდენს მთლიან პროცესზე და გარემოს განსაზღვრაზე ნაწილობრივ. მიზანი შესაძლოა იყოს:

- ორგანიზაციის მიდგომის მხარდაჭერა ინფორმაციული უსაფრთხოებისადმი
- თავსებადობა (Compliance)
- ბიზნეს უწყვეტობის გეგმის მომზადება
- ინციდენტზე რეაგირების გეგმის მომზადება
- ინფორმაციული უსაფრთოების მოთხოვნების აღწერა პროდუქტის ან სერვისის კუთხით

4.1 ძირითადი კრიტერიუმები

შერჩეული და შემუშავებული უნდა იქნას რისკების მართვის შესაბამისი მიდგომა, რომელიც მიმართებაშია ისეთ ძირითად კრიტერიუმებთან, როგორებიცაა: რისკების შეფასების კრიტერიუმები, გავლენის კრიტერიუმები, რისკების მიღების კრიტერიუმები.

ასევე, ორგანიზაციამ უნდა შეაფასოს არსებობს თუ არა საჭირო რესურსები:

- რისკების შეფასებისა და რისკებთან მობყრობის გეგმის შემუშავებისთვის;

- პოლიტიკისა და პროცედურების განსაზღვრა და განხორციელება, მათ შორის შერჩეული კონტროლის მექანიზმების დანერგვა;
- კონტროლის მექანიზმების მონიტორინგი;
- ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის მონიტორინგი.

4.2 რისკების დონის დადგენის კრიტერიუმები

რისკების დონის დადგენის კრიტერიუმები უნდა შემუშავდეს ორგანიზაციის ინფორმაციული უსაფრთხოების რისკების შეფასების მიზნით, რაც ასევე გულისხმობს შემდეგს:

- ბიზნეს ინფორმაციის პროცესის სტრატეგიული მნიშვნელობა;
- ჩართული ინფორმაციული აქტივების კრიტიკულობა;
- იურიდიული და მარეგულირებელი მოთხოვნები, სახელშეკრულებო ვალდებულებები;
- ხელმისაწვდომობის, კონფიდენციალურობისა და მთლიანობის ოპერაციული და ბიზნეს მნიშვნელობა;
- დაინტერესებული პირების მოლოდინები და აღქმა, და რეპუტაციის შელახვის უარყოფითი შედეგები;

დამატებით, ასევე შესაძლოა რისკების დონის დადგენის კრიტერიუმები გამოყენებული იქნას რისკების გადაჭრის პრიორიტეტების განსაზღვრისათვის.

4.3 გავლენის კრიტერიუმები

გავლენის კრიტერიუმები შემუშავებული და განსაზღვრული უნდა იქნას ორგანიზაციისთვის მიყენებული ზიანის ან ხარჯების დონის გათვალისწინებით, რაც შესალოა გამოწვეული იყოს ინფორმაციული უსაფრთხოების შემთხვევის მიერ და მოიცავდეს შემდგომს:

- რისკის გავლენის ქვეშ არსებული ინფორმაციული აქტივის კალსიფიკაციის დონე;
- ინფორმაციული უსაფრთხოების დარღვევა (მაგალითად: კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დაკარგვა);
- გაუარესებული ოპერაციები (შიდა ან მესამე მხარისა);

- ბიზნეს და ფინანსური ღირებულების შემცირება;
- გეგმებისა და მათი შესრულების ვადების დარღვევა;
- რეპუტაციის შელახვა;
- იურიდიული, მარეგულირებელი და სახელშეკრულებო მოთხოვნების დარღვევა.

4.4 რისკის მიღების კრიტერიუმები

შემუშავებული და განსაზღვრული უნდა იქნას რისკის მიღების კრიტერიუმები. რისკის მიღების კრიტერიუმები დამოკიდებულია ორგანიზაციის პოლიტიკაზე, მიზნებზე და დაინტერესებული პირების ინტერესებზე.

ორგანიზაციამ თავად უნდა განსაზღვროს დასაშვები რისკის საკუთარი სქემა. შემუშავების პროცესში გათვალისწინებული უნდა იყოს შემდეგი:

- რისკის მიღების კრიტერიუმებს შესაძლოა ქონდეს შეზღუდვები რისკების სასურველი დონის თვალსაზრისით, მაგრამ აუცილებელია გარკვეულ ვითარებებში ზედა რგოლის მენეჯერების მხრიდან განხორციელდეს რევიზია, რათა მიღებული იქნას თანხმობა ამ კონკრეტული დონის ზემოთ დაფიქსირებულ რისკებზე;
- რისკის მიღების კრიტერიუმები შეიძლება წარმოდგენილი იყოს როგორც გაანგარიშებული მოგების შეფარდება გაანგარიშებულ რისკთან;
- რისკის მიღების სხვადასხვა კრიტერიუმები შეიძლება მიესადაგოს სხვადასხვა კლასის რისკებს, მაგალითად: რისკებმა შესაძლოა თავი იჩინონ მარეგულირებლებთან ან კანონთან შეუსაბამობის შედეგად და, ამდენად, არ მოხდეს ასეთ რისკებზე თანხმობა, მაშინ, როდესაც მაღალი დონის რისკებზე თანხმობა შეიძლება დასაშვები იყოს, თუკი ამის საშუალებას იძლევა სახელშეკრულებო მოთხოვნები;
- რისკის მიღების კრიტერიუმები შეიძლება შეიცავდეს სამომავლოდ მათი გადაჭრის მოთხოვნებს, მაგალითად რისკი შესაძლოა მიღებული იქნას, თუკი არსებობს მტკიცებულება და ვალდებულება იმისა, რომ განხორციელდეს ქმედება რისკის დასაშვებ (მისაღებ) დონემდე შემცირების მიზნით განსაზღვრულ დროის პერიოდში.

რისკის მიღების კრიტერიუმები ერთმანეთისგან რისკის არსებობის მოსალოდნელი ხანგრძლივობით განსხვავდებიან, მაგალითად: რისკი შეიძლება დაკავშირებული იყოს

ხანგრძლივ ან ხანმოკლე ქმედებებთან. რისკის მიღების კრიტერიუმები უნდა ითვალისწინებდეს და ეფუძნებოდეს შემდეგს:

- ბიზნეს კრიტერიუმები;
- იურიდიული და მარეგულირებელი ასპექტები;
- ოპერაციები;
- ტექნოლოგია;
- ფინანსები;
- სოციალური და ადამიანური ფაქტორები.

4.5 გამოყენების სფერო და საზღვრები

ორგანიზაციამ უნდა განსაზღვროს ინფორმაციული უსაფრთხოების რისკის მართვის გამოყენების სფერო და საზღვრები.

ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის მიზნები აუცილებლად უნდა იქნას განსაზღვრული, რათა გათვალისწინებული იყოს ყველა საჭირო აქტივი რისკების შეფასებისას. დამატებით უნდა ითქვას, რომ საზღვრების დადგენა ასევე აუცილებელია, რათა რეაგირება მოხდეს ისეთ რისკებზე, რომლებმაც შესაძლოა თავი იჩინონ კონკრეტულ ფარგლებში.

ორგანიზაციის შესახებ ინფორმაციის შეგროვება აუცილებელია იმ გარემოს დასადგენად, რომელშიც იგი ფუნქციონირებს და ასევე მისი გასათვალისწინებელია მისი აუცილებლობა ინფორმაციული უსაფრთხოების რისკების მართვის პროცესისთვის.

გამოყენების სფეროსა და საზღვრების დადგენისას ორგანიზაციამ უნდა გაითვალისწინოს შემდეგი ინფორმაცია:

- ორგანიზაციის სტრატეგიული ბიზნეს მიზნები, სტრატეგია და პოლიტიკა;
- ბიზნეს პროცესები;
- ორგანიზაციის ფუნქციები და სტრუქტურა;
- ორგანიზაციის შესაბამისი იურდიული, მარეგულირებელი და სახელშეკრულებო მოთხოვნები;
- ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკა;
- ორგანიზაციის ზოგადი მიდგომა რისკების მართვისადმი;

- ინფორმაციული აქტივები;
- ორგანიზაციის ადგილმდებარეობა და მისი გეოგრაფიული მახასიათებლები;
- ორგანიზაციაზე გავლენის მომხდენი ფაქტორები;
- დაინტერესებული პირების მოლოდინები;
- სოციალურ-კულტურული გარემო;
- ინტერფეისები (მაგალითად: გარემოსთან გაცვლილი ინფორმაცია).

დამატებით, ორგანიზაციამ უნდა უზრუნველყოს გამონაკლისების გამართლება.

