უსაფრთხოების უზრუნველყოფის პრობლემის კვლევისადმი სისტემური მიდგომის საკითხები

ოთარ შონია

საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

შესწავლილია ინფორმაციული უზრუნველყოფის თეორიის და პრაქტიკის საკითხები სისტემური მიდგომის საფუძველზე. ინფორმაციული უსაფრთხოება განისაზღვრება,როგორც ინფორმაციის დაცვასთან დაკავშირებული ძირითადი იდეების სისტემა, რომელიც იძლევა დაცვის პრობლემის არსის შესახებ ერთიან წარმოდგენას.

საკვანძო სიტყვები: ინფორმაციული უსაფრთხოება. სისტემური მიდგომა.

1. შესავალი

სახელმწიფოსა და საზოგადოებას შორის დიალოგის მთავარი საკითხი ეროვნული პრიორიტეტების შერჩევა, მათ რეალიზაციაში საზოგადოების ადგილის და როლის განსაზღვრა უნდა იყოს.

ყოველი ჩვენგანი თავისი სამუშაო (ინტელექტუალური) ძალის მესაკუთრეა და ჩვენი ინტერესების დასაცავად განვითარების სტრატეგიული მიზნების ფორმირებაში მონაწილეობისათვის გაერთიანების უფლება გვაქვს.

საკმაოდ ქაოტური შემთხვევითი ფაქტორების დიდი რიცხვების ერთობლივ ქმედებებს შემთხვევისაგან თითქმის დამოუკიდებულ შედეგებამდე მივყავართ, მიუხედავად ამისა, ისინი განვითარების გარკვეულ ვექტორს ქმნიან.

ეროვნული პრიორიტეტების ფორმირება პერსპექტივაში სტრატეგიული მიზნების შესაბამისად უნდა ხდებოდეს. როცა მიზნები განსხვავებულია, შეუძლებელია ერთობლივი გეგმის შემუშავება.

ადამიანის წინაშე არსებული პრობლემები არა მარტო რაოდენობრივად გაიზარდა, არამედ ხარისხობრივადაც შეიცვალა. სამყარო სწრაფად იცვლება, ჩვენ ან ვერ ვიგებთ, ან საკმარისი ხარისხით ვერ განვჭრეტთ პრობლემებს, რომლებთან შეჯახებაც უახლოეს მომავალში მოგვიწევს. ამ ვითარებაში აღმოცენდება და დღითიდღე უფრო აქტიური ხდება ადამიანის უსაფრთხოების უზრუნველყოფის საკითხი. ცნება ,,არსებობა'' პრაქტიკულად ჩანაცვლდება ცნებით ,,გადარჩენა''. განვითარების მდგრადობაზე საუბარი მხოლოდ იმ შემთხვევაში იქნება რეალური, თუ აღნიშნული პროცესის უსაფრთხოება იქნება უზრუნველყოფილი. საჭირო ხდება უსაფრთხოების უზრუნველყოფის სფეროში ფართო აუდიტორიის ჩამოყალიბება.

ეროვნული უსაფრთხოების ქვეშ იგულისხმება ერის ისეთი მდგომარეობა, როცა მცირეა მისი ეროვნული ინტერესების პარამეტრების არსასურველი ცვლილებების ალბათობა.

,,ინფორმაციული უსაფრთხოება'' საკმაოდ ფართოდ გამოიყენება პრაქტიკულ ცხოვრებაში, განსაკუთრებით ხშირად ის შენაცვლებულია მონათესავე ცნებით ,,ინფორმაციის დაცვა'', რის გამოც ის გამოთვლითი ტექნიკის საშუალებებით დამუშავებისას ინფორმაციის სხვადასხვა არხით გაჟონვისაგან დაცვის კერძო ამოცანამდე დაიყვანება.

უსაფრთხოება – ეს არის პროცესების ერთობლიობა, რომელთაგან თითოეული ინდივიდუალურია, ეს არის სისტემური პრობლემა, რომლის გადაჭრა სრულიად განსხვავებული, სხვადასხვა დაქვემდებარების და პასუხისმგებლობის, ტექნიკური და საკადრო უზრუნველყოფის მქონე სამსახურების შეთანხმებული მუშაობით ხორციელდება.

თუ სისტემის უზრუნველყოფას ვაპირებთ, პროცესი უნდა შევიმუშაოთ.

უსაფრთხოების საბოლოო მიზანს დაცულობა წარმოადგენს.

