ინფორმაციის დაცვის მოდელი ავტომატიზებულ საბანკო სისტემაში

ოთარ შონია, მამუკა შონია, გიორგი ცინარიძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია ავტომატიზებული საბანკო სისტემის ინფორმაციის დაცვის უზრუნველყოფის შესაძლებლობა შეზღუდული რესურსების პირობებში. წარმოდგენილია ინფორმაციის დაცვის მოდელი, რომელიც საშუალებას იძლევა მოცემული (შეზღუდული) რესურსების პირობებში არ გაიზარდოს მნიშვნელოვანი ინფორმაციის კომპრომეტირების რისკი.

საკვანძო სიტყვები: ავტომატიზებული სისტემა. კონფიდენციალური ინფორმაცია. ინფორმაციის დაცვა. ბანკი.

1. შესავალი

საბანკო საკრედიტო ორგანიზაციებისათვის თანამედროვე ინფორმაციული ტექნოლოგიების, ავტომატიზებული სისტემების გამოყენება არსებობის და ეფექტური ფუნქციონირების აუცილებელ საშუალებას წარმოადგენს. ამიტომ, ცხადია, განსაკუთრებულ ყურადრებას მოითხოვს ავტომატიზებულ საბანკო სისტემებში ინფორმაციის დაცვის საჭირო დონეზე ორგანიზება [1,2,3].

2. ძირითადი ნაწილი

საბანკო ინფორმაციის დაცის სისტემის პროექტირების საწყის ეტაპზე აუცილებელია შეფასდეს ინფორმაციის, როგორც დაცვის ობიექტის ღირებულება V და სიცოცხლის დრო $T_{ას}$. ერთდროულად უნდა განისაზღვროს დაცვის ობიექტზე შესაძლო მუქარათა სიმრავლე, რომელთა გამოჩენის ალბათობები $\{P_i\}$, $i=\overline{1,N}$, მეტი იქნება წინასწარ მოცემულ ზღვრულ $P_{ზღ}$ მნიშვნელობაზე (ვუწოდოთ მას რისკი). აქვე უნდა იყოს მოცემული ის ეკონომიკური რესურსები R_0, რისი გაღებაც შეუძლია ბანკს კონკრეტული დაცვის სისტემის შექმნაზე.

ცხადია, რეალურად დაცვის სისტემის შექმნისათვის საჭირო რესურსები $R_რ$ ფუნქციაა ობიექტის V ღირებულებისა და მუქარათა ალბათობებისა:

$$R_რ = R_რ(V,\{P_i\}) \tag{1}$$

ამიტომ, $R_რ$-ის დაყვანა R_0 მნიშვნელობამდე ძირითადად დამოკიდებულია ინფორმაციის დაცვის კონცეფციის შერჩევაზე და რისკის დონეზე. მაგრამ, ეს სრულებით არ ნიშნავს იმას, რომ შესაძლებელი იქნება ისეთი კონცეფციის შერცევა, რომლის დროსაც დაცული იქნება პირობა

$$R_რ(V,\{P_i\}) \le R_0 \tag{2}$$

ამ პირობის შესრულება შეიძლება უფრო გაიოლდეს, თუ მოხერხდება ინფორმაცია როგორც დაცვის ობიექტი O დავყოთ სხვადასხვა ღირებულების მქონე ობიექტების სიმრავლედ $\{O_j\}, j=\overline{1,J}$, რომელთა ღირებულებები და სიცოცხლის დროები იქნება შესაბამისად $\{V_j\}$ და $\{t_{ასj}\}$. ასე მაგალითად, ვთქვათ ავტომატიზებულ საბანკო სისტემაში (ასს) კონფიდენციალური საბანკო

ინფორმაცია თავისი ღირებულებიდან (მნიშვნელობიდან) გამომდინარე დაყოფილია სხვადასხვა საიდუმლოების გარაფის მქონე ობიექტებად – კონფიდენციალურ, სრულიად საიდუმლო და განსაკუთრებული მნიშვნელობის მქონე ობიექტებად. იმ შემთხვევაში, თუ (2) პირობის შესრულება $t_{აsj}$ გათვალისწინების გარეშე ვერ ხერხდება, მაშინ შემოგვაქვს დროითი შეზღუდვა $t_{ია0} << t_{აsj}$, რომელიც წარმოადგენს არა საერთოდ O_j ობიექტის სიცოცხლის დროს, არამედ მისი ასს-ში მისაწვდომობის (ყოფნის) და დამუშავების დროს. ვგულისხმობთ, რომ ვთქვათ განსაკუთრებული მნიშვნელობის ინფორმაცია ასს-ში შეიძლება მუშავდებოდეს და ხელმისაწვდომი იყოს მხოლოდ $t^{ზ}_{ია0}$ დროის განმავლობაში. გარანტირებული დაცვის სტრატეგიას დროითი მაჩვენებლის მიხედვით ექნება სახე:

$$T_{აღბ} / t_{გარ} < 1 \tag{3}$$

სადაც $T_{აღბ}$ – დაცვის სისტემის მიერ არასანქცირებულად შეღწევის (აშ) მცდელობის აღმოჩენის და ბლოკირების დროა; $t_{გარ}$ – ბოროტგანმზრახველის მიერ დაცვის ბარიერის გარღვევის მოსალოდნელი (სავარაუდო) დროა.

