ინფორმაციული ტექნოლოგიები ბიზნეს-ინჟინერინგში

სხვადასხვა ხარისხის კონფიდენციალური ინფორმაციის დაცვის მოდელი

თინათინ კაიშური, გიორგი ჯაფარიძე, ნინო ყველაიძე, მზიური ბარბაქაძე

კონფიდენციალური ინფორმაციის დაცვის მექანიზმები მიმართულია **ინფორმაციული უსაფრთხოების** უზრუნველყოფის ცალკეული ასპექტების რეალიზებაზე, რაც ვერ უზრუნველყოფს დაცვის სისტემის მართვის ანალიზისა და სინთეზის ამოცანების კომპლექსურ გადაწყვეტას და ოპტიმალური დაცული ინფორმაციული სისტემებისა და მონაცემთა ბაზების შექმნას.

ამიტომ დიდი ყურადღება ექცევა ინფორმაციული ტექნოლოგიების დაცვის საკითხებს. აქ ძირითადი მოთხოვნაა ინფორმაციული პროდუქტების ინტეგრირებული დაცვის სისტემების შექმნა, რომლებიც ორგანიზებულია მონაცემთა ბაზების სახით.

მონაცემთა ბაზებში ინახება მრავალფეროვანი ინფორმაცია არა მარტო წარმოდგენის ფორმის თვალსაზრისით, არამედ კონფიდენციალობის დონის მიხედვითაც. კორპორაციული, ინფორმაციული, საერთო და შეზღუდული გამოყენების მუქარის ანალიზმა გვიჩვენა, რომ ინფორმაციული დაცვის სისტემების ორგანიზაციისათვის აუცილებელია დამუშავდეს ინფორმაციული ტექნოლოგია, რომელშიც შეზღუდული მოხმარების დოკუმენტებთან ერთად გათვალისწინებული იქნება მუშაობის მოთხოვნები. ეს მოთხოვნები სახელმწიფოში შესაბამისი კანონით, კანონებით ან სხვა ნორმატიული დოკუმენტების უნდა იყოს განსაზღვრული. ჩვენ მიერ წარმოდგენილი ტექნოლოგია უზრუნველყოფს ინფორმაციასთან დაშვების მრავალდონიან კონტროლს კრიპტოგრაფიული დაცვით, რაც საშუალებას იძლევა ღია საკომუნიკაციო არხებით შენახული და გადაცემული სხვადასხვა კონფიდენციალობის მქონე ინფორმაცია მაღალი საიმედოობით დავიცვათ.

ჩვენ ინფორმაციის დაცვის კონფიდენციალურ მოდელში ვგულისხმობთ პროცესს, რომელიც შედგება ინფორმაციული პროდუქტების (მონაცემთა ბაზები, ელექტრონული დოკუმენტები, შეტყობინებები და ა. შ.) დაცული ოპერაციებისაგან. მრავალდონიანი დაცვისას ხდება სხვადასხვა დონისა და კატეგორიის მონაცემების შენახვა და დამუშავება მაშინ, როდესაც არსებობს პერსონალის სხვადასხვა დონე. ამით გამოირიცხება ინფორმაციასთან იმ პირების დაშვება, რომელებიც არ პასუხობენ საიდუმლოობის შესაბამის დონეს.

კვლევის ობიექტი არის ინფორმაცია კონფიდენციალობის სხვადასხვა ხარისხით. ის ინახება მონაცემთა ბაზებში და გადაიცემა კავშირის ღია არხებით. ჩვენი მიზანია გადაწყდეს კონფიდენციალობის შენარჩუნების ამოცანა შეზღუდული მოხმარების ინფორმაციისთვის და მთლიანობის ურღვევობის ამოცანის მხარდაჭერა საერთო ხელმისაწვდომი ინფორმაციისათვის. სხვადასხვა კონფიდენციალობის ხარისხის ინფორმაციული რესურსების დაცვისას ძირითად მოდელებს შორის ურთიერთკავშირი მიიღწევა ინფორმაციული უსაფრთხოების უზრუნველყოფის თითოეული ტექნოლოგიური ეტაპის ამოცანების გადაწყვეტის შედეგების გამოყენებით, რომლებიც სტრუქტურირებული და ორგანიზებულია სპეციალურად დაპროექტებული მონაცემთა ბაზებისა და მეტამონაცემების ბაზების სახით.

