ინფორმაციის დაცვისა და უსაფრთხოების რისკების მართვა ეკონომიკური გლობალიზაციის პირობებში (თსუ-ის მაგალითზე)

შორენა დავითაია

პროფესორის ასისტენტი ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

ზურაბ თოფურია

საინფორმაციო ტექნოლოგიების მხარდაჭერის განყოფილების უფროსი სპეციალისტი, საქართველოს სახელმწიფო ელექტროსისტემა

თანამედროვე მსოფლიოში გლობალიზაციამ მკვეთრად შეცვალა ინფორმაციული ტექნოლოგიების მიმართულებები. აუცილებელი გახდა მსოფლიო ინფორმაციული სივრცის ფორმირება და სათანადო დაცვის სისტემების დანერგვა.

ორგანიზაციისთვის ინფორმაცია მნიშვნელოვანი აქტივია, რომელსაც ესაჭიროება დაცვა. ინფორმაციული უსაფრთხოება არის ინფორმაციის დაცვა ბიზნეს-პროცესების უწყვეტობის უზრუნველსაყოფად. ინფორმაციული უსაფრთხოების სისტემა უნდა დაინერგოს და ფუნქციონირებდეს საქმიანობის მართვის სხვა პროცესებთან ერთად.

მოცემული სტატიის მიზანია ინფორმაციული ტექნოლოგიების უსაფრთხოებასთან დაკავშირებული რისკების მართვის აუცილებლობის ჩვენება. მოცემული მიზნიდან ჩამოყალიბდა შემდეგი ამოცანები:

- საქართველოში არსებული ინფორმაციული უსაფრთხოების სტანდარტების ანალიზი;
- ინფორმაციული უსაფრთხოების რისკების მართვის განხილვა საქართველოში არსებული კანონმდებლობის მიხედვით;
- რისკების მართვის ტექნოლოგიის შესწავლა;
- კვლევის ობიექტის (ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის) მაგალითზე არსებული ინფორმაციული უსაფრთხოების რისკების მართვის შესწავლა და რეკომენდაციები მის გასაუმჯობესებლად.

საქართველოში არსებობს კანონი ინფორმაციული უსაფრთხოების შესახებ. ამ კანონის მიზანია, ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, დააწესოს საჯარო და კერძო სექტორების უფლება-მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, აგრეთვე განსაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები.

საქართველოში ინფორმაციის დაცვისა და უსაფრთხოების რისკების მართვის შესახებ არ მოიპოვება სტატისტიკური მონაცემები, მაგრამ არსებობს მონაცემთა გაცვლის სააგენტოს მიერ დამტკიცებული ინფორმაციული უსაფრთხოების რისკების მართვის საერთაშორისო სტანდარტი მგს 27001:2011.

აღნიშნული სტანდარტი წარმოადგენს ორგანიზაციაში ინფორმაციული უსაფრთხოების რისკების მართვის სახელმძღვანელოს, კერძოდ მხარს უჭერს ინფორმაციული უსაფრთხოების მართვის სისტემების (იუმს) მოთხოვნებს ISO 27001:2011-ის (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები) თანახმად.

ნებისმიერი ორგანიზაციის ინტერესებში შედის ინფორმაციული უსაფრთხოების რისკების მართვა. ინფორმაციული უსაფრთხოების რისკების მართვისადმი სისტემური მიდგომა აუცილებელია ორგანიზაციის საჭიროებების იდენტიფიცირებისათვის ინფორმაციული უსაფრთხოების მოთხოვნების თვალსაზრისით და ეფექტური ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) შესაქმნელად. ეს მიდგომა უნდა შეესაბამებოდეს ორგანიზაციულ გარემოს. უსაფრთხოების მიმართულებით გამოსაყენებელმა ძალისხმევამ ეფექტურად და დროულად უნდა განახორციელოს საპასუხო ქმედებები. ინფორმაციული უსაფრთხოების რისკების მართვა უნდა იყოს ინფორმაციული უსაფრთხოების მართვის განუყოფელი ნაწილი და უნდა გამოიყენებოდეს იუმს-ის როგორც დანერგვის, ასევე მისი ფუნქციონირების ეტაპებზე.

ინფორმაციული უსაფრთხოების რისკების მართვა უნდა იყოს უწყვეტი პროცესი. პროცესმა უნდა დაადგინოს ორგანიზაციული გარემო, შეაფასოს და გადაჭრას რისკები დადგენილი გეგმის მიხედვით და გასცეს რეკომენდაციები და გადაწყვეტილებები დასანერგად.