რისკის მართვის მიზნის მაგალითად შესაძლოა ჩაითვალოს ი.ტ. პროგრამული უზრუნველყოფები, ი.ტ. ინფრასტრუქტურა, ბიზნეს-პროცესი ან ორგანიზაციის განსაზღვრული ნაწილი.

4.6 ინფორმაციული უსაფრთხოების რისკების მართვის ორგანიზაციული სტრუქტურა

უნდა დადგინდეს და დაცული იქნას ინფორმაციული უსაფრთხოების რისკების მართვის პროცესისთვის საჭირო ორგანიზაციული სტრუქტურა და პასუხისმგებლობები. ძირითადი როლები და პასუხისმგებლობები გახლავთ:

- ორგანიზაციაზე მორგებული ინფორმაციული უსაფრთხოების რისკების მართვის პორცესის შემუშავება;
- დაინტერესებული პირების გამოვლენა და ანალიზი;
- ყველა მხარის (როგორც შიდა ასევე გარე) როლებისა და პასუხისმგებლობების განსაზღვრა ორგანიზაციისათვის;
- ორგანიზაციასა და დაინტერესებულ პირებს შორის საჭირო ურთიერთობის დამტკიცება, ასევე ორგანიზაციის მაღალი დონის რისკების მართვის ფუნქციებისთვის ინტერფეისების დადგენა (მაგალითად: ოპერაციული რისკების მართვა), ასევე სხვა პროექტების და ქმედებებისთვის საჭირო ინტერფეისები;
- გადაწყვეტილების მიღების წესის განსაზღვრა;
- აღრიცხვიანობის (რეგისტრირების, ჩანაწერების) მახასიათებლები.

ამგვარი ორგანიზაციული სტრუქტურა დამტკიცებული უნდა იქნას მენეჯერების მიერ.

3. ინფორმაციული უსაფრთხოების რისკების შეფასება

რისკი, ეს არის არასასურველი მოვლენით ან მისი ხდომილების ალბათობით გამოწვეული უარყოფითი შედეგების კომბინაცია. რისკების რაოდენობრივი და ხარისხობრივი შეფასება აღწერს რისკს და საშუალებას აძლევს მენეჯერებს პრიორიტეტები მიანიჭონ რისკებს სერიოზულობისა ან სხვა დადგენილი კრიტერიუმების მიხედვით.
რისკების შეფასება შედგება შემდეგი ქმედებებისგან:

- რისკის ანალიზი, რომელიც შეიცავს:
    - რისკების იდენტიფიცირებას
    - რისკების მიახლოებითი შეფასება
- რისკის დონის დადგენა

რისკების შეფასება განსაზღვრავს ინფორმაციული აქტივების ფასულობას, ახდენს მოსალოდნელი საფრთხეების და არსებული (ან შესაძლო) სუსტი წერტილების იდენტიფიცირებას, განსაზღვრავს არსებულ კონტროლის მექანიზმს და მის გავლენას აღმოჩენილ რისკებზე, ასევე განსაზღვრავს პოტენციურ უარყოფით შედეგებს და საბოლოოდ ანიჭებს პრიორიტეტებს გამოვლენილ რისკებს და ახდენს მათ კლასიფიცირებას კონკრეტულ გარემოში.

რისკების შეფასება ხშირად წარიმართება ორ (ან მეტ) განმეორებად ციკლად. პირველ რიგში უნდა ჩატარდეს ზედა დონის შეფასება, რათა მოხდეს პოტენციურად მაღალი რისკების გამოვლენა, რაც წარმოადგენს საფუძველს შემდგომი შეფასებისთვის. მომდევნო განმეორებადი ციკლი მოიცავს იმ მაღალი რისკების შემდგომ სიღრმისეულ განხილვას, რომლებიც აღმოჩენილი იქნა საწყისი ციკლის დროს. თუკი გარკვეულ ეტაპზე იგი იძლევა რისკის შეფასების თვალსაზრისით არასაკმარის ინფორმაციას, მაშინ ხორციელდება შემდგომი დეტალური ანალიზი, სავარაუდოდ განსხვავებული მეთოდების გამოყენებით კონკრეტულ ნაწილზე.

მთლიანად ორგანიზაციაზეა დამოკიდებული რისკების მართვისადმი საკუთარი მიდგომის არჩევა, რაც დაფუძნებული იქნება რისკების შეფასების მიზნებსა და ამოცანებზე.

5.1 რისკების ანალიზი

5.1.1 რისკების იდენტიფიკაცია

რისკების იდენტიფიკაციის მიზანია განისაზღვროს თუ რა შეიძლება მოხდეს პოტენციური დანაკარგის გამოწვევით, და მოვიპოვოთ ცოდნა იმისა, თუ როგორ, სად და რატომ შეიძლება მოხდეს დანაკარგი.

5.1.2 აქტივების იდენტიფიკაცია

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.

5.1.3 საფრთხეების დადგენა

საფრთხეს შეუძლია ზიანი მიაყენოს ისეთ აქტივებს, როგორებიცაა ინფორმაცია, პროცესები და სისტემები, და აქედან გამომდინარე თავად ორგანიზაციასაც. საფრთხეები შეიძლება იყოს ბუნებრივი ხასიათის ან ადამიანის მიერ შექმნილი, და ასევე შემთხვევითი ან გამიზნული. აუცილებლად უნდა იქნას იდენტიფიცირებული როგორც შემთხვევითი, ასევე

გამიზნული სართხეების წარმოშობის წყაროები. საფრთხე შეიძლება წარმოიშვას როგორც ორგანიზაციის შიგნით, ასევე მის გარეთ. უნდა გაიმიჯნოს ზოგადი და ტიპიური საფრთხეები (მაგალითად: არაავტორიზებული ქმედება, ფიზიკური ზიანი, ტექნიკური ჩავარდნა) და შემდეგ განხორციელდეს ინდივიდუალური საფრთხეების მიკუთვნება გარკვეული სახეობების კლასისადმი. ეს გულისხმობს, რომ არც ერთი სართხე, მათ შორის მოულოდნელიც, არ რჩება გამოვლენისა და ამოცნობის გარეშე, მაგრამ ამასთან დაკავშირებული სამუშაოების მოცულობა შესაძლოა დაკავშრებული იყოს გარკვეულ შეზღუდვებთან.

ზოგიერთმა საფრთხემ შესაძლოა რამდენიმე აქტივზე იქონიოს გავლენა. ასეთ შემთხვევაში, მათი ზეგავლენა სხვადასხვანაირი იქნება აქტივიდან გამომდინარე.

საფრთხის იდენტიფიკაცია და მათი ხდომილების ალბათობის შეფასება შეიძლება მოვიპოვოთ აქტივების მფლობელების ან მომხმარებლებისაგან, მომსახურე პერსონალისგან, ინფრასტრუქტურის მართვაში ჩართული პერსონალისაგან და ინფორმაციული უსაფთხოების სპეციალისტებისგან, ფიზიკური უსაფრთხოების ექსპერტებისგან, იურიდიული დეპარტამენტისგან და სხვა ორგანიზაციებისგან, მათ შორის სამართალდამცავი ორგანოებისგან, ისევე როგორც ხელისუფლების, სადაზღვევო კომპანიებისა და ქვეყნის მმართველობისგან. საფრთხეზე რეაგირებისას აუცილებლად გათვალისწინებული უნდა იქნას გარემო და კულტურული ასპექტები.

მიმდინარე შეფასებებში აუცილებლად გათვალისწინებული უნდა იყოს შიდა ინციდენტების შესახებ არსებული გამოცდილება და ასევე წარსული საფრთხეების შეფასება. მნიშვნელოვანია ასევე სხვა სახის საფრთხეების კატალოგების გათვალისწინება (მაგალითად კონკრეტული ორგანიზაციისა ან ბიზნესისთვის სპეციფიკური), რათა ხელთ გვქონდეს ძირითადი საფრთხეების სახეობების (ნომენკლატურის) სრულყოფილი სია საჭიროების შემთხვევაში. საფრთხეების კატალოგების და სტატისტიკის წყაროს შესაძლოა წარმოადგენდნენ დარგობრივი ორგანოები, მთავრობა, სამართალდამცავი ორგანოები, სადაზღევვო კომპანიები.

საფრთხეების კატალოგის ან წინა საფრთხის შეფასების შედეგების გამოყენების დროს აუცილებლად უნდა გავაცნობიეროთ: მნიშვნელოვანი საფრთხეები მუდმივად იცვლებიან, განსაკუთრებით იმ შემთხვევაში, როდესაც იცვლება ბიზნეს გარემო ან ინფორმაციული სისტემა.

