Scientific and Practical Cyber Security Journal (SPCSJ) 6(3): 25-34 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

ინფორმაციული უსაფრთხოების რისკების მართვა: სტანდარტები და გამოწვევები

INFORMATION SECURITY RISK MANAGEMENT: STANDARDS AND CHALLENGES

აკაკი შეყელაძე, საქართველოს ტექნიკური უნივერსიტეტი
Akaki Shekeladze, Georgian Technical University

ანოტაცია: კიბერსივრციდან მომდინარე საფრთხეებისა და მსოფლიოს სხვადასხვა წერტილში განუწყვეტლივ მიმდინარე კიბერშეტევების პარალელურად, უფრო და უფრო დიდი მნიშვნელობა ენიჭება ინფორმაციის დაცვას. ინფორმაციისთვის შექმნილისაფრთხეებისა და რისკების მართვა შეუძლებელია შესაბამისი მიდგომისა და მეთოდოლოგიის გამოყენების გარეშე. მოცემულ სტატიაში მიმოვიხილავთ ინფორმაციული უსაფრთხოების რისკების მართვის არსს, მის საჭიროებას და პროცესის ადმინისტრირების შესაძებლობებს ისეთი საერთაშორისო სტანდარტების გამოყენებით, როგორიცაა ISO, NIST, COBIT და სხვა. ასევე, შევეხებით შესაბამის გამოწვევებს და მათთან გამკლავების შესაძლო საშუალებებს.
საკვანძო სიტყვები: *ინფორმაციული უსაფრთხოება, ინფორმაციული უსაფრთხოების რისკი, ინფორმაციული აქტივი, კიბერსაფრთხეები, ISO27005, NIST RMF*

ABSTRACT: ALONG WITH CYBER THREATS AND CYBER ATTACKS CONTINUOUSLY OCCURRING IN ANY PART OF THE WORLD, INFORMATION SECURITY GAINS MORE AND MORE IMPORTANCE. THREATS AND RISKS REGARDING INFORMATION CANNOT BE ADDRESSED WITHOUT ADEQUATE APPROACH AND STRUCTURED METHODOLOGIES. THIS PAPER WILL COVER INFORMATION SECURITY MANAGEMENT CONCEPT, ITS NECESSITY AND MANAGEMENT OF THE PROCESS VIA USING INTERNATIONAL STANDARDS, INCLUDING ISO, NIST, COBIT, ETC. WE WILL ALSO COVER CHALLENGES IN THIS REGARD AND WAYS TO TACKLE WITH THEM.

KEYWORDS*: Information Security, Information Security Risk, Information Asset, Cyber Threats, ISO27005, NIST RMF*

შესავალი

ხანძარი, წყალდიდობა, ძლიერი ყინვა, აფეთქება და ვულკანის ამოფრქვევა იმ მოვლენათა არასრული ჩამონათვალია, რაც საუკუნეების განმავლობაში კაცობრიობის მიერ ფიზიკური ინფრასტრუქტურის წინაშე მდგარ საფრთხეებად მიიჩნეოდა. თუმცა, 21-ე საუკუნეში, თითოეულ მათგანს უკვე ინფორმაციისა და ინფორმაციული სისტემების საფრთხედაც მიიჩნევენ და ისინი განგაშის საფუძველსაც ხშირად ქმნიან. ამას ემატება უშუალოდ კიბერსივრცეში არსებული საფრთხეები, როგორიცაა შპიონაჟი, ფინანსური თაღლითობები, საბოტაჟი, ინფორმაციის მოპარვა, დაკარგვა და სხვა.

მართლაც, ინფორმაციის მნიშვნელობამ დღეს უმაღლეს ნიშნულს მიაღწია, რითაც ის გახდა ყველაზე კრიტიკული აქტივი, რომელსაც ორგანიზაცია იღებს, ამუშავებს, ცვლის და ინახავს.

ორგანიზაციის ინფორმაციულ სისტემებში არსებული პერსონალური და კონფიდენციალური ინფორმაცია მოწყვლადია როგორც ზემოაღნიშნული ფიზიკური, ასევე კიბერსაფრთხეების წინაშე, რის გამოც ინფორმაციული უსაფრთხოების რისკების მართვას უფრო და უფრო დიდი მნიშვნელობა ენიჭება როგორც კერძო, ასევე საჯარო სექტორში.

