ინფორმაციული უსაფრთხოების მართვა

ოთარ შონია[1], იბრაიმ დიდმანიძე[2], ზებურ ბერიძე[2]
1-საქართველოს ტექნიკური უნივერსიტეტი
2. შოთა რუსთაველის სახელმწიფო უნივერსიტეტი (ბათუმი)

რეზიუმე

განიხილება თანამედროვე პირობებში ინფორმაციული უსაფრთხოების მართვის სისტემის აგების ძირითადი პრინციპები. გაანალიზებულია ინფორმციული უსაფრთხოების სფეროს დამახასიათებელი ძირითადი შედეგები. წარმოდგენილია ინფორაციის დაცვის მარვის სისტემის აგების თავისებურებები.

საკვანძო სიტყვები: ინფორმაცია, უსაფრთხოება, მართვა, მართვის სისტემა, ინფორმაციული უსაფრთხოება, ინფორმაციული უსაფრთხოების მართვის სისტემა.

1. შესავალი

საგარეო და საშინაო საფრთხეების მრავალფეროვნება, კრიმინალური ბიზნესის განვითარება, რაც დაკავშირებულია კონფიდენციალური მონაცემების გატაცებასა და კომპრომეტირებასთან, განსაკუთრებასთან, განსაკუთრებულ აქტუალობას ანიჭებს ინფორმაციული უსაფრთხოების სწორი ორგანიზების ამოცანებს. ამ ამოცანის გადაწყვეტა შეზღუდული რესურსების პირობებში გვიწევს.

2. ძირითადი ნაწილი

არსებობს ინფორმაციული უსაფრთხოების მართვის ოპტიმიზების საბაზისო პრინციპები. ინფორმაციული უსაფრთხოება არის დაცვის მექანიზმი, რომელიც უზრუნველყოფს ინფორმაციის კონფიდენციალურობას, ფასეულებრიობას და ხელმისაწვდომობას.

ინფორმაციული უსაფრთხოება მიიღწევა დონისძიებათა კომპლექსით, რომლებსაც გვთავაზობენ პოლიტიკოსები, ორგანიზაციული სტრუქტურებით, მეთოდებით, პროცედურებით პროგრამული და აპარატული საშუალებების გამოყენებით.

ინფორმაციული უსაფრთხოების მართვის სისტემა სამ ფუნდამენტურ პრინციპს ემყარება:

- გახსნილი მართვის პრინციპი. ამ პრინციპით იქნება უსაფრთხოების საკუთარი პოლიტიკები, რომელთა შესრულებას აკონტროლებს გადაწყვეტილებების მიმღები პირი. გამოყოფენ სპეციალურ პირს, რომელიც პასუხისმგებელია ინფორმაციული უსაფრთხოების პოლიტიკის დამუშავებასა და რეალიზაციაზე.
- კომპენსაციის პრინციპი გულისხმობს, რომ დამუშავებული უსაფრთხოების პოლიტიკიდან გადახრის ან გარეფაქტორების წარმოქმნის შემთხვევაში აუცილებელია შესაბამისი შესწორებების (კორექტივების) შეტანა მართვის ალგორითმში, რომელიც გარე ზემოქმედების ნეგატიური შედეგების კომპრესირებას შეძლებდა. ამიტომ გამორჩეულად მნიშვნელოვანია არა მხოლოდ უკვე მომხდარი ინციდენტების ანალიზი, არამედ აქტიური დაცვის სისტემის აგება, რომელსაც შეეძლება შეტევის მოგერიება მანამდე, ვიდრე პრობლემა გაჩნდება.
- მნიშვნელოვანია უკუკავშირის პრინციპის დაცვა, რომელიც ინფორმაციული უსაფრთხოების მართვის შესაძლებლობას იძლევა ჩაკეტილ წრეში. ინფორმაციული უსაფრთხოების მართვის სისტემაში უკუკავშირის რგოლის არსებობა მხოლოდ ცალკეული საფრთხის გამომჟღავნების საშუალებას კი არ იძლევა, არამედ იმ მოვლენებზე რეაგირებასაც, რომლებიც ერთი შეხედვით, ერთმანეთთან კავშირში არ არიან.

ინფორმაციული უსაფრთხოების მართვის სისტემის აღნიშნული პრინციპებით აგება, ოპტიმიზების არსებული მეთოდების გამოყენების საშუალებას იძლევა სისტემის სხვადასხვა მაჩვენებლის გაუმჯობესებისათვის, ე. წ. მართვის მდგრადობის, არსებულ და უცნობ საფრთხეებზე რეაქ-

ციის სისწრაფის, ინფორმაციულ უსაფრთხოებაში ინვესტიციების ანაზღაურებადობის ხარისხისათვის და ა. შ.