მონაცემთა ბაზებში შენახული ინტეგრირებული ინფორმაციის კონფიდენციალობის უზრუნველყოფა მიიღწევა ინფორმაციის დაცვის მართვის ამოცანების ეტაპობრივი გადაწყვეტით. ამაში შედის დაშვების მანდატური გამოვლინით სისტემის აგების მოდელი და კრიპტოსისტემების აგების მოდელი. მანდატური გამოვლინით სისტემის მოდელში მოიაზრება დაცვის სუბიექტების და ობიექტების დამუშავება, მონაცემთა ბაზებთან დაშვების სახეებისა და უფლებების კონტროლი და ანალიზი, მრავალდონიანი დაცვით მონაცემთა ბაზების შექმნა და ფუნქციონირება, ან-

გარიშების გენერირება. კრიპტოსისტემების აგების მოდელში შედის მონაცემების დაშიფვრა საიმედოობის მოცემული მახასიათებლებით, ასევე გასაღებების გენერაცია და გავრცელება.

მონაცემთა მთლიანობის კონტროლი ხორციელდება ხარისხის შემდეგი კრიტერიუმების მიხედვით: სისრულე (მიმდინარეობს მონაცემთა სტრუქტურის სრული აღწერის შემოწმება), არაწინააღმდეგობრიობა (მოწმდება მონაცემებს შორის ლოგიკური კავშირები, გამოვლინდება ჭარბი და წინააღმდეგობრივი აღწერები, ხდება მნიშვნელობების დიაპაზონის საზღვრების კონტროლი) და აქტუალობა (მონაცემთა ბაზებში ხდება ერთდროული და ცალკეული ცვლილებების შეყვანის კონტროლი).

მრავალდონიანი დაცვის სისტემის ბირთვს წარმოადგენს მოთხოვნების დამუშავების მონიტორი, რომელიც ამოწმებს მომხმარებლის ყოველ მიმართვას მონაცემებთან ან პროგრამასთან, თუ რამდენად შეესაბამებიან ისინი იმ მოქმედებების სიას, რომელიც დაშვებულია მომხმარებლისათვის. მრავალდონიანი დაცვის სისტემა ლოგიკური დაშვების კონტროლისას საშუალებას იძლევა თავიდან იქნას აცილებული გაურკვევლობის ელემენტები.

დაშვების მანდატური გამოჯვნისას მრავალდონიანი დაცვით მონაცემთა ბაზებში ხდება ფორმირებადი დაცვის სუბიექტებისა და ობიექტებისათვის ხისებრი სტრუქტურის მინიჭება, რაც იძლევა დაშვების მართვის ოპტიმალურ სურათს და უზრუნველყოფს კორექტული მართვისათვის დაშვების ისეთი წესების რეალიზებას, როგორიცაა "ახალი ობიექტების შექმნის უფლება", "დაშვების უფლებების გადაცემა სუბიექტებს შორის", "მოთხოვნის რეალიზაციის უფლება". სუბიექტის მოთხოვნის რეალიზაციის უფლების შემოწმება აუცილებალია იმ შემთხვევაში, როდესაც დაშვების საკმარისი კატეგორიისას სუბიექტს შეიძლება ჰქონდეს მინიჭებული უფლება გაეცნოს კონკრეტულ შემოსულ დოკუმენტს საიდუმლოობის შედარებითი ხარისხით.

გათვალისწინებულია აგრეთვე დაცვის სუბიექტებისა და ობიექტებისათვის ძირითადი პარამეტრების მინიჭება მათი ინფორმაციული დაცულობის დონის მიხედვით. დაცვის სუბიექტისათვის ინფორმაციის ნაწილი საიმედოდ უნდა იყოს დაშიფრული. მაღალეფექტური და საიმედო გამოთვლითი სისტემების პროექტირებისას სიმეტრიული კრიპტოსისტემების მიმართ გამოიყენება შიფრაციისა და დეშიფრაციისადმი არატრადიციული მიდგომა, რომელიც საშუალებას იძლევა მოვახდინოთ კრიპტოალგორითმის საიდუმლოობის ვარირება ნებისმიერი კლასის საიდუმლო ინფორმაციის დაცვის დონის გათვალისწინებით.

შემოთავაზებული დაშიფვრის არატრადიციული მეთოდით მიიღწევა კრიპტომდგრადობა, რომელის დამოკიდებულია არა მარტო გასაღების სიგრძეზე, არამედ შერეული პოლინომიალური საფუძვლის სისტემაზე.

შეზღუდული მოხმარების ინფორმაციის დამუშავების, შენახვის ან გადაცემისას გამოიყენება ისეთი მექანიზმები და საშუალებები, რომლებიც ერთდროულად უზრუნველყოფენ დაცულობის საჭირო დონეს და აკმაყოფილებს შეზღუდვებს ამ საშუალებების და პროექტებისა და ექსპლუატაციის ღირებულებაზე.