ინფორმაციული უსაფრთხოების რისკების მართვა არის უსაფრთხოების წინაშე მდგარი საფრთხეების იდენტიფიცირების, შეფასებისა და მართვის უწყვეტი პროცესი. ის წარმოადგენს ორგანიზაციის მიერ რისკების მართვის განუყოფელ, მნიშვნელოვან ნაწილს, ვინაიდან მის საფუძველზე უნდა იყოს შეთავაზებული უსაფრთხოების ადეკვატური გადაწყვეტები ინფორმაციული სისტემებისა და მონაცემებისთვის.

სხვადასხვა საერთაშორისო სტანდარტები, როგორიცაა ISO, NIST წარმოგვიდგენენ ინფორმაციული უსაფრთხოების რისკის მართვის მეთოდოლოგიას, რომელთაც მსოფლიოში ფართოდ იყენებენ და მათგან მიღებულ სარგებელს დადებითად აფასებენ. თუმცა, ამ სტანდარტების დანერგვას სჭირდება გარკვეული რესურსი და ძალისხმევა, დაწყებული მმართველი რგოლის მხარდაჭერით და დასრულებული ფინანსური ინვესტიციით.

მოცემულ სტატიაში მიმოვიხილავთ ინფორმაციული უსაფრთხოების რისკების მართვის საჭიროების მიზეზებს, მის სარგებელს, რისკების მართვის პროცესს აღიარებული სტანდარტების მიხედვით და ამ პროცესში წარმოშობილ გამოწვევებს ქართული რეალობის კონტექსტში.

რა არის ინფორმაციული უსაფრთხოების რისკი?

ინფორმაციული უსაფრთხოების რისკი, საერთაშორისო სტანდარტების თანახმად, განიმარტება როგორც შესაძლებლობა იმისა, რომ კონკრეტული საფრთხე, ინფორმაციული აქტივ(ებ)ის სისუსტის გამოყენებით, ზიანს მიაყენებს აქტივს ან აქტივთა ჯგუფს და აღნიშნულით ზიანი მიადგება ორგანიზაციას.

ცხადია, იმ ეპოქაში, როდესაც კიბერთაღლითობას უამრავი მსხვერპლი ჰყავს, ერთ კიბერშეტევას კი შეუძლია ორგანიზაციას ასი ათასობით დოლარის ზარალი მოუტანოს, რეპუტაცია შეულახოს და, უფრო მეტიც, ინფრასტრუქტურა ფიზიკურად გაანადგუროს, საჯარო არეულობა გამოიწვიოს, ან ეროვნული უსაფრთხოების საკითხი კითხვის ნიშნის ქვეშ დააყენოს, საფრთხეების პრევენციის საჭიროებაზე ყურადღების გამახვილების საჭიროება აღარ დგას.

მართლაც, შეუძლებელია 21-ე საუკუნეში კერძო თუ საჯარო დაწესებულება ფუნქციონირებდეს შესაბამისი საფრთხეების იდენტიფიცირებისა და რისკების შეფასების გარეშე. ინფორმაციას და ინფორმაციულ სისტემებს შეიძლება საფრთხე შეუქმნას ფიზიკურმა ზიანმა (ხანძარი, ნგრევა, ყინვა), ბუნებრივმა პროცესებმა (წყალდიდობა, მიწისძვრა), ძირითადი სერვისების შეფერხებამ (კონდიცირების სისტემა დაზიანება, კვების შეწყვეტა), ინფორმაციის კომპრომეტირებამ (შპიონაჟი, დეზინფორმაცია, არასანქცირებული შეღწევა სისტემებში), ტექნიკურმა გაუმართაობებმა (მოწყობილობის გაუმართაობა, პროგრამის შეფერხებით მუშაობა), მესამე პირის არაავტორიზებულმა ქმედებებმა თუ სხვა.

ინფორმაციული უსაფრთხოების რისკების მართვა კი გულისხმობს როგორც ამ საფრთხეების, ასევე ამ საფრთხეების შესაბამისი მოწყვლადობის იდენტიფიცირებას. მაგალითისთვის, თუკი საფრთხედ მივიჩნევთ შპიონაჟს და ორგანიზაციას ქსელის დაუცველი არქიტექტურა აქვს, ამ შემთხვევაში, მან იცის, რომ ეს პრობლემა დაუყოვნებლივ გადასაჭრელია.

რაში გვჭირდება ინფორმაციული უსაფრთხოების რისკების მართვა?