5.1.4 არსებული კონტროლის მექანიზმების იდენტიფიკაცია

არსებული კონტროლის მექანიზმების იდენტიფიკაცია უნდა განხორციელდეს იმ მიზნით, რათა თავიდან იქნას აცილებული ზედმეტი უსარგებლო სამუშაო და ხარჯები, მაგალითად: კონტროლის მექანიზმის დუბლირება. დამატებით უნდა ითქვას, რომ არსებული კონტროლის მექანიზმების იდენტიფიცირებისას, შემოწმებამ უნდა უზრუნველყოს კონტროლის მექანიზმის ზუსტი (უშეცდომო) მუშაობა. თუ კონტროლის მექანიზმი არ სრულდება მოლოდინის შესაბამისად, მაშინ მან შეიძლება გამოიწვიოს სუსტი წერტილები. მხედველობაში უნდა იქნას მიღებული ის სიტუაცია, როდესაც არჩეული კონტროლის მექანიზმი (ან სტრატეგია) განიცდის წარუმატებლობას ოპერაციისას და ამდენად საჭირო ხდება დამატებითი კონტროლის მექანიზმების გამოყენება იდენტიფიცირებულ რისკზე ეფექტური რეაგირებისათვის.კონტროლის მექანიზმის ეფექტის შეფასების გზა გახლავთ დავინახოთ თუ როგორ ამცირებს იგი საფრთხის ალბათობას, სუსტი წერტილებით სარგებლობის სიმარტივეს, ან ინციდენტის მიერ მოხდენილ უარყოფით გავლენას. არსებული კონტროლის მექანიზმები ეფექტიანობაზე ინფორმაციას იძლევა ასევე ხელმძღვანელობის მიერ ჩატარებული განხილვა (ანალიზი, შეფასება) და აუდიტის ანგარიშები.

რისკების გადაჭრის გეგმის მიხედვით დასანერგი კონტროლის მექანიზმების დანერგვისას გათვალისწინებული უნდა იყოს უკვე დანერგილი კონტროლის მექანიზმების დანერგვის გამოცდილება.

არასებული ან დაგეგმილი კონტროლის მექანიზმი შესაძლოა მიჩნეული იყოს როგორც არაეფექტური, ან არასაკმარისი ან უსაფუძვლო. უსაფუძვლობის ან არასაკმარისობის შემთხვევაში უნდა შემოწმდეს კონტროლის მექანიზმი, რათა განისაზღვროს საჭიროა თუ არა მისი გაუქმება, შეცვლა სხვა მეტად შესაბამისი კონტროლის მექანიზმით, თუ უნდა დავტოვოთ არსებული კონტროლის მექანიზმი, მაგალითად ხარჯების თვალსაზრისით.
არსებული ან დაგეგმილი კონტროლის მექანიზმების იდენტიფიკაციის დამხამრე ქმედებებია:

- კონტროლის მექანიზმების შესახებ დოკუმენტაციის გადახედვა (მაგალითად, რისკებთან მობყრობის გეგმა).
- ინფორმაციულ უსაფრთხოებაზე პასუხისმგებელ პირებთან (მაგალითად, ინფორმაციული უსაფრთხოების ოფიცერი და ინფორმაციული სისტემის

უსაფრთხოების ოფიცერი, შენობის კომენდანტი ან ოპერაციათა მენეჯერი) და მომხმარებლებთან გადამოწება იმისა, თუ რომელი კონტროლის მექანიზმი ხორციელდება რეალურად კონკრეტული ინფორმაციული პროცესებისა და ინფორმაციული სისტემებისთვის;

- ფიზიკური კონტროლის მექანიზმების ადგილზე დაკვირვება, შედარება უკვე განხორციელებული კონტროლის მექანიზმებისა და კონკრეტულად დასანერგი კონტროლის მექანიზმების სიისა, უკვე განხორციელებული კონტროლის მექანიზმების გადამოწმება იმ მიზნით, რამდენად სწორად და ეფექტიანად მუშაობენ, ან
- შიდა აუდიტის შედეგების მიმოხილვა.

5.1.5 სუსტი წერტილების იდენტიფიცირება

სუსტი წერტილების გამოვლენა შესაძლებელია:

- ორგანიზაციაში;
- პროცესებსა და პროცედურებში;
- ხელმძღვანელობაში;
- პერსონალში;
- ფიზიკურ გარემოში;
- ინფორმაციული სისტემის კონფიგურაციაში;
- აპარატურაში, კომპიუტერულ პროგრამებში ან საკომუნიკაციო აღჭურვილობებში;
- მესამე მხარეებზე დამოკიდებულებაში.

თავისთავად სუსტი წერტილების არსებობა არ გულისხმობს ზიანის გამოწვევას, თუკი არ არსებობს საფრთხე, რომელიც ამ სუსტი წერტილებით ისარგებლებს. სუსტი წერტილი შესაბამისი საფრთხის არ არსებობის შემთხვევაში, არ საჭიროებს მასზე კონტროლის მექანიზმის განხორციელებას, მაგრამ უნდა იქნას გაცნობიერებული და ხდებოდეს მისი ცვლილებების მონიტორინგი. უნდა აღინიშნოს, რომ არაკორექტულად ან შეფერხებებით განხორციელებული კონტროლის მექანიზმი ან არაკორექტულად გამოყენებული კონტროლის მექანიზმი თავად შეიძლება აღმოჩნდეს სუსტი წერტილი. კონტროლის მექანიზმი შეიძლება იყოს ეფექტიანი ან არაეფექიანი, რაც დამოკიდებულია იმ გარემოზე,

რომელშიც ის ფუნქციონირებს. მეორეს მხრივ, საფრთხე, რომელსაც არ გააჩნია შესაბამისი სუსტი წერტილი, არ იწვევს რისკს.

აქტივებს შესაძლოა ახასიათებდეს სუსტი წერტილები, რომლებიც გამოიყენება გარკვეულწილად, ან გარკვეული მიზნებისათვის (გარდა იმისა, რომ ვიცოდეთ თუ როდის იქნა შეძენილი და წარმოებული აქტივი). მხედველობაში უნდა იქნას მიღებული სუსტი წერტილების წარმოშობის სხვადასხვა წყარო, მაგალითად თვისობრივი და შემთხვევითი.

5.1.6 უარყოფითი შედეგების იდენტიფიკაცია

უარყოფითი შედეგი შეიძლება იყოს ეფექტიანობის არარსებობა, მავნე სამუშაო პირობები, ბიზნესის დაკარგვა, რეპუტაციის შელახვა, ზარალი და ასე შემდეგ.

აღნიშნული ქმედება განსაზღვრავს ორგანიზაციის ზიანს ან მისთვის უარყოფით შედეგებს, რაც შესაძლოა გამოწვეული იყოს ინციდენტის სცენარის შესაბამისად. ინციდენტის სცენარი არის საფრთხის მიერ სუსტი წერტილით ან სუსტი წერტილების ნაკრებით სარგებლობის აღწერა ინფორმაციული უსაფრთხოების ინციდენტის დროს. გარემოს განსაზღვრის დროს დადგენილი გავლენის კრიტერიუმების გათვალისწინებით უნდა მოხდეს ინციდენტების სცენარების გავლენების განსაზღვრაც. მან შესაძლოა გავლენა იქონიოს ერთ ან მეტ აქტივზე ან მის ნაწილზე. თუმცაღა აქტივებს შესაძლოა დადგენილი ქონდეთ ფასეულობა როგორც ფინანსური თვალსაზრისით, ასევე ბიზნესისთვის უარყოფითი შედეგების კუთხით, თუკი მოხდება მათი დაზიანება ან საფრთხის ქვეშ დაყენება. უარყოფითი შედეგები შესაძლოა იყოს დროებითი ან პერმანენტული, მაგალითად, აქტივის განადგურება.

ორგანიზაციამ უნდა მოახდინოს ინციდენტების სცენარების უარყოფითი ოპერაციული შედეგების იდენტიფიკაცია შემდეგი მიზნებისთვის:

- გამოძებისა და აღდგენის (გამოსწორების) დრო;
- (სამუშაო) დროის არასწორად გამოყენება;
- სახარბიელო სიტუაციის დაკარგვა;
- ჯანმრთელობა და უსაფრთხოება;
- ზარალის აღდგენისთვის საჭირო სპეციფიკური უნარ-ჩვევების გამოყენებისას ფინანსური დანახარჯები;
- რეპუტაცია.