შექმნილმა მონაცემთა ბაზამ უნდა უზრუნველყოს დაცვის ტექნოლოგიის საიმედო ფუნქციონირება, მაგრამ უნდა გავითვალისწინოთ ისიც, რომ თვითონაც შეიძლება გახდნენ ბოროტგანმზრახველების ზემოქმედების ობიექტები.

ინფორმაციის დაცვის მართვის მოდელირებისას უნდა განისაზღვროს დასახარჯი რესურსების ჩამონათვალი და მათი შემდგომი გამოყენების ოპტიმალური ვარიანტები. უნდა განისაზღვროს აგრეთვე დაცვის უზრუნველყოფის ღირებულება, დაცვის სისტემის ეფექტურობა, დაცვისათვის გამოყენებული ყველა მეთოდის გატეხის ალბათობა და ღირებულება, დაცვის ყველა მეთოდის გატეხვით მიყენებული ზარალის სიდიდე.

ჩვენ მიერ შემოთავაზებულ მრავალდონიან დაცვის მოდელში რეალიზებულია დაშვების უფლებათა გაფართოებული სია და დაშვების უფლებების მართვა არსებული ნორმატიული დოკუმენტებისა და ორგანიზაციული ტიპის განაწილებულ მონაცემთა ბაზებში კრიტიკული ინფორმაციის დამუშავების წესების დაცვით. დამუშავებულია დაცვის სუბიექტებისა და ობიექტების იერარქიების გამოყოფის პროცედურები, აგრეთვე სუბიექტების, როგორც ობიექტების მფლობელების ქვესიმრავლეების, დანაწილება ინტერფეისის ნდობით აღჭურვილ და სისტემის მოშორებულ აბონენტებს შორის.

კრიპტოგრაფიული დაცვის სისტემა, რომელიც ინტეგრებულია დაშვების მანდატურ გამოჯვნასთან, საშუალებას იძლება მოცემულ იქნას კრიპტოგარდასახვის საიმედოობის მახასიათებლები შენახული ან გადასაცემი ინფორმაციის საიდუმლოობის ხარისხის მიხედვით.

შემოთავაზებული ალგორითმების მაღალი კრიპტოგრადობა საშუალებას იძლევა უზრუნველყოფილი იქნას შეზღუდული მოხმარების ინფორმაციის კონფიდენციალობა და მთლიანობა მისი შენახვისას და

ღია კავშირით გადაცემისას. დამუშავებული მოდელები და მეთოდები ითვალისწინებს მონაცემთა ბაზების მომხმარებლების საგნობრივი არის თავისებურებებს და აპარატურულ-პროგრამული პლატფორმების მახასიათებლებს, ინფორმაციული რესურსების საიდუმლოობის დონის მიმართ მოთხოვნებს და კონფიდენციალურ ინფორმაციასთან მომხმარებლების დაშვების უფლებებს.

ლიტერატურა:

1. Конявский В. А., Гадасин В. А., Основы понимания феномена электронного обмена информацией. – Минск: Беллифонд, 2004.
2. Конявский В. А., Гадасин В. А., Информационные технологии как объект защиты и классификация антивирусных программ // Управление защитой информации. 2007, т. 11, №4.
3. Защита от несанкционированного доступа к информации. Термины и определения: Рук. док-т // Сб. рук. док-в по защите информации от несанкционированного доступа. М.: Гостехкомиссия России. 1928.
4. Горковенко Е. В. Контроль и анализ задания видов и прав доступа;
5. O.Shonia, T. Kaishauri, I. Kartvelishvili, Software Complex of Automated System, Supporting Security of Wireless Networks, Georgian International Journal of Science and Technology, Nova Science Publishers, Volume 4, Issue 4, 1, 2 (2012)https:www.novapublishers.com/catalog/product info.php? products id=34525
6. ო. შონია, თ. შეროზია, ინფორმაციული ტექნოლოგიები და უსაფრთხოება, სტუ, დამხმარე სახელმძღვანელო, 2008.
7. გ. გოგიჩაიშვილი, ო. შონია, კ. ოდიშარია, ინფორმაციის დაცვა ავტომატიზებულ სისტემებში, დამხმარე სახელმძღვანელო, 2008.

Protection Model of Confidential Information of Different Levels

SUMMARY

Protection mechanisms of confidential information ensure security of information. Complex solution of the tasks of analysis and synthesis of protection system management requires creation of optimally protected informational systems and data bases. By multi-level protection, tree-shaped structure is assigned to the formed protection subjects and objects, providingoptimal picture of access and ensuring realization of access rules for correct management. High-level protection of the proposed algorithms allows ensuring of confidentiality and integrity of information of limited use in the case of its storage and transfer through open connection.