ინფორმაციული უსაფრთხოების რისკების მართვას აქვს რიგი სარგებელი, კერძოდ [1]:

- ის ორგანიზაციას უჩენს კონკურენტულ უპირატესობას, ზრდის მის რეპუტაციას და მის მიმართ ნდობას, რაც საბოლოოდ ბიზნესის შედეგებზე აისახება;
- ის ამცირებს ინფორმაციული უსაფრთხოების ინციდენტის მოხდენის ალბათობას, ვინაიდან ორგანიზაციას აქვს ინფორმაცია შესაბამის საფრთხეზე და ამ საფრთხის თავიდან ასარიდებელ საშუალებებს იყენებს;
- ის საშუალებას აძლევს ორგანიზაციას მიიღოს სწორი გადაწყვეტილება, რომელიც ემყარება რეალურ რისკებს;
- ის ზოგავს ორგანიზაციის ხარჯებს ეფექტური და ეფექტიანი კონტროლის მექანიზმების დანერგვით;
- ის არის საქმიანობის უწყვეტობის წინაპირობა;
- ის ორგანიზაციას აძლევს სრულ ხედვას ინფორმაციული აქტივების წინაშე მდგარი გამოწვევების შესახებ.

უნდა აღინიშნოს ისიც, რომ მხოლოდ ამ პროცესის წარმატებით განხორციელების შემთხვევაში შეუძლია ორგანიზაციას იყოს სრულად თავსებადი ისეთ საერთაშორისო სტანდარტებთან, როგორიც არის ISO27001, NIST და სხვა. მეტიც, ინფორმაციული უსაფრთხოების რისკების მართვა ISO სტანდარტის ერთ-ერთი ძირითადი მოთხოვნაა და მის გარეშე ორგანიზაცია შესაბამის სერტიფიკატს ვერ მოიპოვებს.

რისკების მართვა სტანდარტების გამოყენებით

ინფორმაციული უსაფრთხოების რისკების მართვისთვის მნიშვნელოვანია განისაზღვროს მეთოდოლოგია. თითოეული ორგანიზაცია განსხვავდება თავისი შიდა და გარე გარემოს მიხედვით, სტრატეგიული მიზნებით, ამოცანებით, სტრუქტურით, ინფორმაციული სისტემებით, ქსელის არქიტექტურით. შესაბამისად, ზოგი საჭიროებს საბაზისო მიდგომას, ზოგი კი უფრო სიღრმისეული მეთდოლოგიის გამოყენებას. არსებობს ამ პროცესის მართვის რამდენიმე საერთაშორისოდ აღიარებული სტანდარტი, თუმცა რომელიმე მათგანის გამოყენება ვალდებულება ნამდვილად არ არის. ორგანიზაციას შეუძლია შექმნას საკუთარიც. მთავარი ისაა, რომ მეთოდოლოგია იყოს შესატყვისი ორგანიზაციასთან, მის მიზნებსა და სამუშაო პროცესებთან. წარმოგიდგენთ ყველაზე გავრცელებული მეთოდოლოგიებიდან რამდენიმეს [2]:

OCTAVE:
2001 წელს შექმნილი OCTAVE Allegro კონცენტირდება ინფორმაციულ აქტივებზე. ორგანიზაციის კრიტიკული აქტივები იდენტიფიცირდება და ფასდება მასთან დაკავშირებულ სხვა აქტივებთან მიმართებაში. ამ მეთდოლოგიის დადებით მხარედ მიიჩნევა მორგებისა და დოკუმენტირების შესაძლებლობა, ხოლო უარყოფით მხარედ მისი სირთულე.

FAIR:
FAIR არის რისკის ანალიზის რაოდენობრივი შეფასების მოდელი. ის სპეციალიზდება ფინანსურ შედეგებზე და არ მოიაზრებს ხარისხობრივ შეფასებას. მისი დადებითი მხარეა საფრთხეების, მოწყვლადობებისა და რისკების დონეების დაყოფა, ხოლო უარყოფითი მხარეა სირთულე.

COBIT:
„კონტროლის მექანიზმები ინფორმაციისა და ტექნოლოგიებისთვის“, რომელიც შეიქმნა ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ, ფოკუსირდება კონტროლის მექანიზმების იდენტიფიცირებაზე [3]. ის შედგება 37 პროცესისგან, რომლითაც იმართება და კონტროლდება ინფორმაცია და მასთან დაკავშირებული ტექნოლოგიები. COBIT არ გვთავაზობს რისკების შეფასების მეთდოლოგიას, მაგრამ ქმნის ინფორმაციული ტექნოლოგიების ორგანიზაციის საფუძველს. COBIT მოიცავს ინფორმაციული ტექნოლოგიების რისკების შემცირების კონტროლის მექანიზმებს.