ინფორმაციული უსაფრთხოების მართვის სისტემების მათემატიკური მოდელების აგება, საფრთხეების შეფასება და მათი შედეგები, ინფორმაციის კლასიფიცირება, – ეს ყველაფერი გამოყენებული იქნას ინფორმაციული უსაფრთხოების სისტემის დამუშავებისას. რისკების სწორი შეფასება ინფორმაციული უსაფრთხოების ხარჯების მნიშვნელოვანი შემცირების საშუალებას იძლევა.

მიზანმიმართული მართვის შესაძლებლობა მნიშვნელოვან მოთხოვნას წარმოადგენს ინფორმაციული უსაფრთხოების ეფექტური და უწყვეტი მუშაობისათვის.

ინფორმაციული უსაფრთხოების სფეროში დამახასიათებელი შეცდომები ძირითადად შემდეგი სახისაა:

- ზედმეტი თავდაჯერებულობა იმაში, რომ შეტევა უმეტესობა, სისუსტეები და მათთან ბრძოლის მეთოდები დაწვრილებითაა ცნობილი, დამღუპველია.

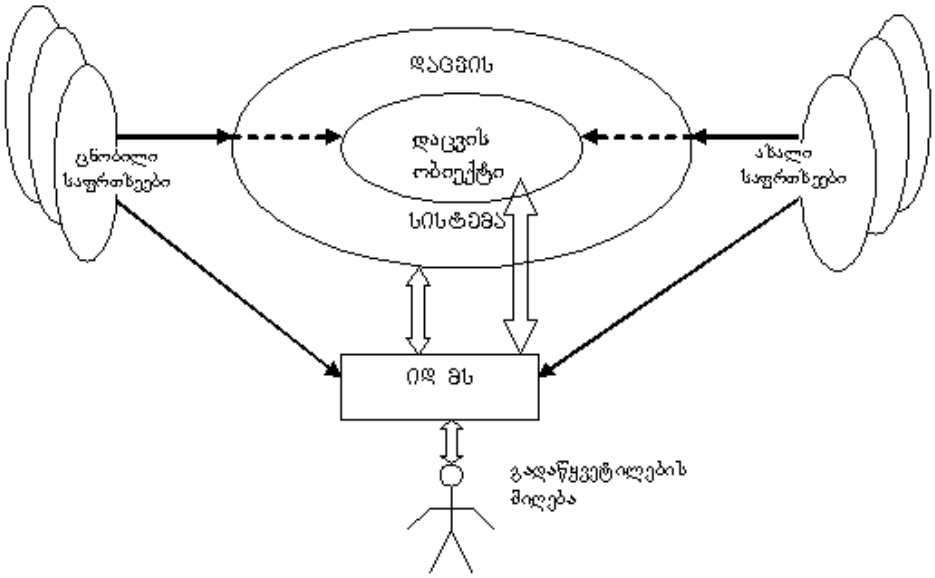
ინფორმაციული უსაფრთხოებისც საშუალებათა დიდი რაოდენობის გამოყენება ყოველთვის არ არის სასარგებლო, რადგან მომსახურების, პერსონალის სწავლების, სერვისული მოდულების განახლების ხარჯების ზრდას იწვევს და არ იძლევა ინფორმაციული უსაფრთხოების სისტემის ცენტრალიზებულად მართვის საშუალებას.

- ვიბის კომპიუტერების, ნოუტბუკების, პერსონალური კომპიუტერების მომხმარებელთა სამუშაო ადგილების დაცვის დონის უკმარობა. ანტივირუსი ამისათვის საკმარისი არ არის. მომხმარებელთა მობილურობა იზრდება მათთან ერთად მატულობს რისკებიც, კონფიდენციალური მონაცემების დაკარგვის, საერთო სარგებლობის ქსელებში მობილურ მოწყობილობებში არასანქცირებული შეღწევის ალბათობები.
- ინფორმაციულ უსაფრთხოებაზე დანახარჯების არასწორი განსაზღვრა - ხარჯები უნდა გაიყოს ცვლად და მუდმივ ოდენობებად. გადაწყვეტილებათა ღირებულების შეფასებისას, საჭიროა ხარჯების სწორად შეფასება თუნდაც სამი წლისათვის, ასევე გარდაუვალი მოდერნიზაციის შესაძლო შედეგებისათვის.