უსაფრთხოება რთული სისტემური პროცესია, რომელიც ყოველთვის, რესურსული მხარდაჭერის პირობებშიც კი, გაქრობისკენ მისწრაფვის. უსაფრთხოების დონის დაცემა პრინციპულად არ ხდება, ვინაიდან ამ შემთხვევაში თვით პროცესის დეზორგანიზაცია მიმდინარეობს.

ძნელია უსაფრთხოების და სირთულის შეთავსება. რაც უფრო რთულია სისტემა, მით უფრო ძნელია მისი უსაფრთხოების უზრუნველყოფა.

არ არსებობს აბსოლუტურად უსაფრთხო სისტემები. თანამედროვე ტექნოლოგიებში იმდენად ბევრი კომპონენტი და მათი კავშირია, რომ ზოგიერთი მათი შემქმნელისა და მითუმეტეს, მომხმარებლისათვისაც, უცნობია და უსაფრთხოების მუქარა ძალაში რჩება.

უსაფრთხოება გრძელ ჯაჭვს წარმოადგენს, რომლის თითოეული რგოლი სხვადასხვა მიზეზის გავლენით სხვადასხვა სიმტკიცისაა. სუსტი რგოლი წყდება და თუ ჯაჭვი დაზღვეული არაა,

უსაფრთხოების დაკარგვა და ინციდენტის თავიდან აცილება შეუძლებელია. ხანძრის შემთხვევაში გვიან იქნება მონაცემთა ბაზების სარეზერვო კოპირება.

უსაფრთხოების უზრუნველმყოფი ქმედებები ხორციელდება შესაძლო მუქარების მოდელირების ბაზაზე, ე. ი. აქვს პროგნოზული ხასიათი. დამცველი ღონისძიებების არჩევა მესაკუთრეზეა დამოკიდებული, რომელიც არჩევანს იმ მუქარების ჩამონათვალის საფუძველზე ახორციელებს, რომლებმაც შეიძლება ის დანაკარგებამდე მიიყვანოს.

დაცვის გარკვეულ დონეზე ორიენტირებულ მკაცრად რეგლამენტირებულ საშუალებებზე გადასვლა უთუოდ ამარტივებს დანახარჯების გათვლას, მაგრამ მოძველებული და გამოუსადეგარია.

მუქარების რეალიზაციის პროცესის განხილვისას მივდივართ მუქარების და მათთან უკუქმედების სწორი სტრატეგიების არჩევის არსის გაგებამდე. გადამწყვეტ როლს ასულებს მოწყვლადობა ანუ პროდუქტის სუსტი მხარეები, რომლებიც გამოიყენება მუქარების რეალიზაციის პროცესში. რეალური მუქარებისაგან დაცული პროდუქტის შემთხვევით მიღება შეუძლებელია, ის პროექტირებისადმი იმ თანამედროვე მიდგომის შედეგია, რომელიც ინფორმაციული პროდუქტების შემუშავების პროცესში ინფორმაციული უსაფრთხოების უზრუნველყოფას გულისხმობს.

სიახლე იმაში მდგომარებს, რომ უსაფრთხოების უზრუნველყოფის პრობლემასთან დაკავშირებული მასალების წარმოდგენის თეორიაში და პრაქტიკასა მუშავდება და ინერგება უსაფრთხოების უზრუნველყოფის ცოდნისა და უნარ-ჩვევების ერთიანი სისტემა. უსაფრთხოების უზრუნველყოფა უნდა ითვალისწინებდეს: წიგნების, ვიდეო (ტელე) ვერსიების გამოცემას, ინოვაციური კომპიუტერული სისტემების შექმნას, გადაწყვეტილებების მიღების პროცესების მოდელირებას, ე. ი. უსაფრთხოების ოპტიმალური სტრატეგიის განსაზღვრის მოდელირების კომპიუტერული სისტემების შემუშავებას ინფორმაციული სიტუაციების გაურკვევლობის პირობებში.

ინფორმაციული ტექნოლოგიების განვითარებასთან ერთად ჩნდება და სწრაფად იზრდება მათ გამოყენებასთან დაკავშირებული რისკები, აღმოცენდება სრულად ახალი მუქარები, რომელთა რეალიზაციის შედეგებს ადრე არ ვხვდებოდით. ინფორმაციული უსაფრთხოების უზრუნველყოფის პრობლემა განსაკუთრებით აქტუალურია. ყველა გადაწყვეტილებას რეკომენდაციების საერთომეთოდოლოგიური ხასითი აქვს.