ვინაიდან „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი ავალდებულებს კრიტიკული ინფორმაციული სისტემის სუბიექტებს, რომ მათი ინფორმაციული უსაფრთხოების პოლიტიკა იყოს თავსებადი სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO), აშშ-ის სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტის (NIST) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილ სტანდარტებსა და მოთხოვნებთან [4], ნაკლებად სავარაუდოა, რომ საქართველოს კრიტიკული ინფორმაციული სისტემის რომელიმე სუბიექტის ინფორმაციული უსაფრთხოების რისკების მართვის პროცესმა ამ სტანდარტებს გვერდი აუაროს.

NIST RMF:
NIST საერთაშორისო სტანდარტის რისკების მართვის ჩარჩო (RMF) არის სტრუქტირებული პროცესი, რომელიც მოიცავს ინფორმაციული უსაფრთხოებისა და რისკების მართვის პროცედურებს. კერძოდ, რისკების მართვა ხორციელდება შემდეგი ეტაპებით [5] (ნახ.1):

ნახაზი 1. *NIST სტანდარტის რისკების მართვის ჩარჩო*

- მომზადება - პირველ ეტაპზე ხდება იმგვარი პროცედურების განხორციელება ორგანიზაციაში, რითაც ის მოემზადება საკუთარი უსაფრთხოების რისკების მართვისთვის RMF ჩარჩოს გამოყენებით. ეს, მაგალითისთვის, მოიცავს როლებისა და პასუხისმგებლობების განსაზღვრას;
- კატეგორიზება - ხდება მოვლენების შეფასება ინფორმაციის ხელმისაწვდომობას, მთლიანობასა და კონფიდენციალურობასთან მიმართებაში, საფრთხეების კლასიფიცირება და შესაბამისი პირების ინფორმირება;
- შერჩევა/აღმოჩენა - ორგანიზაცია აღრიცხავს მოვლენებს, რომლებიც უქმნის საფრთხეს ინფორმაციის უსაფრთხოებას;
- დანერგვა - ამ ეტაპზე ინერგება კონტროლის მექანიზმები შესაბამისი რისკების საპასუხოდ;
- შეფასება - ამ დროს ფასდება დანერგილი კონტროლის მექანიზმების ეფექტურობა და სისწორე, რომ ის პასუხობს უსაფრთხოების პრობლემებს და შესაბამის მოთხოვნებს;
- ავტორიზება - მენეჯმენტის მხრიდან ხდება უსაფრთხოების რისკებისთვის დანერგილი კონტროლის მექანიზმების დამოწმება;
- მონიტორინგი - მოიცავს აღწერილი ეტაპების მონიტორინგის უწყვეტ პროცესს.

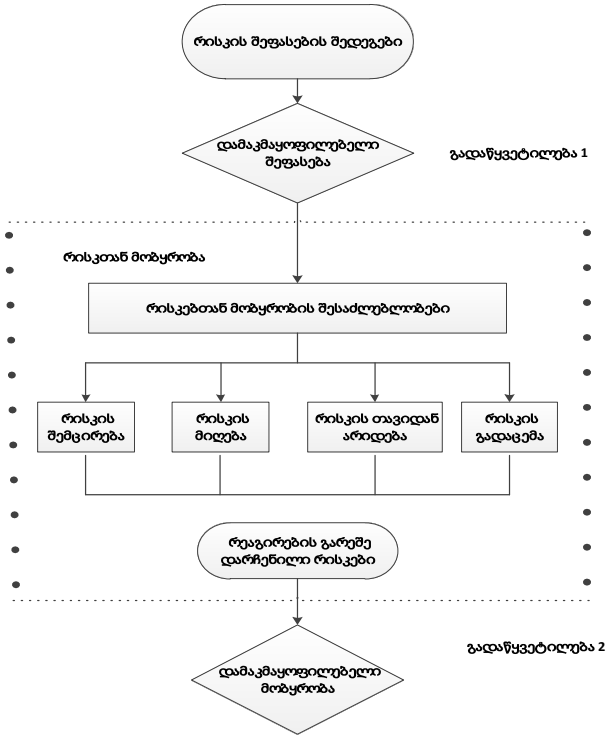
ISO 27001/27005:
ISO ინფორმაციული უსაფრთხოების სტანდარტის თანახმად, ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი შედგება შემდეგი პროცესებისგან:

