ინფორმაციული სისტემის დაცვის უზრუნველყოფის ამოცანის დასმის ეფექტურობა

ოთარ შონია, ლუკა შონია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

ნაშრომში ნაჩვენებია ინფორმაციული სისტემის დაცვის ეფექტურობის გამოთვლის სპეციფიკა არსებული ინფორმაციული სისტემის დაცვის საერთოთეორიული მეთოდების ანალიზის გვერდით. განიხილება სპეციალური ხერხი, რომელიც შეიძლება გამოყენებულ იქნას ინფორმაციული სისტემის კვლევისას.

საკვანძო სიტყვები: ინფორმაციული სისტემა. ინფორმაციის დაცვა.

1. შესავალი

ინფორმაციული სისტემის და მასში შემავალი სხვადასხვა ობიექტების დაცვის უზრუნველსაყოფად აუცილებელია წინასწარი გადაწყვეტილებების ფორმირება, ანუ ამოცანების ფართო წრის გადაწყვეტა.

მთლიანი ინფორმაციული სისტემის დაცვის მიზნით გადაწყვეტილებათა მიღება უნდა იყოს შეთანხმებული ცალკეული ობიექტის ინფორმაციულ დაცვასთან, რითაც უზრუნველყოფილი იქნება დაცვის გადაწყვეტილებების ერთიანი სისტემა. მიზანშეწონილია (სადაც ეს დასაშვებია) ერთნაირი ტიპის ინფორმაციული დაცვის ამოცანების ზოგადი დასმისა და გადაწყვეტილებების მეთოდების გამოყენება. აუცილებელია ინფორმაციული დაცვის ამოცანათა კლასიფიკაცია, ხოლო მათი ამოხსნა უნდა ემყარებოდეს დაგროვებულ გამოცდილებას. ინფორმაციული დაცვის ამოცანების კლასიფიკაცია თავის მხრივ ხელშემწყობი უნდა იყოს მიზანმიმართული მეთოდების დამუშავების და გადაწყვეტილებების მიღებაზე, რომელიც ითვალისწინებს გადაწყვეტილებათა შეპირისპირებას, როგორც ობიექტების, ასევე სისტემისთვის მთლიანად; კვლევის ძირითადი მიმართულების განსაზღვრას, ინფორმაციული დაცვის სისტემის მეთოდების სრულყოფას და საშუალებებით უზრუნველყოფას.

აუცილებელია ერთი ობიექტის ზემოქმედების გათვალისწინება სხვა ობიექტზე. ინფორმაციის დაცვის ამოცანისთვის გადაწყვეტილების მიღება ხდება ან ვარიანტული მეთოდით, ან როცა ეს შესაძლებელი და მიზანშეწონილია ცალკე ნაწილის, ან კიდევ ყველა ობიექტებისათვის ერთად, რომლებიც აფორმირებს ერთიან სისტემას. აქედან წარმოიქმნება ინფორმაციული დაცვის ამოცანები, არა მარტო ცალკეული ობიექტებისათვის, არამედ სისტემის უსაფრთხოებისათვის მთლიანად.

ხშირად აუცილებელია სისტემის ინფომაციული დაცვის მოთხოვნილი ეფექტურობა გამოვთვალოთ (საიმედოობა, მტყუნებამდგრადობა და ა. შ.) დაცვის მექანიზმზე (დმ) არსებული ინფორმაციის ან ინფორმაციული დაცვის სისტემის (იდს) ინფორმაციის საფუძველზე. ამისათვის შეიძლება გამოვიყენოთ სხვადასხვა მიდგომა: ანალიზის ჩატარება ფაქტობრივი მნიშვნელობის საფუძველზე; არსებულ მოწყობილობებზე მიღებული მონაცემების მარტივი პროგნოზირებადი გამოთვლების შესრულება ექსტრაპოლაციის საფუძველზე; პროგრამული მოდელის შექმნა და გაშვება (იმიტაციური მოდელირება). ყველა ჩამოთვლილ მიდგომას აქვს როგორც დადებითი, ასევე უარყოფითი მხარეები. მათი გამოყენება, უმეტეს შემთხვევაში პროექტირების საწყის ეტაპზე რეკომენდირებული არ არის. ამგვარად დამოუკიდებლად იმისა როგორი კარგიც არ უნდა იყოს მოდელი, შედეგის ხარისხი შეზღუდულია საწყისი მონაცემებით. ხშირად პირველ ეტაპზე მიზანშეწონილია (პროგნოზირებადი) შეფასება ჩატარდეს ანალიტიკური მოდელის გამოყენებით,

