კომპიუტერული ქსელების დაცვის უსაფრთხოების მოდელები და მათი გამოყენება

გიორგი მაისურაძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია ინფორმაციული სისტემების დაცვის მეთიდების კონცეფციები, დაცვის მექანიზმის არჩევის საკითხი და დაცულობის ანალიზი, ნაჩვენებია, რომ სპეციალიზებული ინფორმაციული სისტემების დაცვის მექანიზმების ასგებად მნიშვნელოვანია შეტევის მოდელის დამუშავება

საკვანძო სიტყვები: კომპიუტერული ქსელი. სისტემა. ინფორმაციული უსაფრთხოება. დაცვის მოდელები. დაცვის საშუალებები. შეზღუდვები.

1. შესავალი

კომპიუტერული ქსელის დაცვის მოდელების გამოყენებით თეორიულად მტკიცდება ინფორმაციული სისტემების დაცვის შესაბამისობა უსაფრთხოების მოთხოვნებისადმი.

ეს მოდელები საშუალებას იძლევიან დამტკიცდეს, რომ ინფორმაციის დაცვის სისტემა არ უშვებს დაცული ინფორმაციაზე არასანქცირებულ წვდომას. ამავე დროს ამ მოდელების გადაწყვეტა გართულებულია, რადგან „ნების“ დამრთველ პროცედურებს აქვთ გარკვეული პრობლემები და მათი ლეგიტიმურობისათვის ყველა ელემენტის განსაზღვრა შეუძლებელია.

ამავდროულად ინფორმაციის დაცვის სისტემის ასაგებად აუცილებელია გადაწყდეს დაცვის (Mz) მექანიზმების არჩევის პრობლემა, რომელიც უზრუნველყოფს i – ქვესისტემის უსაფრთხოებას დაცვის მექანიზმების ნაკრებიდან: {Mz_{di1} Mz_{di2}, Mz_{di3},... Mz_{oil1}, Mz_{0l2} ...}, სადაც Mz_{dij} - დაცვის საშუალებებია, რომლებიც ახორციელებენ მოთხოვნებს ქვესისტემის სუბიექტისადმი, Mz_{oij}– დაცვის საშუალებებია, რომლებიც ახორციელებენ მოთხოვნებს ქვესისტემის ობიექტებისადმი.

დაცვის საშუალებებისა და კომპონენტის არჩევა ემყარება გასანაალიზებელი ობიექტების პარამეტრულ მაჩვენებლებს. რეალიზაციის თითოეული საშუალება ფლობს მნიშვნელოვან პარამეტრებს. ეს უპირველეს ყოვლისა არის ღირებულება, საიმედო მუშაობის ალბათობა და განსახორციელებელი ტექნოლოგიის დაცვის უზრუნველყოფის დონე. მეორე ხარისხოვან კრიტერიუმებს შორის შეიძლება გამოიყოს ექსპლუატაციის ღირებულება, ერთ ტრანზაქციაზე დახარჯული დრო, ერთი ტრანზაქციის განხორციელების ხვედრითი ღირებულება, ოპერატიული მეხსიერების აუცილებელი მოცულობა, ერგონომიკური და ეფექტურობის სხვა მაჩვენებელი, გამოყენების სიმარტივე და მოხერხებულობა და ა.შ.

დაცვის საშუალებებიდან ცალკეული აღიწერება როგორც მინიმუმ რამდენიმე პარამეტრის ნაკრები, რომლებიც აინტერესებთ სისტემის პროგრამისტებს და დამკვეთებს: Mz = {C_{ij}, P_{ij}, T_{ij}, V_{ij}, ,...}, სადაც, C_{ij} - დაცვის საშუალებების ღირებულებაა, P_{ij} – დაცვის დონე, T_{ij}– ელემენტალური ოპერაციის განხორციელებისათვის საჭირო დრო, V_{ij} – ოპერატიული მეხსირების აუცილებელი მოცულობა.

აღნიშნულიდან გამომდინარე ინფორმაციის დაცვის სისტემის პარამეტრებად გამოდიან ღირებულება, სამუშაოს დრო, ინფორმაციის კონფიდენციალურობის შენახვის ვადა, გამოსაყენებელი მეხსიერების მოცულობა და ა.შ.