- ორგანიზაციული გარემოს განსაზღვრა - მოიცავს საჭირო კრიტერიუმების დადგენას ინფორმაციული უსაფრთხოების რისკების მართვის გამოყენების სფეროსა და ჩარჩოების განსაზღვრას, ასევე ორგანიზაციული სტრუქტურის შექმნას, რომელიც განახორციელებს ინფორმაციული უსაფრთხოების რისკების მართვას. ამ პროცესში ხდება შიდა და გარე პროცესების, შეზღუდვების, საჭიროებების, მიზნების გათვალისწინება;
- რისკების შეფასება - მოიცავს რისკის ანალიზს (შედგება რისკების იდენტიფიცირებისგან და რისკების მიახლოებითი შეფასებასისგან) და რისკის დონის დადგენას;
- რისკებთან მოპყრობა - მოიცავს არჩევენს რისკებთან მოპყრობის შესახებ (ნახ.2);
- რისკების შესახებ ინფორმირება;
- რისკების მონიტორინგი და განხილვა.

რისკების შეფასებისთვის პირველ ეტაპს წარმოადგენს რისკების იდენტიფიკაცია. ამ პროცესში შემავალ ინფორმაციას წარმოადგენს ორგანიზაციის ინფორმაციული აქტივები. თითოეული აქტივისთვის უნდა დადგინდეს შესაბამისი საფრთხე. საფრთხე, წარმოშობის წყაროს მიხედვით, შეიძლება იყოს შიდა, გარე და ბუნებრივი. აუცილებელია მოწყვლადობების იდენტიფიკაცია, რომელი სისუსტეებით სარგებლობაც წარმოადგენს საფრთხეს აქტივებისთვის ან ორგანიზაციისთვის.

შემდეგ ხდება რისკების მიახლოებითი შეფასება. ის შეიძლება ჩატარდეს დეტალურობის სხვადასხვა დონეზე და დამოკიდებულია აქტივის კრიტიკულობაზე, წინა გამოცდილებაზე (ინციდენტებზე), ცნობილ მოწყვლადობებზე. რისკების მიახლოებითი შეფასება შეიძლება იყოს როგორც ციფრული (რაოდენობრივი), ასევე თვისობრივი (ხარისხობრივი). მიახლოებით შეფასებული რისკი წარმოადგენს ინციდენტის სცენარის და მისი უარყოფითი შედეგების ალბათობის კომბინაციას.

შემდეგ ხდება გადაწყვეტილების მიღება რისკებთან მოპყრობასთან დაკავშირებით, სადაც წარმოდგენილია შემდეგი ვარიანტები:



ნახაზი 2. *რისკებთან მოპყრობის ქმედება*

1. რისკების შემცირებისთვის (შემსუბუქება) საჭიროა კონტროლის მექანიზმის სწორად შერჩევა. კონტროლის მექანიზმების შერჩევის და მათი დანერგვის დროს უნდა მოხდეს შეზღუდვების გათვალისწინება, როგორიცაა: ტექნიკური, სამართლებრივი, საკადრო, ფინანსური, დროითი და სხვა.
2. თუ რისკის დონე შეესაბამება რისკის მიღების კრიტერიუმებს, მაშინ არ არის აუცილებელი დამატებითი კონტროლის მექანიზმის დანერგვა და ხდება რისკის დაშვება.
3. რისკის თავიდან არიდება გამართლებულია, როდესაც რისკებთან მოპყრობის სხვა ვარიანტების განხორციელების დანახარჯები მეტია სარგებელზე და ასეთ დროს ხდება რისკის მთლიანად აღმოფხვრა.
4. რისკის გადაცემა გულისხმობს გადაწყვეტილებას გარკვეული რისკების მესამე მხარისთვის გაზიარების შესახებ. ეს შეიძლება იყოს ქვეკონტრაქტორი კომპანია ან დაზღვევა.

აღსანიშნავია, რომ ISO27001 სტანდარტით მოცემული ოთხი ვარიანტი არ არის ურთიერთგამომრიცხავი, ვინაიდან გარკვეულ შემთხვევებში გამართლებულია მათი კომბინაციაც.