რომელიც წარმოადგენს განტოლებათა ერთობლიობას. ისინი შეიძლება ამოხსნილ იქნას მოთხოვნილი პარამეტრების მისაღებად. ეს შედეგები აღმოჩნდება საკმაოდ კარგ შესაბამისობაში და რეალურია ისეთ სფეროში, სადაც ფართოდ გამოიყენება კომპიუტერები, ქსელები და ა. შ. ანალიტიკური მეთოდების ნაკლი მდგომარეობს იმაში, რომ ჩვენთვის საინტერესო პარამეტრების მიმართ განტოლებების შედგენა გვიწევს, რიგი დაშვებების მიღებით. მიუხედავად ნაკლისა, მოდელირების ამ მეთოდებით მიღებული შედეგები საკმაოდ ახლოსა იმასთან, რომელიც მიღებულია სხვა უდრო მნიშვნელოვანი მეთოდებით.

ანალიტიკური მიდგომების საფუძველზე დამპროექტებელს ხშირად შეუძლია შეასრულოს გამოთვლები ქაღალდის ნახევზე, რამდენიმე ცხრილის გამოყენებით ან მარტივი კომპიუტერული პროგრამით, მხოლოდ რამდენიმე სტრიქონიანი კოდით.

მეთოდები, რომლებიც საშუალებას გვაძლევს მათემატიკურ მოდელში გავითვალისწინოთ უკვე არსებული ინფორმაციული დაცვის მექანიზმი (დმ), ძალზე მნიშვნელოვანია სისტემის ინფორმაციული დაცულობის რაოდენობრივი შეფასებისათვის. ასეთი სისტემის მუშაობა ახდენს არასანქცირებული წვდომის (ასწ) ნაკადის ფაქტს. იმ შემთხვევაში, როდესაც ხდება არასანქცირებული წვდომის მოთხოვნის აღმოჩენა, ბლოკირების სისტემა შეუდგება მათ განადგურებას, ხოლო თუ ასწ ვერ აღმოაჩენს, სისტემა აგრძელებს ფუნქციონირებას მანამ, სანამ არ მოხდება აღმოჩენილი არასანქცირებული ქმედება.

მათემატიკური მოდელი ზოგადი მიდგომით უნდა განვიხილოთ – სისტემა ნორმალურად ფუნქციონირებს და აბსოლუტურად სუფთაა ინფორმაციასთან წვდომის არასანქცირებული მცდელობის მიმართ. წარმატებული მცდელობა არასანქცირების მხრივ მიიღოს წვდომა ინფორმაციასთან განიხილება, როგორც სისტემის მტყუნება, რომლის ნაწილი აღმოჩნდება მყისიერად, ხოლო ნაწილი წარმოადგენს აღმოუჩენადს და აღმოჩენა ხდება მისი განდევნის პროცესში გამოვლენილი არასანქცირებული ნაკადის შემდეგ (ინფორმაციის შენახვის შემდეგ, პაროლის შეცვლის, ტერმინალების, მომხმარებლის, ფაილების, ჩაწერის აღდგენის დამახინჯებული ინფორმაციის აღდგენის და ა. შ.) ერთნაირი, ერთგვაროვანი სისტემისათვის.