5.2 რისკების მიახლოებითი შეფასება

5.2.1 რისკების შეფასების მეთოდოლოგიები

რისკის ანალიზი შესაძლოა ჩატარდეს დეტალურობის სხვადასხვა დონეზე, რაც დამოკიდებულია აქტივის კრიტიკულობაზე, ცნობილი სუსტი წერტილების ხარისხზე და ორგანიზაციაში არსებულ წინა ინციდენტებზე. შეფასების მეთოდოლოგია შეიძლება იყოს ხარისხობრივი ან რაოდენობრივი, ან ორივე ერთად გამომდინარე ვითარებიდან. როგორც პრაქტიკაშია მიღებული, თავდაპირველად გამოიყენება ხარისხობრივი შეფასება, რათა მოპოვებული იქნას რისკის დონის ზოგადი მახასიათებელი და გამოვლენილი იქნას ძირითადი რისკები. მოგვიანებით კი შესაძლოა ჩატარდეს უფრო სპეციფიკური ხასიათის ან რაოდენობრივი ანალიზი ძირითადი რისკებისა, რადგანაც რაოდენობრივი ანალიზის პროცესი ხასიათდება ნაკლები კომპლექსურობით და დანახარჯებით, ვიდრე ხარისხობრივისა.

ანალიზის ფორმა შეთავსებადი უნდა იყოს რისკების დონის დადგენის კრიტერიუმებთან, რომლებიც შემუშავებული იქნა როგორც ორგანიზაციული გარემოს ნაწილი.

შეფასების მეთოდოლოგიის შემდგომ დეტალებს განვიხილავთ ქვემოთ:

(a) **ხარისხობრივი შეფასება:**

ხარისხობრივი შეფასება გამოიყენებს ხარისხობრივი ატრიბუტების შკალას, რათა აღწერილი იქნას პოტენციური უარყოფითი შედეგების მნიშვნელოვნება (მაგალითად, დაბალი, საშუალო და მაღალი) და ასევე ამ უარყოფითი შედეგების დადგომის ალბათობა. ხარისხობრივი შეფასების უპირატესობა არის მისი აღქმის სიმარტივე, მაშინ, როდესაც მისი უარყოფითი მხარე შკალის სუბიექტურ არჩევანში მდგომარეობს.

შეიძლება ამ შკალების ადაპტირება და მორგება გარკვეულ ვითარებებზე, ასევე სხვადასხვა რისკებისთვის სხვადასხვა აღწერილობების გამოყენება. ხარისხობრივი შეფასება შეიძლება გამოყენებული იქნას:

- როგორც საწყისი გადამოწმება რისკების იდენტიფიცირებისათვის, რაც მოითხოვს შემდგომ დეტალურ ანალიზს;
- იქ, სადაც ამგვარი ანალიზი მისაღებია გადაწყვეტილების მისაღებად;
- იქ, სადაც ციფრობრივი მონაცემები ან რესურსები არაადექვატურია რაოდენობრივი შეფასებისათვის.

ხარისხობრივი ანალიზი უნდა ტარდებოდეს ფაქტებზე დაყრდნობით და გამოიყენებდეს მოპოვებულ მონაცემებს.

(b) **რაოდენობრივი შეფასება:**

რაოდენობრივი შეფასებისას გამოიყენება ციფრული მნიშვნელობის შკალა სხვადასხვა წყაროების მონაცემებით (შედარებით ხარისხობრივ შეფასებასთან, სადაც გამოიყენება აღწერითი შკალა). ანალიზის ხარისხი დამოკიდებულია ციფრული მნიშვნელობის სიზუსტესა და სრულყოფილებაზე და გამოყენებული მოდელების სანდოობაზე. რაოდენობრივი შეფასება ხშირ შემთხვევაში გამოიყენებს წინა ინციდენტების მონაცემებს, რაც განაპირობებს იმ უპირატესობას, რომ იგი შესალოა დაკავშირებული იყოს პირდაპირ ინფორმაციული უსაფრთხოების მიზნებთან და ორგანიზაციისთვის პრობლემატურ საკითხებთან. უარყოფითი მხარე კი მდგომარეობს ახალი რისკების შესახებ მონაცემების სიმცირეში ან ინფორმაციული უსაფრთხოების სისუსტეში. რაოდენობრივი მიდგომის უარყოფითმა მხარემ შესაძლოა თავი იჩინოს იქ, სადაც ფაქტებით გამყარებული, შემოწმებადი მონაცემები არ არის ხელმისაწვდომი და ამდენად იქმნება რისკების შეფასების მნიშვნელობისა და სიზუსტის შესახებ მცდარი წარმოდგენა.

უარყოფითი შედეგები და ალბათობა, ასევე მათი გაერთიანება რისკის დონის გამოსავლენად შესაძლოა იცვლებოდეს რისკის ტიპის მიხედვით და ასევე იმ მიზნის შესაბამისად, რისთვისაც რისკების შეფასების შედეგი გამოიყენება. უარყოფითი შედეგებისა და ალბათობის ბუნდოვანება და ცვალებადობა გათვალისწინებული უნდა იყოს ანალიზისას და ინფორმაცია უნდა იცვლებოდეს ეფექტურად.

5.2.2 უარყოფითი შედეგების შეფასება

დაკვირვების ქვეშ მყოფი აქტივების იდენტიფიკაციის შემდეგ, უარყოფითი შედეგების შეფასებისას გათვალისწინებული უნდა იყოს ამ აქტივების მნიშვნელობა და ფასეულობა. ბიზნესზე გავლენის მნიშვნელობა შეიძლება გამოიხატოს ხარისხობრივად ან რაოდენობრივად, მაგრამ მისთვის ფულადი ფასეულობის მინიჭების ნებისმიერმა მეთოდმა შესაძლოა უზრუნველყოს მეტი ინფორმაცია გადაწყვეტილების მიღებისთვის და ამდენად ხელი შეუწყოს გადაწყვეტილების მიღების კიდევ უფრო ეფექტურ პროცესს.

აქტივების ფასეულობის დადგენა იწყება აქტივების კლასიფიკაციით, გათვალისწინებული უნდა იყოს მათი კრიტიკულობაც, ასევე აქტივების მნიშვნელობა

ორგანიზაციის ბიზნეს მიზნების შესრულების თვალსაზრისით. ფასეულობა დგინდება ორი საზომის გამოყენებით:

- აქტივის შეცვლის ღირებულება: ინფორმაციის აღდგენითი სამუშაოების და შეცვლის დანახარჯების დაფარვა (თუ საერთოდ შესაძლებელია), და
- ბიზნესის უარყოფითი შედეგები ან აქტივის საფრთხის ქვეშ დაყენება, როგორიცაა პოტენციური მავნე ბიზნეს და/ან იურიდიული ან მარეგულირებელი ხასიათის უარყოფითი შედეგები ინფორმაციის სააშკარაოზე გამოტანის, შეცვლის, ხელმიუწვდომლობის და/ან განადგურების შედეგად, და სხვა ინფორმაციული აქტივები.

ბიზნესზე გავლენის ანალიზი განსაზღვრავს ამგვარი ფასეულობის დადგენას. ღირებულება, რომელიც განსაზღვრულია ბიზნესისთვის უარყოფითი შედეგებით, ჩვეულებრივ მნიშვნელოვანწილად უფრო მაღალია ვიდრე უბრალოდ შეცვლის ღირებულება, რაც თავის მხრივ დამოკიდებულია ორგანიზაციისათვის აქტივის მნიშვნელობაზე საკუთარი ბიზნეს მიზნების მისაღწევად.

აქტივების ფასეულობის დადგენა წარმოადგენს ინციდენტების სცენარის გავლენის შეფასების ძირითად ფაქტორს, რადგანაც ინციდენტმა შესაძლოა გავლენა მოახდინოს ერთ ან რამდენიმე აქტივზე (მაგალითად, დამოკიდებული აქტივები), ან აქტივის მხოლოდ ნაწილზე. სხვადასხვა საფრთხეები და სუსტი წერტილები სხვადასხვა გავლენას ახდენენ აქტივებზე, მაგალითად: კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის დაკარგვა. უარყოფითი შედეგების შეფასება ამგვარად დაკავშირებულია აქტივების ფასეულობის დადგენასთან, რაც თავის მხრივ ეფუძნება ბიზნესზე გავლენის ანალიზს.
უარყოფითი შედეგები ან ბიზნესზე გავლენა შეიძლება განპირობებული იყოს შემთხვევის ან შემთხვევების შედეგების მოდელირებით, ან ექსპერიმენტული ან წარსული მონაცემების ექსტრაპოლაციის მეშვეობით.

უარყოფითი შედეგები შეიძლება გამოიხატოს ფულადი, ტექნიკური ან ადამიანური (სოციალური) გავლენის კრიტერიუმებით, ან სხვა ორგანიზაციისათვის მნიშვნელოვანი კრიტერიუმებით. ზოგიერთ შემთხვევაში ერთზე მეტი ციფრული საზომია საჭირო შედეგების განსასაზღვრად სხვადასხვა დროის, ადგილის, ჯგუფისა ან სიტუაციისათვის.
დროული და ფინანსური ხასიათის უარყოფითი შედეგები უნდა იზომებოდეს ერთნაირი მიდგომით, რაც გამოიყენება ასევე საფრთხის ალბათობისა და სუსტი წერტილის

შემთხვევაში. თანმიმდევრულობა (ლოგიკურობა) შენარჩუნებული უნდა იყოს რაოდენობრივი ან ხარისხობრივი მიდგომით.