ტექნიკურ პარამეტრებად ასევე შეიძლება შეირჩეს: კრიპტოგრაფიული სტანდარტი, გასაღების სიგრძე, გასაღების პაროლის სიცოცხლის დრო, გასაღებების განაწილების სისტემა და სხვა. მსგავსი პრობლემის გადაწყვეტისას დამატებით კრიტერიუმად შეიძლება გამოვიდეს დრო და

შემუშავების ღირებულება, დრო და დაცვის სისტემების დანერგვის ღირებულება, დრო და ექსპლუატაციის ღირებულება, ინფორმაციის დამუშავების პროცესზე ზეგავლენის ხარისხი, ძირითადი გამომთვლელი სისტემების მაჩვენებლების გაუარესების ხარისხი (ტრანსაქციების დამუშავების დრო, მომხმარებლების კონფორტულობა, ექსპლუატაციის ღირებულება და ა.შ.). გარდა ამისა, უნდა მოხდეს შესაბამისი შეზღუდვების იდენტიფიცირება.

2. შეზღუდვების იდენტიფიკაცია

დაცვის ღონისძიებების არჩევაზე მრავალი შეზღუდვა მოქმედებს. მათი იდენტიფიკაციის პროცესში განისაზღვრება ინფორმაციის დაცვის სისტემის ეფექტურობისადმი მოთხოვნები, რადგან დადგენილი შეზღუდვები ასაბუთებენ დაცვის ფუნქციის მოცულობას, რომლებიც ან განსაზღვრავენ საფრთხის ალბათობის დონეს და რისკის დაშვებას (რაც მისაღებია კონფედენციალური ინფორმაციის შემცველი ბევრი ინფორმაციული სისტემისათვის), ან აღმოფხვრიან სრულად საფრთხეს და რისკის ფაქტორს (რაც ახასიათებს ბირთვული და ატომური ენერგული კომპლექსის ავტომატური მართვის სისტემებს).

როგორც წესი ტიპიურ შეზღუდვებს მიაკუთვნებენ [1]:

შეზღუდვები დროში – ხორციელდება ღონისძიებების შესრულებასთან კავშირში შესასრულებელი დროის პერიოდის ფარგლებში, შესაბამისი სისტემის სასიცოცხლო ვადის განმავლობაში.

ფინანსური შეზღუდვები (ეკონომიური თვალსაზრისით) - უკავშირდება დაცვითი ღონისძიებების ექსპლუატაციისა და რეალიზაციის ღირებულებას, რომლებმაც არ უნდა გადააჭარბოს აქტივების ღირებულებას, რომელთა უსაფრთხოებისთვისაც არიან ისინი განკუთვნილნი. აუცილებელია გაკეთდეს ყველაფერი, იმისათვის რომ არ გადავიდეს ამ მიზნებისათვის გამოყოფილ ასიგნირების ფარგლებიდან.

ტექნიკური შეზღუდვები – პროგრამებისა ან აპარატურული საშუალებების, ასევე შესაბამისი დამცავი ღონისძიებების ადრე განხორციელებული ღონისძიებებისადმი შეთავსება, რადგან განსახორციელებელ ღონისძიებებს შესაძლებელია ორგანიზაციის სტრუქტურის რეორგანიზაცია მოყვეს და მთელი ინფორმაციული სისტემების გარდაქმნა. მსგავსი სიძნელეების არსებობამ შესაძლოა შეცვალოს დამცავი ღონისძიებების მიმართულება დაცვის ორაგანიზაციულ და ფიზიკური მეთოდების მხრივ.

სოციოლოგიური შეზღუდვები – ტექნიკური დამცავი ღონისძიებების გამოყენების ეფექტურობა დამოკიდებულია ორგანიზაციის თანამშრომელთა აქტიურ მხარდაჭერაზე. ამიტომ, თუ თანამშრომლებს არ ესმით ასეთი ღონისძიებების აუცილებლობა ან თვლიან, რომ ეს მიღებელია მათი მორალისათვის, მაშინ არსებობს დიდი ალბათობა იმისა რომ დაცვითი ღონისძიებების ეფექტურობა დროთა განმავლობაში შემცირდება.