აღვნიშნოთ ნაკადის დროის განაწილების ფუნქცია, როგორც აღმოჩენადი ასევე აღმოუჩენადი არასანქცირებული მცდელობებისათვის $F_1(t)$ და $F_2(t)$ შესაბამისად. ინფორმაციული სისტემა, არასანქცირებადი ქმედების აღმოჩენის შემდეგ, აწარმოებს მის დამუშავებას სპეციალისტების მიერ. ისინი უფლებამოსილია ამ ქმედებათა განადგურებაზე. ვთქვათ ბლოკირების და განადგურების დრო წარმოადგენს შემთხვევით სიდიდეს და მას აქვს ზოგადი განაწილების სახე G(t).

ზემოთქმულიდან გამომდინარე, შეიძლება დავასკვნათ, რომ წარმოქმნილი აღმოჩენადი არასანქცირებადი მცდელობები განპირობებულია ორი ობიექტური მიზეზით: არასანდო და არასრული ინფორმაციის დაცვის სისტემით.

სისტემის ინფორმაციის დაცულობის გათვლისას ძალიან მნიშვნელოვანია, რომ მათემატიკურ მოდელში შედიოდეს სისტემის ინფორმაციის არასრული დაცულობა.

შემოვიღოთ აღნიშვნა P(t) – ალბათობა იმისა, რომ t მომენტში ინფორმაციული სისტემა არ ექვემდებარება არასანქცირებულ ზემოქმედებას იმ პირობით, რომ საწყის მომენტში t=0. ის ასევე არ ექვემდებარებოდა ასეთივე ზემოქმედებას.

ზოგადი ალბათური მსჯელობის საფუძველზე $P(t)$ -ს განსაზღვრისათვის, შეიძლება დაიწეროს შემდეგი ინტეგრალური განტოლება:

$$P(t) = \bar{F}_1(t) - \bar{F}_2(t) + \int_0^t dF_1(u) \int_0^{t-u} p(t-u-v)dG(v), \quad (1)$$

სადაც $\bar{F}_1(t) = 1 - F_1(t)$, $\bar{F}_{21}(t) = 1 - F_2(t)$.

(1)-განტოლებიდან გამომდინარეობს, რომ პირველი წევრები $\bar{F}_1(t) - \bar{F}_2(t)\bar{F}_1(t)$ იმ ხდომილების ალბათობაა, რომლისათვისაც t დროის პერიოდში არ ქონდა ადგილი, როგორც აღმოჩენადი, ასევე აღმოუჩენადი არასანქცირებადი ქმედებებით; მეორე წევრი ინტეგრალქვეშა გამოსახულებაა იმ რთული ხდომილებისა, რომლისთვისაც (u÷u+du) დროის ინტეგრალში სისტემა ექვემდებარება ამ ქმედებას, (v÷v+dv) დროის ინტერვალში ის იყო მდგომარეობაში, რომელიც არ ექვემდებარება დარღვევას, ანუ სისტემა აბსოლუტურად სუფთაა ინფორმაციაზე არასანქცირებული ქმედებებისაგან, t მომენტისათვის ინფორმაციული სისტემა იქნება დაცული ინფორმაციის არასანქცირებული გამოყენებისაგან p(t-u-v) ალბათობით.

თუ გამოვიყენებთ (1)-ის მიმართ ლაპლას-სტილტესის გარდასახვას, შესაბამისი გარდაქმნების შემდეგ მივიღებთ:

$$p(s) = \frac{1 - f_1(S) - f_2(S) + f(S)}{S[1 - f_1(S)\cdot g(S)]} \qquad (2)$$

სადაც

$$f_1(S) = \int_0^\infty \exp(-st)\, dF_1(t); \quad f_1(S') = \int_0^\infty \exp(-st)\, d[F_1(t)\cdot F_2(t)];$$

$$f_2(S) = \int_0^\infty \exp(-st)\, dF_2(t); \quad G(S) = \int_0^\infty \exp(-st)\, dG(t);$$