5.2.3 ინციდენტის 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 წყროებისთვის: 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. მაგალითად, გეოგრაფიული მდებარეობების მიხედვით, ერთი და იმავე ტიპის

აქტივებისთვის შეიძლება არსებობდეს ცვალებადი საფრთხეები, ასევე ცვალებადია არსებული კონტროლის მექანიზმების ეფექტიანობა ასეთ სიტუაციაში.

5.2.4 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.

5.3 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.

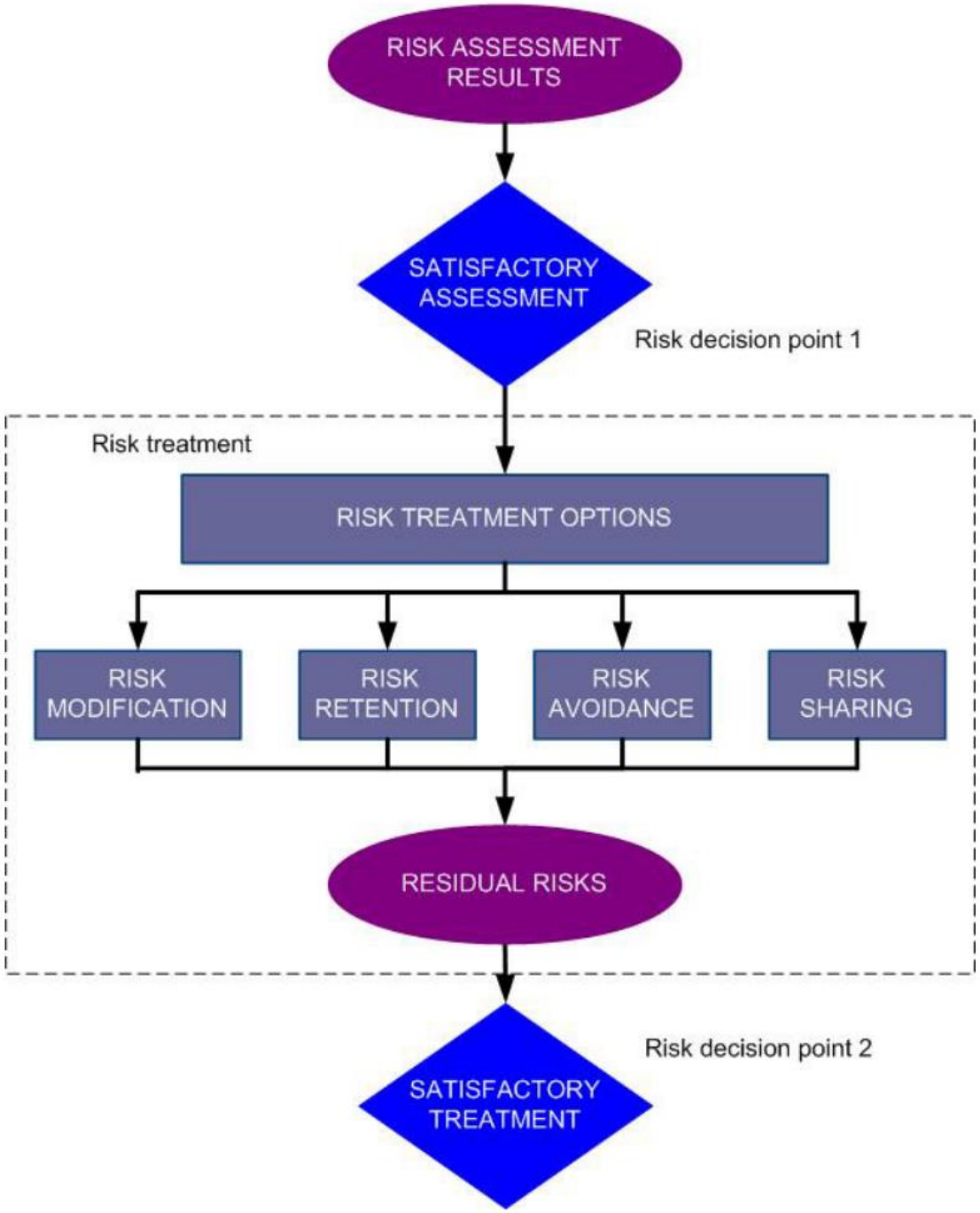
რისკების დონის დადგენა ითვალისწინებს რისკების ანალიზისას გამოვლენილ რისკებს, რათა მიღებული იქნას გადაწყვეტილებები სამომავლო ქმედებების განსახორციელებლად. გადაწყვეტილებები უნდა შეიცავდეს:

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

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

4. ინფორმაციული უსაფრთხოების რისკებთან მობყობა

არსებობს რისკებთან მობყრობის ოთხი შესაძლებლობა: რისკის შემცირება, რისკის მიღება, რისკის თავიდან არიდება და რისკის გადაცემა.


RISK ASSESSMENT RESULTS
SATISFACTORY ASSESSMENT
Risk decision point 1
Risk treatment
RISK TREATMENT OPTIONS
RISK MODIFICATION
RISK RETENTION
RISK AVOIDANCE
RISK SHARING
RESIDUAL RISKS
Risk decision point 2
SATISFACTORY TREATMENT

.

რისკებთან მობყოროობის შესაძლებლობების არჩევა უნდა ეფუძნებოდეს რისკების შეფასების შედეგებს, ამ შესაძლებლობების განხორციელების მოსალოდნელ დანახარჯებს და მათგან მიღებულ შესაძლო მოგებებს.

თუკი რისკების დიდი რაოდენობით შემცირება შესაძლებელია შედარებით დაბალი დანახარჯებით, მაშინ ასეთი შესაძლებლობა უნდა იქნას გამოყენებული.

ზოგადად, რისკების არასასურველი შედეგები საკმაოდ უნდა შემცირდეს. მენეჯერებმა უნდა განიხილონ იშვიათი, მაგრამ ამვდროულად საკმაოდ მძიმე რისკები. ასეთ შემთხვევებში, ეკონომიკური თვალსაზრისით გაუმართლებელი კონტროლის მექანიზმები უნდა დაინერგოს (მაგალითად, ბიზნესის უწყვეტობის კონტროლი მაღალი დონის რისკების დასაფარად).

რისკებთან მობყრობის მოცემული ოთხი ვარიანტი არ არის ურთიერთგამომრიცხავი. ზოგიერთ შემთხვევაში ორგანიზაციამ შეიძლება მიმართოს ამ შესაძლებლობების კომბინაციებს, და ამგავარდ მოიპოვოს უპირატესობები, მაგალითად: რისკების ალბათობის შემცირება, მათი უარყოფითი შედეგების შემცირება, ნებისმიერი რეაგირების გარეშე დარჩენილი რისკის გადაცემა ან მიღება.

რისკებთან მობყრობის ზოგიერთმა შემთხვევამ შესაძლოა ეფექტიანი რეაგირება მოახდინოს ერთ ან რამდენიმე რისკზე (მაგალითად, ინფორმაციული უსაფრთხოების ტრენინგი და ინფორმირებულობა). რისკებთან მობყრობის გეგმამ უნდა განსაზღვროს ის პრიორიტეტულობა, რომლის მიხედვითაც უნდა განხორციელდეს ინდივიდუალურ რისკებთან მობყრობა და მათი ვადები. პრიორიტეტების დადგენა ხდება სხვადასხვა მექანიზმების, მათ შორის რისკების რანგირებისა და სარგებლიანობის ანალიზის მეშვეობით. ორგანიზაციის მენეჯერების პასუხისმგებლობაში შედის ურთიერთშესაბამისობაში მოიყვანონ კონტროლის მექანიზმების დანერგვის ხარჯები და ბიუჯეტი.

არსებული კონტროლის მექანიზმების იდენტიფიკაცია განსაზღვრავს, რომ არსებული კონტროლის მექანიზმები აჭარბებენ მიმდინარე დონეს, გამომდინარე ხარჯების შედარებიდან, მათ შორის ტექნიკური მხარდაჭერის ხარჯები. თუ დაიგეგმება ზედმეტი ან უსარგებლო კონტროლის მექანიზმების ამოგდება (განსაკუთერბით თუ ასეთი კონტროლის მექანიზმები იყოს მაღალი საექსპლუატაციო ხარჯებით), მაშინ გათვალისწინებული უნდა იქნას ინფორმაციული უსაფრთხოებისა და ხარჯების ფაქტორები. იმდენად, რამდენადაც კონტროლის მექანიზმები შესაძლოა ერთმანეთზე ახდენდნენ გავლენას, ზედმეტი

კონტროლის მექანიზმების ამოდგებამ შეიძლება შეამციროს საერთო უსაფრთხოება. დამატებით უნდა აღინიშნოს, რომ ჭარბი კონტროლის მექანიზმების დატოვება შეიძლება უფრო იაფი იყოს ვიდრე მათი ამოგდება.