პროექტირების პროცესში ნებისმიერი ავტომატიზებული სისტემის ინფორმაციული უსაფრთხოების უზრუნველყოფის პოლიტიკამ უნდა გაითვალისწინოს ორი ფუნდამენტური რამ: სისტემაში ცირკულირებული ინფორმაციის ღირებულება (მნიშვნელობა) და მის წინააღმდეგ მიმართული შესაძლო მუქარები. ეს კი იმას ნიშნავს, რომ დაცვის სისტემის პროექტირებისას სისტემაში ცირკულირებადი ინფორმაციის ღირებულებიდან გამომდინარე შეფასდეს კლასიფიცირებული მუქარებისაგან დამცავი ზღუდეები (მექანიზმების, მეთოდების და ა. შ.) სიმტკიცე და ამისათვის გაწეული ხარჯების მიზანშეწონილობა. ამ შემთხვევაში გასათვალისწინებელია მუქარები (საერთოდ შესაძლო საფრთხეების) ხასიათი, განეკუთვნებიან თუ არა ისინი შემთხვევით ან წინასწარგანზრახულ საფრთხეების კლასს. თუ შემთხვევითი მუქარების ქვეშ ვიგულისხმებთ სუბიექტურ, ტექნოგენურ და ბუნებრივ საფრთხეებს, შეიძლება ითქვას, რომ ამ შემთხვევაში საკმაოდ დიდი გამოცდილებაა დაგროვილი მათი თავიდან აცილების თვალსაზრისით: გამოირიცხოს სუბიექტური შეცდომები სისტემის პროექტირებისა და ექსპლუატაციის პროცესში, გათვალისწინებულ იქნას საიმედოობისა და სხვა ტექნიკური მოთხოვნები, საჭიროებისა (თუ ეს ეკონომიკურად მიზანშეწონილია), უზრუნველყოფილ იქნას სისტემის კატასტროფაშედეგობა. თუ ამ ტიპის საფრთხეებს ასე თუ ისე სტაბილური ხასიათი აქვთ, ამას ვერ ვიტყვით წინასწარგანზრახულ საფრთხეებზე, რომლებიც მთლიანად დაკავშირებული არიან ადამიანის (ადამიანების) მუქარებებთან და გამოირჩევიან დინამიზმით. თუ დასაცავი ავტომატიზებული სისტემის პროექტირების პროცესში

გათვალისწინებული იყო მოცემული მომენტისათვის ცნობილი წინასწარგანზრახული რეალურად არსებული ან შესაძლო მუქარები და ჩადებული იყო სისტემაში მათგან დაცვის ადექვატური მექანიზმები, სისტემის ექსპლუატაციაში შეყვანის შემდეგ, როგორც პრაქტიკა გვიჩვენებს, ჩნდება სრულიად ახალი ტიპი საფრთხეებისა, რომელთა აღმოჩენა – პროგნოზირებას თუ არ ექნება პრევენციული ხასიათი, დაცვის ობიექტმა შეიძლება განიცადოს ისეთი ზემოქმედება, რამაც შეიძლება კითხვის ნიშნის ქვეშ დააყენოს მისი არსებაც კი.

ამრიგად, გამოიკვეთა ავტომატიზებული სისტემის ინფორმაციის არა უბრალოდ დაცვის სისტემის შექმნის აუცილებლობა, არამედ მოხდეს ინფორმაციის დაცვის მართვის ისეთი სისტემის ორგანიზება, რომელიც შეძლებს დინამიკაში აკონტროლოს როგორც ინფორმაციის დაცვის სისტემის ფუნქციონირება, ასევე უზრუნველყოს უცნობი საფრთხეების (მუქარების) პრევენციული აღმოჩენა, პროგნოზირება და დაცვის პოლიტიკის და დაცვის მექანიზმების განახლება-განმტკიცება. ე. ი. ინფორმაციის დაცვის მართვის სისტემამ (იდ მს) (ნახ. 1) უნდა უზრუნველყოს ინფორმაციული ტექნოლოგიების და ინფორმაციული უსაფრთხოების ისეთი მნიშვნელოვანი ამოცანების ავტომატიზაცია, როგორიცაა: რესურსების ინვენტარიზაცია, მოწყვლადობების (სუსტი ადგილების) მართვა, უსაფრთხოების პოლიტიკებთან შესატყვისობის კონტროლი და ცვლილებათა კონტროლი.