როგორც ვნახეთ, სხვადასხვა სტანდარტების ანალიზის შედეგად დგინდება [6], რომ პირველი ეტაპი უნდა იყოს ინფორმაციული აქტივების იდენტიფიცრება. ეს აქტივები შეიძლება იყოს სერვერები, ქსელური მოწყობულობები, სისტემები, კომპიუტერული ტექნიკა და ნებისმიერი მოწყობილობა, რომელშიც ინახება, მუშავდება და გაიცვლება

ინფორმაცია. აქტივი შეიძლება იყოს დოკუმენტიც, ორგანიზაციაში დასაქმებული თანამშრომლებიც.

მეორე ეტაპი არის საფრთხეების იდენტიფიცირება აქტივებთან მიმართებაში. საფრთხე არის უცნობი ინციდენტის პოტენციური მიზეზი, რომელმაც შეუძლია ზიანი მოუტანოს ორგანიზაციას. ეს შეიძლება იყოს ქურდობა, მავნე პორგრამული უზრუნველყოფა, ბუნებრივი მოვლენები, ინფორმაციის გამჟღავნება და სხვა.

მესამე ეტაპი არის მოწყვლადობების იდენტიფიცირება. ეს შეიძლება იყოს სარეზერვო ასლების არარასებობა, დაშიფვრის არარსებობა, არასაიმედო პაროლები, დაბალი კიბერცნობიერება, ქსელური დაცვის ეკრანის შეუსაბამობა, ბიზნესის უწყვეტობის გეგმის არქონა და სხვა.

მეოთხე ეტაპი არის საფრთხის ალბათობის დადგენა. ალბათობის დადგენისთვის შესაძლებელია სტატისტიკის, ანგარიშების გამოყენება. ალბათობის დონეები შეიძლება იყოს როგორც რაოდენობრივი, ასევე თვისობრივი (მაგ.: დაბალი, საშუალო, მაღალი).

მეხუთე ეტაპზე ალბათობა უნდა დავუკავშიროთ გავლენას. შესაძლოა, ალბათობა იყოს დაბალი, ხოლო საფრთხის სიმძიმე ძალიან მაღალი, ან პირიქით და ეს შემთხვევები განსხვავებულ სურათს იძლევა. სწორედ ალბათობისა და გავლენის ურთიერთშეკავშირება გვაძლევს საშუალებას შევაფასოთ რისკი. რისკის შეფასებისთვის, ასევე შეგვიძლია გამოვიყენოთ შკალა, ან შევაფასოთ ის ხარისხობრივად.

წარმოგიდგენთ რისკების შეფასების მაგალითს (ცხრ.1), სადაც ვიყენებთ რაოდენობრივ მეთოდს და ალბათობასა და გავლენას ვაფასებთ 1-დან 5 ქულამდე. ბოლო სვეტში ვიღებთ რისკის შეფასების შედეგს.

აქტივი	საფრთხე	მოწყვლადობა	რისკის მფლობელი	გავლენა (1-5)	ალბათობა (1-5)	რისკი
სერვერი (ტექნიკური უზრუნველყოფა)	კვების წყვეტა	უწყვეტი კვების წყაროს (UPS) არარსებობა	ინფორმაციული უსაფრთხოების მენეჯერი	4	2	**6**
	ხანძარი	ცეცხლმაქრის არარსებობა		5	3	**8**
ხელშეკრულება (დოკუმენტი)	წვდომის მიღება არაავტორიზებული პირის მიერ	ხელშეკრულება დატოვებულია მაგიდაზე	აღმასრულებელი დირექტორი	4	4	**8**
	ხანძარი	ხანძრისგან დამცავი სისტემის არარსებობა		4	3	**7**

სისტემის ადმინისტრატორი (ადამიანი)	ავარია	სხვამ არავინ იცის პაროლი	დეპარტამენტის უფროსი	5	3	**8**

ცხრილი 1. *რისკების შეფასება*

ბოლო ეტაპზე ხდება გადაწყვეტილების მიღება რისკებთან მოპყრობასთან დაკავშირებით. სხვადასხვა სტანდარტების მიხედვით, ეს შეიძლება იყოს [7]: რისკის შემცირება (შემსუბუქება), რისკის თავიდან არიდება, რისკის გადაცემა, რისკის მიღება. წარმოგიდგენთ შესაბამის მაგალითს (ცხრ.2):