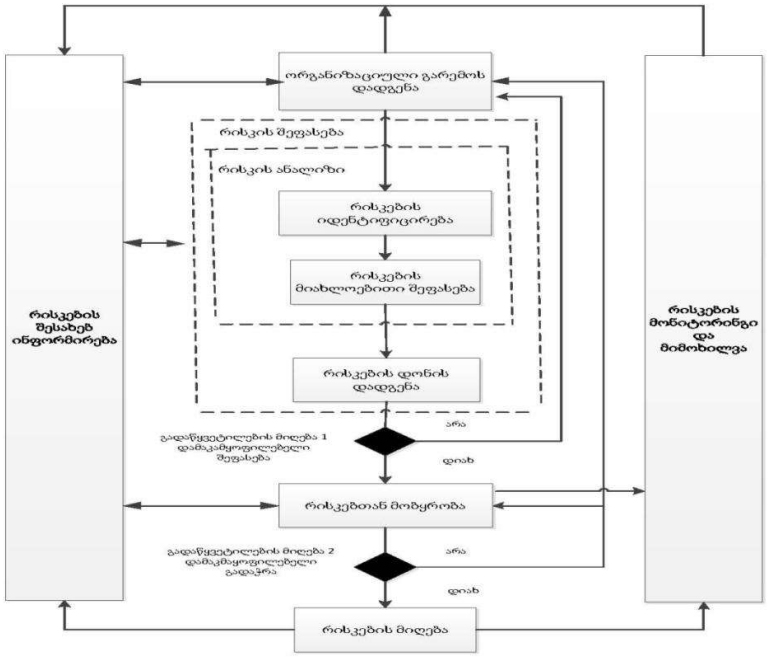
ინფორმაციული უსაფრთხოების რისკების მართვამ ხელი უნდა შეუწყოს:

- რისკების იდენტიფიცირებას;
- რისკების შეფასებას იმისდა მიხედვით, თუ რა შედეგები მოჰყვება მათ ბიზნესთან მიმართებაში და მათი ხდომილების ალბათობა;
- ამ რისკების დადგომის ალბათობას და მათ შესაძლო შედეგებს, მათ შესახებ ინფორმირებულობის არსებობას;
- რისკებთან მობყროობის პრიორიტეტულობის დადგენას;
- რისკების შემცირების შესახებ ქმედებების პრიორიტეტულობას;
- რისკების მართვასთან დაკავშირებული გადაწყვეტილებების მიღებაში ჩართული დაინტერესებული პირები და მათი ინფორმირებულობა რისკების მართვის სტატუსის შესახებ;
- რისკებთან მოპყრობის 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.

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

სქემა 1-ზე ნაჩვენებია რისკების მართვის პროცესი.



სქემა 1 გვიჩვენებს ინფორმაციული უსაფრთხოების მართვის პროცესს, რომელიც შეიძლება იყოს განმეორებადი ხასიათის რისკების შეფასებისას და/ან რისკებთან მოპყრობის 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 ორგანიზაციის 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 მოპყრობა. 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 (იხილეთ სქემა 1, გადაწყვეტილების მიღება 1).

რისკებთან მოპყრობის ეფექტიანობა დამოკიდებულია რისკის შეფასების შედეგებზე. შესაძლებელია რისკებთან მოპყრობამ 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 მოპყრობა (იხილეთ სქემა 1, გადაწყვეტილების მიღება 2).

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 მოპყრობას შორის, ასევე შესაბამის მენეჯერებსა და საოპერაციო თანამშრომლებს შორის. რისკებთან მოპყრობამდე კი ძალზე მნიშვნელოვანია ინფორმაცია იდენტიფიცირებული რისკის შესახებ, რათა მოხდეს ინციდენტის მართვა, რამაც შესაძლოა ხელი შეუწყოს პოტენციური ზიანის შემცირებას. მენეჯერების 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.

იუმს-ის მიერ განსაზღვრული გარემო, რისკების შეფასება, რისკებთან მოპყრობის გეგმის შემუშავება და რისკების მიღება გახლავთ „დაგეგმვის—ფაზის ნაწილი. იუმს-ის მიერ განსაზღვრული „აღსრულების—ფაზა გულისხმობს, რომ რისკების დასაშვებ დონეზე დაყვანასთან დაკავშირებული საჭირო ქმედებები და კონტროლის მექანიზმები დანერგილია რისკებთან მოპყრობის გეგმის თანახმად. იუმს-ის მიერ განსაზღვრული „შემოწმების—ფაზა გულისხმობს, რომ მენეჯერებმა უნდა განსაზღვრონ რისკების შეფასების და მათთან მოპყრობის გადასინჯვის საჭიროება ინციდენტებისა და ცვლილებების გათვალისწინებით. „ქმედების— ფაზაში სრულდება ნებისმიერი საჭირო ქმედება, მათ შორის ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი.