ბოროტგამზრახველის მიერ ასს დაცვის ბარიერის დაძლევის ალბათობა შეიძლება ვიანგარიშოთ ასე:

$$P_{გარi} = 1 - \frac{t_{გარ}}{T_{აღბ}} \tag{4}$$

სადაც i-ინდექსი მიუთითებს კონკრეტულ i-ურ მუქარაზე.

თუ ასს-ის მუშაობის სადღეღამისო პერიოდს $T_ჳ$ დავყოფთ $t_{აsj}$ მონაკვეთად

$$n = T_ჳ / t_{აsj} \tag{5}$$

და ჩავთვლით, რომ დროის ნებისმიერ მომენტისათვის (1,2,....n) ასს-ში დაცვის O_j ობიექტის დამუშავების პროცესის არსებობის და მისაწვდომობის ალბათობა ერთნაირია, მაშინ ბოროტგანმზრახველისათვის აუცილებელია, რომ დაცვის ბარიერის დაძლევისას სისტემაში მიმდინარეობსდეს მისთვის საინტერესო O_j ობიექტის დამუშავება, ამისი ალბათობა კი ტოლია

$$P_{0j} = 1/n \tag{6}$$

ე. ი. თავდასხმის წარმატებით დაგვირგვინების ალბათობა იქნება:

$$P'_{გარi} = P_{0j} \cdot P_{გარi} = P_{გარi} / n \tag{7}$$

მივიღეთ, რომ ბოროტგანმზრახველის მიერ საჭირო ინფორმაციის ხელში ჩაგდების ალბათობა n -ჯერ მცირდება. ამ შემთხვევაში შეიძლება ვთქვათ, რომ დაცვის წარმოდგენილი კონცეფცია საშუალებას იძლევა გაძლიერდეს i-ური მუქარისაგან დაცვა, რაც დაცვის შესაბამის მექანიზმზე დანახარჯების შემცირების ექვივალენტურია. ასეთი ანალიზი უნდა ჩატარდეს ყველა O_j და $P_{გარi}$-თვის.

ასეთი მიდგომა საშუალებას იძლევა ასს-ის, მისი თითოეული ობიექტის დაცვის სისტემა გავხადოთ თვითდაცვადი, დაცვის სისტემის დინამიური ცვლით, რაც სრულად შეესაბამება თანამედროვე კომპიუტერულ სისტემებში დაცული გამოთვლების ახალ მოდელს, რომელიც

ემყარება ბოლო 30 წლის განმავლობაში ამ სფეროში დაგროვილ ფუნდამენტურ ცოდნასა და გამოცდილებას და ითვალისწინებს:

- თვითდაცვადი სისტემების შექმნას;
- დაცვის მძლავრი მექანიზმების გამოყენებას;
- უსაფრთხოების უზრუნველყოფის დინამიურად ცვლადი სტრატეგიის გამოყენებას;
- მობილურობის და დიდ ტერიტორიაზე განაწილების ფაქტორების გათვალისწინებას.

3. დასკვნა

ნებისმიერი ავტომატიზებული სისტემის ინფორმაციის დაცვა აუცილებლად მოითხოვს, პირველ რიგში, შეფასდეს თვით ინფორმაცია როგორც დაცვის ობიექტი, თანაც მიზანშეწონილია მოხდეს მისი დაყოფა სხვადასხვა კატეგორიის დასაცავ ობიექტებად, რაც აადვილებს ასს-ში თვითდაცვის პრინციპის გამოყენებას და შეზღუდული რესურსების პირობებში უზრუნველყოფს მნიშვნელოვანი ინფორმაციის საჭირო დონით დაცვას.

ლიტერატურა

1. Банковские риски: учебное пособие / кол. авторов, под ред. О. И. Лаврушина и Н. И. Валенцевой – 2-е изд., стер. – М.: КНОРУС, 2008;
2. Аудит информационной безопасности: глобальное исследование КПРМГ. – http://goap.ru.
3. Мельников В. В. Защита информации в компьютерных системах. – М.: „Финансы и статистика; Электроинформ, 1997.

MODEL OF INFORMATION SAFETY OF AUTOMATED BANK SYSTEM

Shonia Otar, Shonia Mamuka, Tsinaridze Giorgi
Technical University of Georgia

Summary

The article concerns to the possibility of information safety of automated bank system under the limited terms. The article represents the model of information safety resisting the growth of risk of important information distortion under the conditions of given (limited) resources.

МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ БАНКОВСКОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Шония О., Шония М., Цинаридзе Г.
Грузинский Технический Университет

Резюме

Рассмотрена возможность обеспечения защиты информации автоматизированной банковской системы в условиях ограниченных возможностей. Представлена модель защиты информации, которая препятствует росту риска искажения важной информации в условиях данных (ограниченных) ресурсов.