$$p(S) = \int_0^\infty \exp(-st)\, dP(t).$$

ცხადია, რომ სისტემა ინფორმაციის არასანქცირებული გამოყენების დაცულობის კოეფიციენტი

$$K_დ = K_დ(t) = \frac{\lambda\mu}{(\lambda+\beta)(\lambda+\mu)} + \frac{\lambda\mu}{(\lambda+\mu)(\mu-\beta)} e^{-(\lambda+\mu)t} + \frac{\beta}{(\lambda+\mu)}\left[\frac{\mu}{\lambda+\beta} + \frac{\lambda}{\beta-\mu}\right] e^{-(\lambda+\beta)t} \qquad (3)$$

თუ აღვნიშნავთ $T_{აღ} = -f'_1(0)$, $T_{აღმ} = -f'_2(0)$, $-g'(0) = T_{ბლ}$ და $T = -f'(0)$

აღმოჩენად $T_{აღ}$, აღმოუჩენად $T_{აღმ}$, ბლოკირებისა და განადგურების $T_{ბლ} = -g'(0)$ საშუალო დროებს მაშინ (3) მიიღებს შემდეგ სახეს:

$$K_დ = \frac{T_{აღ} + T_{აღმ} + T}{T_{აღ} + T_{ბლ}} \qquad (4)$$

კერძო შემთხვევისათვისმ, როცა აღმოჩენადი, აღმოუჩენადი არასანქცირებული ქმედებები, ასევე ბლეირებისა და განადგურების დროის განაწილების ფუნქციებს აქვს პუასონის სახე λ, β და პარამეტრებით $K(t)$ ინფორმაციული დაცვის ფუნქციას აქვს სახე:

$$K_დ(t) = \frac{\lambda\mu}{(\lambda+\beta)(\lambda+\mu)} + \frac{\lambda\mu}{(\lambda+\mu)(\mu-\beta)} e^{-(\lambda+\mu)t} + \frac{\beta}{(\lambda+\mu)}\left[\frac{\mu}{\lambda+\beta} + \frac{\lambda}{\beta-\mu}\right] e^{-(\lambda+\beta)t} \qquad (5)$$

3. დასკვნა

ამგვარად, ინფორმაციის ეფექტურად დაცვის მიზნით, ზემოთ აღწერილი მათემატიკური მოდელის (ინტეგრალური განტოლების) მიდგომით, რომელიც წარმოადგენს უაღრესად ზოგადს, შეიძლება გამოყენებულ იქნას ინფორმაციული სისტემის აღდგენის დროს ზოგადი განაწილების შემთხვევაში, როგორც ითქვა ის იძლევა ინფორმაციული სისტემის დაცვის მექანიზმის ოპტიმალური შერჩევის გადაწყვეტილების საშუალებას.

ლიტერატურა:

1. Карпов В. В. Вероятная модель оценок защищенности средств вычислительной техники с аппаратно-программным комплексом защиты информации от несанкционированного доступа „Программные продукты и системы – 2000“, №1, 6, 31

2. Беляев Ю. К. Предельные теоремы для передающих потоков – М.: Советское радио, 1967

3. Кокс Д. Смит В. Теория восстановления. М.: Советское радио, 1967.

PERFORMANCE PROBLEM STATEMENT FOR PROTECTION OF INFORMATION SYSTEM

Shonia Otar, Shonia Luka
Georgian Technical University

Summary

We discuss the specifics of computing tasks on protection of complex information systems. Together with the study of the general theoretical analysis methods to protect information system, is considered a special device that can be used with great efficiency to information system security.

ЭФФЕКТИВНОСТЬ ПОСТАНОВКИ ЗАДАЧИ ПО ЗАЩИТЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Шония О., Шония Л.
Грузинский Технический Университет

Резюме

В работе показана специфика расчетных задач по защите сложных информационных систем. Вместе с изучением общетеоретических методов анализа по защите информационной системы, рассмотрен особый прием, который может быть использован с особой эффективностью и в системах информационной безопасности.