აქტივი	საფრთხე	მოწყვლადობა	რისკთან მოპყრობა	დანერგვის საშუალება
სერვერი	ხანძარი	ცეცხლმაქრის არარსებობა	რისკის გადაცემა	დაზღვევის პოლისის შესყიდვა
პორტატული კომპიუტერი	არაავტორიზებული პირის მიერ წვდომა	არასაიმედო პაროლი	რისკის შემცირება	პაროლების წესის შემუშავება
სისტემის ადმინინისტრატორი	სამსახურის დატოვება	შემცვლელი კადრის არარსებობა	რისკის შემცირება	სისტემის მეორე ადმინისტრატორის დასაქმება

ცხრილი 2. *რისკებთან მოპყრობა*

გამოწვევები

ინფორმაციული უსაფრთხოების რისკების მართვა, ცხადია, საკმაოდ კომპლექსური პროცესია, რომელიც მოითხოვს გარკვეულ ძალისხმევას ორგანიზაციის თითოეული რგოლისგან. რისკების მართვის პროცესის ჩავარდნის მიზეზები ხშირად ხდება [8]:

- მმართველი რგოლის მხარდაჭერის არარსებობა: ინფორმაციული უსაფრთხოება იმართება მენეჯმენტის გადაწყვეტილებების საფუძველზე. მმართველი რგოლის მხარდაჭერის არარსებობა იწვევს რესურსების ფლანგვას, არასწორ შეფასებებს, რაც საბოლოოდ რისკების შეფასების შედეგების უგულებელყოფამდე მიგვიყვანს;
- ინფორმაციული უსაფრთხოების პოლიტიკის/პროცედურების არარსებობა: შესაბამისი დოკუმენტების არარსებობა მიგვიყვანს რისკების შეფასების არასისტემურ მიდგომასთან;
- არასწორი მართვა: მიუხედავად რისკების მართვის მნიშვნელობისა, ზოგჯერ ის არ იმართება, როგორც პროექტი და არ განიხილება ოპერაციად. რისკების მართვის პროცესის გაუთვალისწინებლობა გადაწყვეტილების მიღების, დაგეგმვის და აღსრულების პროცესში იწვევს რესურსების არამიზნობრივ ხარჯვას;
- აქტივების მფლობელი დაუდგენელია: შეუძლებელია ინფორმაციული უსაფრთხოების რისკი შეფასდეს აქტივების მფლობელის ჩართულობის გარეშე. როდესაც აქტივებს არ გააჩნიათ მფლობელი, მის წინაშე მდგარი საფრთხეების და შესაბამისი მოწყვლადობების ჯეროვნად მოკვლევა და შემდეგ ინფორმაციული უსაფრთხოების რისკების მართვის პროცესში გამოყენება შეუძლებელია;

- რისკების მართვის მეთოდოლოგიის შერჩევა: ზოგიერთი ორგანიზაცია რისკების მართვისთვის იყენებს რამდენიმე მეთოდოლოგიას, რითაც მართვის პროცესი კიდევ უფრო ჩახლართული ხდება.

ასევე, მივიჩნევ, რომ ამ პროცესში გამოწვევას წარმოადგენს კადრების დეფიციტი და კვალიფიკაციის ნაკლებობა. ინფორმაციული უსაფრთხოების რისკების მართვა კომპლექსური პროცესია და მასზე პასუხისმგებელი პირი უნდა ფლობდეს შესაბამის ცოდნას. ამის მიუხედავად, საქართველოში ჯერ კიდევ მრავლად შევხვდებით კრიტიკული ინფორმაციული სისტემის სუბიექტებს, რომელთაც არ ჰყავთ ინფორმაციული უსაფრთხოების მენეჯერი ან ინფორმაციულ უსაფრთოებაზე პასუხისმგებელი პირი.

დასკვნა

ამრიგად, არის თუ არა ორგანიზაცია კრიტიკული ინფორმაციული სისტემის სუბიექტი, მისთვის ნათელი უნდა იყოს ის პრობლემები, რომლებიც აღმოცენდება ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის არარსებობის შემთხვევაში. თანამედროვე სამყაროში არ არსებობს ორგანიზაცია, რომელიც არ ფლობს პერსონალურ და კონფიდენციალურ ინფორმაციას, რის გამოც გარდაუვალი ხდება ინფორმაციულ ტექნოლოგიებთან დაკავშირებულ გამოწვევებზე რეაგირება.