ქვემოთ მოყვანილი ცხრილი აჯამებს ინფორმაციული უსაფრთხოების რისკების მართვის ყველა საჭირო ქმედებას იუმს-ის მიერ განსაზღვრული ოთხივე ფაზისათვის:

ცხრილი 1 - იუმს-ის და ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის შესაბამისობა[1]

იუმს-ის პროცესი	**ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი**
დაგეგმვა	გარემოს განსაზღვრა რისკების შეფასება რისკებთან მობყრობის გეგმის შემუშავება

[1] საქართველოს იუსტიციის სამინისტრო. ინფორმაციული უსაფრთხოების რისკების მართვა. 28 ნოემბერი, 2011 წელი.

	რისკების მიღება
აღსრულება	რისკებთან მობყრობის გეგმის დანერგვა
შემოწმება	რისკების უწყვეტი მონიტორინგი და მიმოხილვა
ქმედება	ინფორმაციული უსაფრთხოების მართვის პროცესის მხარდაჭერა და გაუმჯობესება

თბილისის სახელმწიფო უნივერსიტეტის ინფორმაციული ტექნოლოგიების დეპარტამენტის მიდგომა ინფორმაციის დაცვისა და უსაფრთხოების რისკების მართვის მიმართ ძალიან საინტერესოა, მიზნებიც და გეგემებიც სწორი მიმართულებითაა არჩეული. მაგრამ, ვფიქრობთ მომავალში ამ კუთხით შესაძლებელია მათი გაუმჯობესება.

გამოკითხვის შედეგად დადგინდა, რომ სასურველია გადაიხედოს უნივერსიტეტის მომხმარებლებისთვის სერვისების მიწოდების მიმართ დამოკიდებულება. კერძოდ, კლასტერული სისტემის არარსებობამ შეიძლება გამოიწვიოს ერთერთი სერვერის მწყობრიდან გამოსვლისას მასზე არსებული სერვისებზე წვდომის შეფერხება.

კლასტერი არის სერვერების ერთობლიობა, დაკავშირებული ერთმანეთთან მაღალსიჩქარიანი კომუნიკაციური ნაკადებით, რომელიც მომხმარებლისთვის წარმოადგენს ერთიან ინფორმაციულ რესურსს. კლასტერის სისტემის არსებობა საშუალებას იძლევა მომხმარებელს შეუფერხებლად მიეწოდოს სერვისები. ამასთან კლასტერის ტექნოლოგიის გამოყენება ხელს უწყობს მონაცემების სინქრონიზაციას და დატვირთვების განაწილებას ამ სისტემაში შემავალ ყველა სერვერზე. კლასტერის სისტემის დანერგვა ერთი-ორად გაზრდის უნივერსიტეტში არსებული ინფორმაციული სისტემის მდგრადობას.

გამოკითხვის შედეგად ასევე გაირკვა, რომ უნივერსიტეტს ამჟამად ალტერნატიული ინტერნეტის ხაზი არ გააჩნია. ასეთი ხაზის უქონლობა დაკავშირებულია დიდ რისკებთან, ვინაიდან პროვაიდერის შიგნით ხარვეზების შექმნისას ან ოპტიკურ-ბოჭკოვანი კაბელის ფიზიკური დაზიანებისას, გაითიშება ინტერნეტი მთელ უნივერსიტეტში, მის კორპუსებსა და დაქვემდებარებულ კვლევით ცენტრებში. ალტერნატიული ინტერნეტის ხაზის შემოყვანა შეამცირებს უნივერსიტეტის სამუშაო გარემოში შეფერხებების რისკებს. ერთი ხაზის გამორთვის შემთხვევაში, მომხმარებელი ავტომატურად გადაერთვება ალტერნატიულ ხაზზე, ისე რომ ვერც შეიტყობს მთავარი ხაზის მწყობრიდან გამოსვლას.