გარემოს შეზღუდვები – ეკოლოგიური ფაქტორები, რომლებიც უნდა გათვალისწინდეს დაცვითი სისტემების აგებისას არსებული ტერიტორიის, ექსტრემალური ბუნებრივი პირობების გამო მათი განხორციელების გაზრდა ან შემცირება.

სამართლებრივი შეზღუდვები – სავალდებულოა გათვალისწინებული იქნას საკანონმდებლო ნორმები არა მარტო ინფორმაციული უსაფრთხოების სფეროში, ასევე სხვა სამართლებრივი ნორმატივების აქტებში, თუმცა როცა მათ არ აქვთ პირდაპირი კავშირი ინფორმაციული ტექნოლოგიების დაცვასთან, მაგრამ ზემოქმედებენ დაცვითი ღონისძიებების არჩევაზე.

3. კომპიუტერული ქსელის დაცვის სისტემის ეფექტურობის შეფასება

კომპიუტერული ქსელის დაცვის სისტემის შექმნის პროცესში აუცილებელია განისაზღვროს რომელ ხარისხზე უნდა ავიღოთ ორიენტირება ღირებულების შეზღუდვის პირობებში, როგორ მიიღწეს ეს, რა ტექნიკური რისკი შენარჩუნდება, თანამდებობის პირთა მომზადების რა დონეა საჭირო სისტემის ეფექტური ფუნქციონირებისათვის, რომელ სუსტ ადგილებს აქვს ადგილი და რომელს აქვს აღმოფხვრის პრიორიტეტი ინფორმაციული სისტემის სრულყოფისა და განვითარებისას.[2]

ასეთი კვლევის ჩატარების აუცილებლობა გამომდინარეობს კომპიუტერული ქსელის დაცვის სისტემის აგების შესახებ მიღებული გადაწყვეტილებების ობიექტური შფასების მოთხოვნილებიდან, ინფორმაციის დაცვაზე მიმართული ხარჯების ეფექტურობიდან და ასევე დასაცავი ობიექტის არასანქცირებული გავრცელების დროს ეკონომიური სანქციების სიდიდის განსაზღვრიდან.

ამავე დროს, ინფორმაციის დაცვის სისტემის ეფექტურობის ძირითად კრიტერიუმად დგინდება დაცვის სისტემაზე გაწეული დანახარჯების შეფარდება ინფორმაციული სისტემის უსაფრთხოების დარღვევით მიღებულ ზარალთან დესტრუქციული ზემოქმედების რეალური შესაძლობების გათვალისწინებით. [3].

ეფექტური შეფასების არსებული მეთოდები შეიძლება გაიყოს ინსტრუმენტალურ-მოდელირებად, საკონტროლო-გამოსაცდელ და ლოგიკურ-ანალიტიკურად.

სტანდარტული დებულებები წარმატებით გამოიყენება ტექნიკური დავალების მოთხოვნების ფორმირებისას, შედარებითი ანალიზისას, ტექნიკური გადაწყვეტილებების შეფასებისა და დასაბუთების დროს,გამოცდის ჩატარებისას (მათ შორის სერტიფიცირებულისაც)და ინფორმაციული სისტემების ტექნიკური პარამეტრების დაყენებისას, შექმნილი, მოდერნიზირებული და ექსპლუატაციაში არსებული ინფორმაციული სისტემების ფუნქციონირების ხარისხის შემოწმებისას.

4. ეფექტურობის შეფასების ინსტრუმენტული მოდელირების მეთოდი

ყველაზე მეტად ცნობილია ინსტრუმენტალური-მოდელირების КОК მეთოდი [4].

ინფორმაციის დაცვის სისტემის ეფექტურობის გასაანგარიშებლად იგი წარმოიდგინება წინაღობების თანმიმდევრობის სახით, რომელთა წარმატებული გადალახვის შემდეგ, ბოროტმომქმედი ღებულობს წვდომას ინფორმაციისა ან პროგრამული რესურსებისადმი.