ინფორმაციული უსაფრთხოების რისკების მართვა არ წარმოადგენს ინფორმაციული უსაფრთხოების მენეჯერის ერთპიროვნულ პასუხისმგებლობას. პირიქით, ეს არის მაღალი რგოლის მენეჯმენტის მიერ გასააზრებელი და მისაღები გადაწყვეტილება, რომელშიც ორგანიზაციას გარკვეული ინვესტიცია დაჭირდება. თუმცა, ჩადებული რესურსი შეუძლებელია ჩაითვალოს ფუჭად, ვინაიდან რისკების შემცირებით სუბიექტი მნიშვნელოვნად ამცირებს ინფორმაციული უსაფრთხოების ინციდენტების ალბათობას, თავიდან ირიდებს რეპუტაციულ და ფინანსურ ზიანს, რაც, საბოლოო ჯამში, ხაზს უსვამს გაღებული ძალისხმევის სისწორესა და ეფექტურობას.

იმისთვის, რომ რისკების მართვის პროცესთან დაკავშირებით სუბიექტი არ შეხვდეს ჩვენ მიერ განხილულ პრობლემებს, მან საწყის ეტაპზე შეიძლება გაითვალისწინოს ISO 27001 Academy-ს მიერ წარმოდგენილი რისკების მართვასთან დაკავშირებულ რჩევები [9]:

- სწორი მეთდოლოგიის არჩევა - საჭიროა სწორი მეთოლოგიის არჩევა და საჭიროებისამებრ მისი გამარტივება;
- სწორი საშუალების არჩევა - რისკების მართვის პროცესში რეკომენდებულია პროგრამული უზრუნველყოფის გამოყენება. ზოგიერთ შემთხვევაში, ჩახლართულ პროგრამას სჯობს Microsoft Office Excel-ის ფორმის გამოყენება;
- საჭირო პერსონალის ჩართვა - საჭიროა მმართველობითი რგოლის ჩართვა ამ პროცესებში, ვინაიდან სტრუქტურული დანაყოფების უფროსებმა იციან, რის უკან იმალება პრობლემები;
- მიზანი არ არის სრულყოფილება - რისკების მართვა უწყვეტი პროცესია. პირველ ეტაპზე, შეუძლებელია ყველა საფრთხის გამოვლენა და აღწერა.

რაც შეეხება კონკრეტულ სტანდარტებს, მხოლოდ ორგანიზაციაზეა დამოკიდებული ის, თუ რომელ მიდგომას აირჩევს ინფორმაციული უსაფრთხოების რისკების მართვისთვის და ის იცვლება საქმიანობის სფეროს, მასშტაბების, ამოცანების, საჭიროებებისა და

შესაძლებელობების მიხედვით. თუმცა, მნიშვნელოვანია სტატიაში განხილული მეთოდოლოგიების გათვალისწინებაც, ვინაიდან მოცემულმა სტანდარტებმა უკვე მრავალწლიანი აპრობაცია გაიარეს და მათი ეფექტურობის ხარისხი კითხვის ნიშნის ქვეშ კიბერუსაფრთხოების ექსპერტებს ნამდვილად არ დაუყენებიათ.

გამოყენებული ლიტერატურა

1. James, Dave. n.d. “Seven Solid Benefits of Information Risk Management.” Ascentor. Accessed July 17, 2022. https://insights.ascentor.co.uk/blog/2012/02/seven-solid-benefits-of-information-risk-management
2. Refile, Olivia. 2020. “Information Security Risk Management: A Comprehensive Guide.” Linford & Company LLP. Accessed July 17, 2022. https://linfordco.com/blog/information-security-risk-management
3. Simplelearn. 2022. “What is COBIT? Understanding the COBIT Framework.” Accessed July 17, 2022. https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article
4. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი
5. NIST. n.d. “Risk Management Framework for Information Systems and Organizations.” Accessed July 17, 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
6. PECB. n.d. “Information Security Risk Management.” Accessed July 17, 2022. https://pecb.com/pdf/articles/61-pecb-information-security-risk-management.pdf
7. Infosec. 2018. “Risk treatment options, planning and prevention.” Accessed July 17, 2022. https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/
8. Walid Al-Ahmad, Bassil Mohammad. 2013. “Addressing Information Security Risks by Adopting Standards.” INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE. Accessed July 17, 2022. https://www.ijiss.org/ijiss/index.php/ijiss/article/view/20
9. Kosutic, Dejan. n.d. “ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide.” Accessed July 17, 2022. https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/