რისკებთან მოპყრობის შესაძლებლობების განხილვისას გათვალისიწნებული უნდა იქნას:

- თუ როგორ აღიქმება რისკი გავლენის ქვეშ მყოფი მხარეების მიერ;
- ამ მხარეებთან კომუნიკაციის ყველაზე მისაღები გზები.

გარემოს წინასწარი განსაზღვრა უზრუნველყოფს ირუდიული და მარეგულირებელი მოთხოვნების შესახებ ინფორმაციას, რომელსაც უნდა აკმაყოფილებდეს ორგანიზაცია. ყველა პირობა - ორგანიზაციული, ტექნიკური, სტრუქტურული და ა.შ. - რომლებიც დადგინდა გარემოს განსაზღვრის დროს, აუცილებლად უნდა იქნას გათვალისწინებული რისკებთან მოპყრობისას.

რისკებთან მოპყრობის გეგმის შედგენის შემდეგ აუცილებლად უნდა განისაზღვროს რეაგირების გარეშე დარჩენილი რისკები. ეს პროცესი მოიცავს რისკების შეფასების განახლებასა და განმეორებად ციკლს, რომლის დროსაც მხედველობაში უნდა იქნას მიღებული შემოთავაზებული რისკებთან მობყრობით გამოწვეული მოსალოდნელი შედეგები. თუ რეაგირების გარეშე დარჩენილი რისკები ჯერ კიდევ არ პასუხობენ ორგანიზაციის მიერ განსაზღვრულ რისკების მიღების კრიტერიუმებს, მაშინ საჭირო ხდება რისკებთან მობყრობის ციკლის ხელახლა გაშვება მანამ, სანამ უზრუნველყოფილი აქ იქნება რისკის მიღება.

6.1 რისკების შემცირება

შერჩეული უნდა იყოს შესაბამისი კონტროლის მექანიზმები რისკების შეფასებისა და მათთან მობყრობის მოთხოვნების დასაკმაყოფილებლად. ასევე გათვალისწინებული უნდა იქნას როგორც რისკების მიღების კრიტერიუმები, ასევე იურიდიული, მარეგულირებელი და სახელშეკრულებო მოთხოვნები. მხედველობაში უნდა იქნას მიღებული კონტორლის მექანიზმების დანერგვის ხარჯები და ვადები, ტექნიკური, გარემოს და კულტურული ასპექტები. სწორად შერჩეულმა ინფორმაციული უსაფრთხოების კონტროლის მექანიზმებმა შესაძლებელია შეამციროს სისტემის მფლობელობის ხარჯები.

კონტროლის მექანიზმებმა ზოგადად შეიძლება უზრუნველყოს ერთი ან მეტი შემდეგი ტიპის დაცვის მექანიზმები: შესწორება, განადგურება, თავიდან არიდება, გავლენის

შემცირება, აღმოჩენა, აღდგენა, მონიტორინგი და ინფორმირებულობა. კონტროლის მექანიზმის შერჩევისას მნიშვნელოვანია მათი შეძენის, დანერგვის, ადმინისტარციული, ოპერაციული, მონიტორინგისა და მხარდაჭერის ხარჯების შეფასება დასაცავი აქტივების ფასეულობასთან მიმართებაში. უფრო მეტიც, გათვალისწინებული უნდა იყოს რისკების შემცირების შედეგად მიღებული საინვესტიციო მოგებები და გარკვეული კონტროლის მექანიზმების მიერ ახალი ბიზნეს შესაძლებლობების პოტენციალი. ყურადღება უნდა გამახვილდეს სპეციალიზირებულ უნარ-ჩვევებზე, რაც აუცილებელია ახალი კონტროლის მექანიზმების განსაზღვრისა და დანერგვისათვის ან არსებული კონტროლის მექანიზმების შეცვლისთვის.

არსებობს მრავალი პირობა, რამაც შესაძლოა გავლენა იქონიოს კონტროლის მექანიზმების შერჩევაზე. ტექნიკური ხასიათის შეზღუდვები, როგორებიცაა ფუნქციონირების მოთხოვნები, მართვადობა (ოპერაციული მხარდაჭერის მოთხოვნები) და თავსებადობის საკითხები, რომლებმაც შესაძლოა ხელი შეუშალონ კონკრეტული კონტროლის მექანიზმების გამოყენებას ან ბიძგი მისცენ ადმიანური ფაქტორით გამოწვეულ შეცდომას, რაც გამოიხატება როგორც კონტროლის მექანიზმის გაბათილებაში, უსაფრთხოების შესახებ მცდარი წარმოდგების შექმნაში, ასევე კონტროლის მექანიზმის არ ქონით რისკების გაზრდაში (მაგალითად: შესაბამისი ტრენინგის გარეშე მოითხოვო კომპლექსური პაროლები, რაც იძულებულს ხდის მომხმარებლებს ფურცელზე ჩაიწერონ პაროლები). ასევე შესაძლებელია, რომ კონტროლის მექანიზმმა გავლენა იქონიოს წარმადობაზე. მენეჯერებმა უნდა მიიღონ ისეთი გადაწყვეტილება, რომელიც დააკმაყოფილებს წარმადობის მოთხოვნებს და ამავდროულად უზრუნველყოფს ადექვატურ ინფორმაციულ უსაფრთხოებას. ამ ეტაპის შედეგი გახლავთ შესაძლო კონტროლის მექანიზმების ჩამონათვალი მათი დანახარჯების, სარგებელის და დანერგვის პრიორიტეტებთან ერთად.

კონტროლის მექანიზმების შერჩევისა და მათი დანერგვის დროს სხვადასხვა შეზღუდვები უნდა იქნას გათვალისწინებული. ტიპიურად:

- ვადები;
- ფინანსური შეზღუდვები;
- ტექნიკური შეზღუდვები;
- ოპერაციული;
- კულტურული;

- ეთიკური;
- გარემო პირობებისა;
- იურიდიული შეზღუდვები;
- ადვილად გამოყენებადი
- საკადრო შეზღუდვები;
- არსებული და ახალი კონტროლის მექანიზმების ინტეგრირების შეზღუდვები.

6.2 რისკების დაშვება

თუ რისკის დონე შეესაბამება რისკის მიღების კრიტერიუმებს, მაშინ არ არის აუცილებელი დამატებითი კონტროლის მექანიზმების დანერგვა და შესაძლებელია რისკის დაშვება (ანუ არ მოხდეს მასზე დამატებითი ქმედება).

6.3 რისკის თავიდან აცილება

როდესაც იდენტიფიცირებული რისკები მიჩნეულია როგორც საკმაოდ მაღალი დონის, ან რისკებთან მოპყრობის სხვა ვარიანტების განხორციელების ხარჯები მეტია სარგებელზე, შესაძლოა აუცილებელი გახდეს გადაწყვეტილების მიღება რისკების მთლიანად აღმოფხვრის თაობაზე, რისთვისაც საჭიროა დაგეგმილი ან არსებული ქმედების ან ქმედებათა ნაკრების შეწყვეტა, ან იმ პირობების შეცვლა, რომლებშიც აღნიშნული ქმედების განხორციელება ხდება. მაგალითად, ბუნებრივი მოვლენებით გამოწვეული რისკების შემთხვევაში უფრო მისაღებია, ხარჯების დაზოგვის თვალსაზრისით, ინფორმაციის დამამუშავებელი მოწყობილობების ფიზიკური გადაადგილება უსაფრთხო ან კონტროლირებად ადგილას.

6.4 რისკების გადაცემა

რისკის გადაცემა გულისხმობს გადაწყვეტილებას ცალკეული რისკის გარე მხარისათვის გაზიარების შესახებ. რისკის გადაცემამ შეიძლება შექმნას ახალი რისკები ან გამოიწვიოს არსებულის, უკვე აღმოჩენილის შეცვლა. ამდენად აუცილებელი ხდება დამატებითი რისკის აღმოფხვრა.

რისკების გადაცემა შეიძლება განხორციელდეს დაზღვევის მეშვეობით, რაც მოიცავს უარყოფითი შედეგების დადგომი შემთხვევაში დახმარებას, ან ქვე-კონტრაქტორი პარტნიორის მეშვეობით, რომელიც ახორციელებს ინფორმაციული სისტემის მონიტორინგს

და მიმართავს სასწრაფო ზომებს თავდასხმის შესაჩერებლად მანამ, სანამ იგი გამოიწვევს გარკვეული დონის ზარალს.