ამოცანის ამოხსნის ამოსავალი მონაცემებია: წინაღობების რაოდენობა Mi (1,…M); წინაღობის გადალახვის საშუალო დრო (Um); მარეგულირებელი პარამეტრების მნიშვნელობების შეცვლის შორის საშუალო დრო (f_m); სისტემის დაცულობის შენარჩუნების მინიმალურად დასაშვები ალბათობა (Pდაც = 0,999); მაშინ მტკიცდება, რომ:

არასანქცირებული წვდომის Pდაც პრევენციის ალბათობა;

$$P_{\text{დაც}} = 1 - \prod_{m-1}^{M} P_{\text{ასწ.}m} \quad (1)$$

ბოროტმოქმედის მიერ m-წინაღობის გადალახვის ალბათობა ($P_{\text{ასწ.m}}$):

$$P_{\text{ასწ.}}m = \frac{1}{fm}\int_0^{\infty}[1 - Fm(t)]Um(t)dt \quad (2)$$

სადაც - საშუალოა $F_m(t)$ - დროის განაწილების ფუნქცია m წინაღობის დამცავი პარამეტრების მეზობელ ცვლილებებს შორის (ბოროტმოქმედის ახალი გაშიფრის აუცილებლობამდე მიმყვანი);

$$Fm(t) = 1 - exp(-\frac{t}{fm}) \quad (3)$$

ახასიათებს m წინაღობის პარამეტრების მნიშვნელობების პერიოდული ცვლის შემთხვევას; Um(t) - m წინაღობის პარამეტრების მნიშვნელობების გაშიფრის დრო (გახსნა);

$$Um(t) = 1 - exp(-\frac{t}{Um}) \quad (4)$$

მიღებული დროითი მაჩვენებლების შესაბამისად გაანგარიშდება არასანქცირებული წვდომის ალბათობა ($P_{ასწ.მ}$) და $P_{დაც}$. გარდა ამისა, კომპლექსი საშუალებას იძლევა დადგინდეს Mi დაცვის ის მექანიაზმები, რომლებიც არ უზრუნველყოფს სისტემის დაცულობის შესამჩნევ ზრდას საწყისი მონაცემების მოცემული მნიშვნელობებისათვის.

5. დასკვნა

მოცემული მეთოდი პირდაპირ დამოკიდებულია შემავალ მონაცემებზე და ობიექტური შეფასებისათვის მოითხოვს წინაღობების გადალახვის ყველა შესაძლო მეთოდის შეფასებას, რომლებიც ან მკაფიოდ უნდა იყოს განსაზღვრული ან წესების სიმრავლის სახით უნდა იყოს ჩამოყალიბებული. ამ სიმრავლეების შემადგენლობა ექსპერტული გზით განისაზღვრება და ფორმალიზაციას მოითხოვს, რადგან წინააღმდეგობების გადასალახი და ადრეულად პროგნოზირებული მოვლენების შესაძლებელი მეთოდების სრული სამუშაო სივრცის მისაღებად მოცემული სიმრავლის ამოუხსნადობისაკენ მიჰყავს, მის გამარტივებას კი შეიძლება ადექვატურობის დაკარგვა მოჰყვეს.

ლიტერატურა:

1. Kent S.T. Internet Security Standards: Past, Present&Future. Standard-View. v.2. 1994. pp.78-85

2. Анин Б.Ю. Защита компьютерной информации. СПб.: БХВ- Петербург, 2000.

3. Галатенко В.А. Основы информационной безопасности. М.: ИНТУИТ.ru "Интернет-Университет Информационных Технологий", 2003

4. Безкоровайный М.М., Львов В.М., Костогрызов А.И. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем "КОК": 150 задач анализа и синтеза и примеров их решения: Руководство системного аналитика. Изд. 2-е, доп. – М.: “Вооружение. Политика.Конверсия”. 2002.

MODELS OF PROTECTING THE SECURITY OF COMPUTER NETS AND THEIR USAGE

Maisuradze Giorgi
Georgian Technical University

Summary

In the article the main concepts of methods of protection of informational systems are discussed. The issues of selection of a protection mechanism and an analysis of safety are considered. It is shown that for building the protection mechanisms of informational systems it is important to develop models of attack.

МОДЕЛИ ЗАЩИТЫ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ И ИХ ИСПОЛЬЗОВАНИЕ

Маисурадзе Г.
Грузинский Технический Университет

Резюме

Рассмотрены концепции методов защиты информационных систем, вопрос выбора механизма защиты и анализ защищенности, показано, что для построения механизмов защиты информационных систем существенным является разработка модели атаки.