ასევე მონაცემთა ბაზის უსაფრთხოება შესაბამისად არ არის უზრუნველყოფილი და არსებობს ბაზებში გარედან არასანქცირებული შეღწევის რისკები. რისკების თავიდან ასაცილებლად აუცილებელია მკაცრად განისაზღვროს მომხმარებლის უსაფრთხოების ქვევით ჩამოთვლილი ყველა პირობა:

1. ქსელური უსაფრთხოების მოწყობილობაზე გაიწეროს ის ჰოსტები, საიდანაც ავტორიზებულ მომხმარებელს აქვს უფლება მიწვდეს მონაცემთა ბაზას;
2. ქსელური მოწყობილობის საშუალებით გაიფილტროს „არასასურველი—ტრაფიკი გარედან;
3. მონაცემთა ბაზის სერვერზე მკაცრად გაკონტროლდეს მომხმარებელი, რომელსაც აქვს წვდომა მონაცემთა ბაზის ფაილებთან;
4. განისაზღვროს მონაცემთა ბაზის „მესაკუთრე—(owner);
5. განისაზღვროს მონაცემთა ბაზაზე პასუხისმგებელი პირი (ბაზის ადმინისტრატორი);
6. განისაზღვროს მომხმარებლების უფლებები, რომელთაც ექნებათ ბაზასთან წვდომა. ასევე მკაცრად უნდა იყოს განსაზღვრული, თუ ბაზის რომელ ობიექტზე აქვთ წვდომა და რა მანიპულაციების ჩატარების უფლებები აქვთ მათ მოცემულ ობიექტზე;
7. ყველა პაროლი უნდა იყოს დაშიფრული;
8. პაროლების ცვლილება უნდა ხდებოდეს არანაკლებ კვირაში ერთხელ;
9. მომხმარებლები, რომელთაც ქონდათ დროებითი წვდომის უფლება ბაზაზე უნდა იყვნენ ამოშლილი სისტემიდან სამუდამოდ;
10. ხდებოდეს მონაცემთა ბაზის ყოველდღიური ბექაფირება;

ამრიგად, ჩვენი პრაქტიკული რეკომენდაციები შეამცირებს ინფომაციის უსაფრთხოების რისკებს და მომავალში უფრო მოქნილს გახდის უნივერსიტეტის ინფორმაციული ტექნოლოგიების დეპარტამენტის ფუნქციონირებას:

- კლასტერული სისტემის დანერგვა;
- ინტერნეტის სარეზერვო ხაზის (პროვაიდერის) შემოყვანა;
- მონაცემთა ბაზაზე წვდომის უსაფრთხოების რისკების შემცირება.

უსაფრთხოების რისკები უნდა იყოს წინასწარ შეფასებული როგორც პოტენციური პრობლემა, რომლისთვისაც თავიდანვე უნდა იყოს შემუშავებული მოქმედების გეგმა და რესურსები ამ პრობლემის აღსაკვეთად, რაც უზრუნველყოფს ორგანიზაციის ბიზნეს-უწყვეტობას.

დღეისათვის ინფორმაციის დაცვა და უსაფრთხოების რისკების მართვა პრიორიტეტულია ნებისმიერი ორგანიზაციისთვის, ვინაიდან გლობალიზაციის პირობებში მსოფლიო ბაზარზე გაზრდილი კონკურენცია იწვევს ინფორმაციული აქტივების მითვისებას არასანქცირებული შეღწევადობის გზით.

გამოყენებული ლიტერატურა

1. Jean-Yves Huwart, Loic Verdier, Economic Globalisation, 2013.
2. В.В.Валтерович, Об определении экономической безопасности в условиях глобализации, 2014г, статья.
3. საქართველოს კანონი, ინფორმაციული უსაფრთხოების შესახებ, 5.06.2012წ.
4. საქართველოს იუსტიციის სამინისტრო, მონაცემთა გაცვლის სააგენტო (მგს 27005:2011) ინფორმაციული უსაფრთხოების რისკების მართვა, 28.10.2011წ.
5. ISO/IEC 27001:2013 – INFORMATION SECURITY MANAGEMENT.
6. ISO/IEC 27005: 2011 – INFORMATION SECURITY RISK MANAGEMENT.
7. www.tsu.edu.ge, თსუ-ს დებულება.

Management of information security and safety risks in Economic Globalization terms (According to the TSU example)

Shorena Davitaia

Iv. Javakhishvili Tbilisi State University, Professor's Assistant

Zurab Topuria

Information Technology Support Department, Chief Specialist, Georgian State Elecrtosystem

Summary

The globalization sharply changed information technology directions. It has become inevitable to form the world information area and introduce appropriate security systems.

The aims and plans of the approach of the Iv. Javakhishvili Tbilisi State University are chosen the right way.

For the future it's possible some practical recommendations to be taken into consideration which will decrease information safety risks and this will make the functioning of the University information technology department more flexible:

- Introduction of Cluster systems;
- Holding of the Internet reserve cable (provider);
- Decrease of the safety risks of the Database.

Safety risks must be assessed in advance as a potential problem, for which an action plan and resources must be made to solve the problem that will guarantee business continuity of the organization.

At present managing information security and safety risks is a priority to any organization, as increased competition on the world market in terms of Economic Globalization causes appropriation of the information actives by unsanctioned ways.