აღსანიშნავია, რომ შესაძლებელია პასუხისმგებლობების გადაცემა რისკის მართვის მიზნით, მაგრამ შეუძლებელია მოსალოდნელი ზეგავლენით გამოწვეული ვალდებულებების გადაცემა. მომხმარებლები, როგორც წესი, უარყოფით გავლენას მიაწერენ ორგანიზაციის შეცდომას.

5. ინფორმაციული უსაფრთხოების რისკების მიღება

რისკებთან მობყრობის გეგმა აღწერს თუ როგორ უნდა მოვებყროთ რისკებს, რათა დაკმაყოფილებული იყოს რისკების მიღების კრიტერიუმები. პასუხისმგებელმა მენეჯერებმა უნდა გადახედონ და დაამტკიცონ შემოთავაზებული რისკებთან მობყრობის გეგმები და რეაგირების გარეშე დარჩენილი რისკები, შესაბამისად დაარეგისტრირონ დამტკიცებასთან დაკავშირებული ნებისმიერი პირობები.

რისკების მიღების კრიტერიუმები არ არის მხოლოდ იმ ფაქტის განსაზღვრა, კონკრეტული რისკი ზღვარს ქვემოთ იმყოფება თუ ზემოთ, იგი უფრო კომპლექსური ხასიათისაა.

ზოგიერთ შემთხვევაში კონკრეტული რისკის დონე შეიძლება არ აკმაყოფილებდეს რისკების მიღების კრიტერიუმებს, რადგან გამოყენებული კრიტერიუმები არ ითვალისწინებენ გავრცელებულ მიდგომებს. მაგალითად, შესაძლოა ამტკიცებდნენ, რომ საჭიროა რისკების მიღება მისი თანმდევი მიმზიდველი სარგებელის გამო, ან რისკების შემცირების მაღალი ხარჯების გამო. ამგავრი ვითარებები მიუთითებენ, რომ რისკების მიღების კრიტერიუმები არაადექვატურია და შეძლებისდაგვარად უნდა იქნას გამოსწორებული. თუმცა, ყოველთვის არ არის შესაძლებელი რისკების მიღების კრიტერიუმების დროული შესწორება. ასეთ შემთხვევაში, გადაწყვეტილების მიმღები პირები იძლებულნი არიან თანხმობა განაცხადონ ისეთ რისკებზე, რომლებიც არ აკმაყოფილებენ მიღების სტანდარტულ კრიტერიუმებს. თუ ეს აუცილებელია, გადაწყევტილების მიმღებმა პირმა დეტალური კომენტარი უნდა გაუწეროს რისკს და თან დაურთოს მიღებული გადაწყვეტილების არგუმენტირება, თუ რატომ მოხდა რისკების მიღების სტანდარტული კრიტერიუმების უგულვებელყოფა.

6. ინფორმაციული უსაფრთხოების რისკების შესახებ ინფორმირებულობა

რისკების შესახებ ინფორმირება წარმოადგენს შეთანხმების მიღწევას იმის თაობაზე, თუ როგორ უნდა მოხდეს რისკების მართვა რისკების შესახებ ინფორმაციის გაცვლისა და გაზიარების მეშვეობით გადაწყვეტილების მიმღებ და სხვა დაინტერესებულ პირებს შორის. ინფორმაცია შეიცავს რისკების არსებობას, რისკის შინაარს, ფორმას, ალბათობას, სირთულეს, დამუშავებას და მასზე თანხმობადობას, ასევე სხვა ფაქტორებსაც.

დაინტერესებულ პირებს შორის ეფექტური კომუნიკაცია მნიშვნელოვანია იმ თვალსაზრისით, რომ ამან შეიძლება მნიშვნელოვანი გავლენა იქონიოს მისაღებ გადაწყვეტილებებზე. კომუნიკაციამ უნდა უზრუნველყოს ის, რომ რისკების მართვის განხორციელებაზე პასუხისმეგებელ პირებს და დაინტერესებულ პირებს ესმოდეთ გადაწყვეტილებების მიღების საფუძველი და კონკრეტული ქმედებების საჭიროება. კომუნიკაცია არის ორმიმართულებიანი.

რისკის აღქმა იცვლება დაინტერესებული პირების საჭიროებების, პრობლემატური საკითხების, კონცეფციების სხვადასხვაგვაროვნების მიხედვით, რადგანაც დაკავშირებული არიან რისკებთან ან განსახილველ საკითხებთან. დაინტერესებული პირები სავარაუდოდ გამოთქვამენ მოსაზრებებს რისკების მიღების შესახებ, რაც დაფუძნებული იქნება მათ მიერ რისკის აღქმაზე. განსაკუთრებით მნიშვნელოვანია დაინტერესებული პირების მიერ რისკების აღქმა და ამ აღქმისგან მიღებული სარგებელი იყოს აღმოჩენილი და დოკუმენტირებული და ასევე ძირითადი მიზეზები ნათლად გასაგები და რეაგირებული.

რისკების კომუნიკაცია უნდა განხორციელდეს რათა მიღწეული იქნას შემდეგი:

- ორგანიზაციის რისკების მართვის შედეგების გარანტიების უზრუნველყოფა;
- რისკების შესახებ ინფორმაციის შეგროვება;
- რისკების შეფასების შედეგების გაზიარება და რისკებთან მობრყობის გეგმის წარმოდგენა;
- ინფორმაციული უსაფრთხოების დარღვევის ხდომილებისა და მისი უარყოფითი შედეგების თავიდან აცილება და შემცირება, რაც შესაძლოა გამოწვეული იყოს გადაწყვეტილების მიმღებ და დაინეტრესებულ პირებს შორის საერთო შეხედულებების არ არსებობის გამო;
- გადაწყვეტილების მიღების მხარდაჭერა;

- ინფორმაციული უსაფრთხოების შესახებ ახალი ცოდნის მიღება;
- სხვა მხარეებთან კოორდინაცია და ინციდენტების უარყოფითი შედეგების შემცირების მიზნით საპასუხო ქმედებების დაგეგმვა;
- გადაწყვეტილების მიმღები და დაინტერესებული პირებისთვის პასუხისმგებლობის გაცნობიერება რისკების დადგომის შემთხვევაში;
- ინფორმირებულობის გაუმჯობესება.

ორგანიზაციამ უნდა შეიმუშაოს რისკების შესახებ ინფორმირების გეგმები როგორც სტანდარტული ოპერაციების, ასევე განსაკუთრებული ვითარებებისთვის. ამდენად, რისკების შესახებ ინფორმირება უწყვეტი პროცესია.

გადაწყვეტილების მთავარ მიმღებ და დაინტერესებულ პირებს შორის კოორდინაცია მიღწეული უნდა იქნას შესაბამისი კომიტეტის შექმნით, სადაც განიხილება რისკების, მათი პრიორიტეტების და შესაბამისი მობყრობის, რისკების მიღების შესახებ.

მნიშვნელოვანია თანამშრომლობა ორგანიზაციის ისეთ სტრუქტურულ ერთეულებთან, როგორებიცაა, მაგალითად, საზოგადოებასთან ურთიერთობის ან ინფორმირებულობის სამსახური, რათა უზრუნველყოფილი იყოს რისკების ინფორმირებულობასთან დაკავშირებული ყველა ამოცანის კოორდინაცია.

7. ინფორმაციული უსაფრთხოების რისკების მონიტორინგი და მიმოხილვა

9.1 რისკ ფაქტორების მონიტორინგი და მიმოხლივა

რისკები არ არის უცვლელი. საფრთხეები, სუსტი წერტილები, ალბათობა ან უარყოფითი შედეგები შეიძლება შეიცვალოს მოულოდნელად, წინასწარი მინიშნების გარეშე. ამდენად საჭიროა მუდმივი მონიტორინგი ამ ცვლილებების აღმოსაჩენად. ეს შეიძლება განხორციელდეს გარე სერვისების მიერ, ინფორმაცია ახალი საფრთხეებისა და სუსტი წერტილების შესახებ შესაძლოა მივიღოთ მესამე მხარეს მიერ.