შეუძლებელია წინასწარ განისაზღვროს მოწყვლადობის სრული ჩამონათვალი, მაგ., ბოროტგანმზრახველი ხვეწს თავდასხმის მეთოდებს ან იყენებს ახალს და შესაძლებელია აირჩიოს ის მახასიათებლები, რომლებიც არ წარმოადგენდა პროდუქტის მოწყვლად ადგილს. სუსტი ადგილები ვლინდება პროექტირების, ექსპლოატაციის და რეალიზაციის ეტაპებზე.

მუქარა პოტენციური შესაძლებლობაა.

მოწყვლადობა ნოყიერი ნიადაგია მუქარების რეალიზაციისთვის.

გამოვლენილ უნდა იქნას შეტევის მიზანი, ზემოქმედების მექანიზმი, შეფასებული - მუქარის აგენტი, მოწინააღმდეგის გამოცდილება, რესურსები და მოტივაცია.

90-იან წლების დასაწყისში ითვლებოდა, რომ შინაური მტრის არსებობა უფრო გამონაკლისი იყო, ვიდრე წესი, ხოლო პერსონალის კონტროლის (დაშვების) არსებობა და დარღვევებისათვის პასუხისმგებლობა ორგანიზაციის შიგნით ინფორმაციული უსაფრთხოების დამაჯერებელი დონის შენარჩუნებისათვის – საკმარისი.

ამჟამად სისტემების რაოდენობის ზრდამ შესაძლებელი გახადა მათი სანდო კომპლექტაციის უზრუნველყოფა, გაჩნდა სისტემების და ქსელების რეგულირების და აწყობის მნიშვნელოვნად დიდი შესაძლებლობები, ანუ გაიზარდა მათი არამეგობრული გამოყენების შანსიც. აღარავის ეშინია „მგლის ბილეთის“ – არსებობს CV გაყალბების ვარიანტი; თავისუფალ ბაზარს არ ადარდებს პერსონალის უმწიკვლობა. გაიზარდა უხარისხო პროდუქტის რაოდენობა, ასევე – ფინანსური ფაქტორის როლი, ხელფასში – დისტანცია, შედეგად – წყენის ფაქტორი და ორგანიზაციისათვის ზიანის მიყენების მცდელობები. შინაგანი მუქარები არა მხოლოდ პოტენციური, არამედ რეალური გახდა ბოროტმოქმედთა ხელში.

ინფორმაციული უსაფრთხოების დაცვა სხვადასხვა საშუალების კომპლექსი კი არა, ინფორმაციული უსაფრთხოების საიმედო სისტემის შესაქმნელი ღონისძიებების კომპლექსია.

ინფორმაციული უსაფრთხოების კომპლექსური სისტემის შექმნის პროცესი იყოფა შემდეგ ეტაპებად:

1. უსაფრთხოების მიმდინარე მდგომარეობის ანალიზი. ისაზღვრება დაცვის ობიექტი, მოდელირდება საინფორმაციო სისტემა და ინფორმაციული უსაფრთხოების მუქარები;

2. მიზნების განსაზღვრა, დაცვის ამოცანების დაყენება, დონეების არჩევა, დაცვის საშუალებების დაცულობისადმი ტექნიკური მოთხოვნების ფორმირება, შესაძლო შედეგების ლიკვიდაციის გზები;

3. სისტემების პროექტირება, დაცვის აპარატული და პროგრამული საშუალებების არჩევა, ტექნიკური მოთხოვნების რეალიზაცია;

ფიზიკურ დონეზე უსაფრთხოება რეალიზდება პროგრამული და აპარატული საშუალებების ფიზიკური დაცვით მეთვალყურეობის და დაცვის ტექნიკური საშუალებების გამოყენებით;

ტექნოლოგიურ დონეზე უსაფრთხოება რეალიზდება, როგორც პროგრამული უზრუნველყოფის და საიმედო აღჭურვილობის (მის საიმედოობაზეა დამოკიდებული ინფორმაციის ხელმისაწვდომობა), ინფორმაციის აკუსტიკური და ვიბროაკუსტიკური დაცვის საშუალებებით პროგრამული და აპარატურული პლატფორმის დაცვის, აპარატურული საშუალებების გვერდითი ელექტრომაგნიტური გამოსხივების და დადგენილი მიმართულების დაცვის გამოყენების შედეგი.