ნახ.1

როგორც აღვნიშნეთ, უმეტეს პრაქტიკულ შემთხვევებში ინვენტარიზაციის, დაცულობის შეფასების და უსაფრთხოების პოლიტიკებთან შესატყვისობის კონტროლის პროცედურები ტარდება არა რეგულარულად, ან დიდი ინტერვალებით. ეს კი იწვევს იმას, რომ ინფორმაცია კარგავს აქტუალობას და სიტუაცია ხდება უკონტროლო. ინფორმაციის დაცვის მართვის სისტემა აუცილებლად უნდა ეფუძნებოდეს კომპლექსურ მიდგომას და თანამედროვე ავტომატიზაციის ინტელექტუალურ საშუალებებს. ეს კი უზრუნველყოფს შრომითი დანახარჯების მინიზებას, რაც საჭიროა იუ-ს მონიტორინგის ამოცანის გადასაწყვეტად, რომელიც საშუალებას იძლევა დროულად იქნას აღმოჩენილი პრობლემები, და როგორც შედეგი – ამაღლებული იქნას ავტომატიზებული საინფორმაციო სისტემის დაცულობა. ინფორმაციის დაცვის მართვის სისტემის ინტელექტუალური ქვესისტემის შემადგენლობაში ფართომასშტაბიანი და მუდმივად განახლებადი ცოდნის ბაზის გამოყენება ინფორმაციული უსაფრთხოების (იუ) ადმინისტრატორებს მისცემს საშუალებას ოპერატიულად შექმნან სისტემის კონფიგურირების ეტალონურ შაბლონები, თვალყური ადევნონ სისტე-

მებს,რომლებიც არ აკმაყოფილებენ უსაფრთხოების პოლიტიკებს და ეფექტურად გამოასწორონ აღმოცენილი სისუსტეები, მათ შორის დაშვებული შეცდომებიც.

ინფორმაციული უსაფრთხოების რეჟიმი შეიცავს შემდეგ ეტაპებს:

– ინფორმაციული უსაფრთხოების პოლიტიკის განსაზღვრა;

– საგნობრივი არის განსაზღვრა ინფორმაციული უსაფრთხოების მართვის სისტემისათვის და მისი შექმნის მიზნების (კონკრეტიზება) დაკონკრეტება;

– რისკების შეფასება და მათი მართვა;

– ინფორმაციული უსაფრთხოების რეჟიმის უზრუნველყოფის ღონისძიებათა, საშუალებათა და მეთოდთა არჩევა;

– ინფორმაციული უსაფრთხოების მართვის სისტემის აუდიტი.

3. დასკვნა

ამრიგად, ინფორმაციული უსაფრთხოების მართვის სისტემების აგების შემოთავა.ზებული კონცეფცია, პირველ რიგში, გულისხმობს ინფორმაციული უსაფრთხოების სფეროში დამახასიათებელი ძირითადი შეცდომების სახეების გათვალისწინებას და უსაფრთხოების უზრუნველყოფის რეჟიმის ყველა ეტაპის უპირობო დაცვას. ეს კი საშუალებას იძლევა შესაძლო რისკების და არსებული ტექნიკურ-ეკონომიკური რესურსების და დასაცავი ინფორმაციის მნიშვნელოვნობის გათვალისწინებით შეიქმნას ინფორმაციული უსაფრთხოების მართვის ოპტიმალური სისტემა.

4. ლიტერატურა

1. Ульрих Д. Эффективное управление персоналом. Пер. с англ.. М., Вильямс, 2007

2. Гришина Н. В. Комплексная защита информации на предприятии, М., Форум. 2009.

3. გოგიჩაიშვილი გ., ოდიშარია კ., შონია ო. ინფორმაციის დაცვა ავტომატიზებულ სისტემებში, თბ., სტუ, 2008

4. შონია ო., შეროზია თ. ინფორმაციული ტექნოლოგიები და უსაფრთხოება, თბ., სტუ, 2008.

MANAGEMENT OF INFORMATION SAFETY

Shonia Otar[1], Didmanidze Ibraim[2], Beridze Zebur[2]
1-Georgian Technical University,
2- Shota Rustaveli State University (Batumi)

Summary

The basic principles of the system construction of information security control under the contemporary conditions are tackled. The basic results, characterizing the sphere of information safety, are analyzed.

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Шония О.[1], Дидманидзе И.[2], Беридзе З.[2]
1-Грузинский Технический Университет,
2-Гос. Университет Шота Руставели (Батуми)

Резюме

Рассматриваются основные принципы построения системы управления информационной безопасностью в современных условиях. Проанализированы основные результаты, характеризующие сферу информационной безопасности.