ორგანიზაციამ უნდა უზრუნველყოს შემდეგი ფაქტორების უწყვეტი მონიტორინგი:

- რისკების მართვის ჩარჩოში დამატებული ახალი აქტივები;
- აქტივების ფასეულობის საჭირო ცვლილება, მაგალითად რომელიც შეიცვალა ბიზნეს მოთხოვნების შედეგად;
- შეუფასებელი, აქტიური საფრთხეები როგორც ორგანიზაციის შეგნით ასევე მის გარეთ;

- სისუსტეებით სარგებლობის გაზრდა შესაძლოა გამოწვეული იყოს როგორც ახალი ისე არსებული სისუსტეების ხარისხის მატებით;
- აღმოჩენილი სუსტი წერტილების მიერ გამოყენებადი სუსტი წერტილების განსაზღვრა, რომლებიც შეიძლება გამოყენებული იქნან ახალი ან ხელახლა გაჩენილი საფრთხეების მიერ;
- შეფასებული საფრთხეების, სუსტი წერტილების და რისკების მომატებული (გაზრდილი) გავლენა ან მისი უარყოფითი შედეგები მთლიანად, რაც იწვევს რისკის დაუშვებელ დონეს;
- ინფორმაციული უსაფრთხოების ინციდენტები.

ახალმა საფრთხეებმა, სუსტმა წერტილებმა ან ცვლილებებმა შესაძლოა გაზარდოს წარსულში დაბალ რისკად შეფასებული რისკების რაოდენობა. თუ რისკები არ იყოფა დაბალ ან დასაშვებ კატეგორიებად, მაშინ მათთან მობყრობა უნდა მოხდეს 9-ე პუნქტში განხილული ერთი ან მეტი ვარიანტების გამოყენებით.

ფაქტორები, რომლებიც გავლენას ახდენენ საფრთხეების ალბათობასა და მათ უარყოფით შედეგებზე, შეიძლება შეიცვალოს, ისევე როგორც ის ფაქტორები, რომლებიც გავლენას ახდენენ რისკებთან მობყრობის სხვადასხვა ვარიანტების შესაბამისობასა და ღირებულებაზე. ძირითადი ცვლილებები, რომლებიც გავლენას ახდენენ ორგანიზაციაზე, აუცილებლად უნდა იქნას განხილული. რისკების მონიტორინგი რეგულარულად უნდა მეორდებოდეს და რისკებთან მობყრობის შერჩეული ვარიანტები პერიოდულად უნდა გადაიხედოს.

რისკის მონიტორინგის შედეგი შესაძლოა წარმოადგენდეს შემავალ რესურსს სხვა რისკის განხილვისთვის. ორგანიზაციამ რეგულარულად უნდა მიმოიხილოს ყველა რისკი და ასევე თუ როდის იჩენს თავს ძირითადი მნიშვნელოვანი ცვლილებები

9.2 რისკების მართვის მონიტორინგი, განხილვა და გაუმჯობესება

მუდმივი მონიტორინგი და მიმოხილვა აუცილებელია, რათა უზრუნველყოფილი იქნას გარემოს, რისკების შეფასების შედეგების და რისკებთან მობყრობის, ასევე მართვის გეგმის აუცილებლობის შენარჩუნება ვითარებების შესაბამისად.

ორგანიზაციამ უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების რისკების მართვის პროცესისა და მასთან დაკავშირებული ქმედებების შესატყვისობა მოცემულ მომენტში არსებულ ვითარებებთან. ნებისმიერი პროცესისა თუ ქმედებების შეთანხმებული

გაუმჯობესების შესახებ უნდა ეცნობოს შესაბამის მენეჯერებს, რათა უზრუნველყოფილი იქნას რისკების ან რისკების ელემენტების აღმოჩენა, მათი სათანადოდ შეფასება და ასევე გატარებული იქნას საჭირო ღონისძიებები და მიღებული იქნას შესაბამისი გადაწყვეტილებები რისკების რეალისტურ აღქმაზე, გაცნობიერებაზე და მათზე რეაგირების მოხდენაზე.

დამატებით უნდა აღინიშნოს, რომ ორგანიზაციამ რეგულარულად უნდა აკონტროლოს რისკებისა და მისი ელემენტების საზომი კრიტერიუმების აქტუალურობა ბიზნეს მიზნებთან, სტრატეგიებთან და პოლიტიკებთან მიმართებაში, ასევე ადექვატურად გათვალისწინებული უნდა იყოს ბიზნესის გარემოს ცვლილებები ინფორმაციული უსაფრთხოების რისკების მართვის პროცესში. მონიტორინგი და მიმოხილვა უნდა ეხებოდეს:

- იურიდიულ და გარემოებრივ პირობებს;
- კონკურენტულ გარემოს;
- რისკების შეფასებებისადმი მიდგომას;
- აქტივების ფასეულობას და კატეგორიებს;
- გავლენის კრიტერიუმებს;
- რისკების დონის დადგენის კრიტერიუმებს;
- რისკების მიღების კრიტერიუმებს;
- მფლობელობის ხარჯებს;
- საჭირო რესურსებს.

ორგანიზაციამ უნდა უზრუნველყოს, რომ რისკების შეფასების და რისკებთან მობყრობის რესურსები მუდმივად ხელმისაწვდომია რისკების გადახედვის, ახალი ან სახეცვლილი საფრთხეებისა ან სუსტი წერტილების რეაგირებისთვის, და ასევე მენეჯმენტისთვის რჩევის მიცემა.

რისკების მართვის მონიტორინგმა შესაძლოა გამოიწვიოს გამოყენებული ხელსაწყოების, მეთოდოლოგიის ან მოწყობილობების შეცვლა ან დამატება, რაც დამოკიდებულია:

- აღმოჩენილ ცვლილებებზე;
- რისკების შეფასების რიგითობაზე;
- ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის ამოცანაზე (მაგალითად: ბიზნეს უწყვეტობა, ინციდენტებისადმი მოქნილობა, შესაბამისობა);

- ინფორმაციული უსაფრთხოების რისკების მართვის პორცესის ობიექტზე) (მაგალითად: ორგანიზაცია, ბიზნეს ერთეული, ინფორმაციული პროცესი, მისი ტექნიკური განხორციელება, გამოყენება, ინტერნეტთან კავშირი).

დასკვნა

რისკი წარმოადგენს ორგანიზაციებში წარმოქმნილი გაურკვეველი სიტუაციების ძირითად მიზეზს, ამიტომაც კომპანიების უმეტესობა დიდ ძალისხმევას ხარჯავენ რისკების იდენტიფიცირებასა და მართვაზე, რათა თავიდან აიცილონ მოსალოდნელი ნეგატიური შედეგები, რომლებიც პირდაპირ გავლენას ახდენენ ბიზნეს გარემოზე. რისკების მართვა ორგანიზაციებს ეხმარება მეტი დამაჯერებლობით მოახდინონ სამომავლო ბიზნეს გადაწყვეტილებების მიღება. არსებული მოსალოდნელი რისკების ცნობადობა, საშუალებას აძლევს ორგანიზაციებს ადექვატურად იმოქმედონ და დაიცვან თავი აღნიშნული რისკების წარმოქმნის შემთხვევაში.

როდესაც ინფორმაციული უსაფრთხოების რისკები სათანადოდ არ არის შეფასებული და შესაბამისი პრევენციული კონტროლები არ არის დანერგილი, ხდება ორგანიზაციაში არსებული ფასეული ინფორმაციის უსაფრთხოების დარღვევა და თავს იჩენს ინფორმაციის გაჟონვა, რასაც ორგანიზციები სავალალო შედეგებამდე მიჰყავს. სავალალო შედეგებში იგულისხმება: უზარმაზარი ფინანსური ჯარიმები, საკანონმდებლო დარღვევები, რეპუტაციის შელახვა და სხვა.

ინფორმაციული უსაფრთხოების რისკების მართვის პროცესს სასიცოცხლო მნიშვნელობა გააჩნია ნებისმიერი ორგანიზაციისთვის, რადგან მის გარეშე წარმოუდგენელია სამომავლო მისიისა თუ გეგმების განსაზღვრა.

ნაშრომში განხილული ინფორმაციის უსაფრთხოების მართვის ძირითადი მეთოდების ანალიზის შედეგად გამოიკვეთა ინფორმაციული უსაფრთხოების რისკების წარმოქმნის მიზეზები და მათი აღმოფხვრის მეთოდები.

შედეგად შემუშავდა რეკომენდაციები რომლებიც შეიცავენ ინფორმაციას ინფორმაციული უსაფრთხოების რისკების იდენტიფიცირების, შეფასების, მოჰყრობისა და მიღების გზებისა და მეთოდების შესახებ.

გამოყენებული ლიტერატურა

ISO/IEC 27005: 2008 – INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - INFORMATION SECURITY RISK MANAGEMENT

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - SPECIAL PUBLICATION 800-39 – MANAGIN INFORMATION SECURITY RISK

COSO – ENTERPRISE RISK MANAGEMENT — RISK ASSESSMENT IN PRACTISE

SYNGRESS – IT SECURITY MANAGEMENT (ISBN: 978-1-59749-227-0)

SANS INSTITUTE – INFOSEC READING ROOM - INFORMATION RISK & RISK MANAGEMENT