სამომხმარებლო დონეზე ინფორმაციული უსაფრთხოების დაცვა – მომხმარებლის პირადი სამუშაო გარემოს დაცვა, რაც რეალიზდება მომხმარებლის იდენტიფიკაციის და აუდენტიფიკაციის გზით, ასევე – ინფორმაციის წყაროს ხელმისაწვდომობის უფლებამოსილების განსაზღვრით.

ინფორმაციული უსაფრთხოების ქსელურ დონეზე - მიიღწევა, როგორც ლოკალური ქსელების სეგმენტების, ისე - კომპანიების ქსელის გარე პერიმეტრის ინტერნეტის გზით მუქარებისაგან ინდივიდუალური დაცვით. ამისთვის აქ გამოიყენება ინფორმაციის ფილტრაცია, ქსელთაშორისი ეკრანები, სანდო მარშრუტიზაცია და VPN (ვირტუალური კერძო ქსელი).

დაცვის ღონისძიებები დეგრადაციას განიცდის. ყველასთვის ყველაფერი ნებადართულია. თავიდან საჭიროა როლების და პასუხისმგებლობების განაწილება. დავუშვათ, როლები რაციონალურად განაწილდება, მაგრამ თუ თანამშრომელი ავად გახდა, მაშინ საჭიროა გარკვეული ვადით უფრო მეტი უფლებამოსილების მინიჭება. რაც მეტი თავისუფლება აქვთ თანამშრომლებს, მით უკეთესია ფირმისთვის.

დაცვა გულისხმობს შეზღუდვას. გაურკვევლობის პირობებში ბიზნეს-დონეზე მიიღება გადაწყვეტილებები ამა თუ იმ მოქმედებების განხორციელების აუცილებლობის, მისი გადავადების, დამატებითი გარანტიების ან რესურსებისთვის ზრუნვის ან ამ ქმედებებზე უარის თქმის შესახებ. ამასთან, გამოიყენება თვითკონტროლის გარკვეული მექანიზმები, რომლებიც იძლევა მიზნის მიღწევის ხარისხის შემოწმების საშუალებას. ინფორმაციულ უსაფრთხოებას არ გააჩნია თვითკონტროლის მექანიზმი, რომელიც მოცემული მიზნის მიღწევის ხარისხის შემოწმების საშუალებას მოგვცემდა.

ინფორმაციული უსაფრთხოების ეფექტურობა რეალურად ვლინდება მხოლოდ შეტევების მომენტებში. ინფორმაციული უსაფრთხოება დეგრადაციას განიცდის ბოროტმოქმედების პასიურობის ინტერვალებში ან სუსტდება მოწინააღმდეგესთან ბრძოლისას.

ლიტერატურა:

1. Прангишвили А. И., Прокопьев С. В., Шония О. Б. Модель поддержки принятия решений в конфликтологии. Жн: Информационные технологии в проектировании и производстве. М., ВИМИ, №3. 2007

2. Галатеико В. А. Основы информационной безопасности. Бином. Москва, 2008

3. Белов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А. Основы информационной безопасности. Горячая линия – Телеком. М., 2006

4. Люгер Д. Ф. Искусственный интеллект. Стратегии и методы решения сложных проблем. Вильямс. М., 2003.

5. ჩოგოვაძე გ., გოგიჩაიშვილი გ., სურგულაძე გ., შეროზია თ., შონია ო. მას-ის დაპროექტება და აგება. თბ., სტუ, 2001.

6. შონია ო., ნარეშელაშვილი გ., ქართველიშვილი ი. უმავთულო ქსელების უსაფრთხოება, თბ., სტუ, 2008.

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

ISSUES PERTAINING TO SYSTEM APPROACH TO RESEARCH OF THE PROBLEM OF THE SAFETY

Shonia Otari
Georgian Technical University

Summary

This article presents the issues of theory and practice for establishment of information safety on the basis of systems approach. Information safety is defined as the basic ideas system, which relate to the protection of information and it gives complete idea about the essence of the protection problem.

ВОПРОСЫ СИСТЕМНОГО ПОДХОДА К ИССЛЕДОВАНИЮ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Шония О.
Грузинский Технический Университет

Резюме

Изложены вопросы теории и практики обеспечения информационной безопасности на основе системного подхода. Информационная безопасность определяется как система основных идей, относящихся к защите информации, дающая полное представление о сущности проблемы защиты.