ორგანიზაციაში ინფორმაციის უსაფრთხოების მხარდამჭერი პროგრამული საშუალებები

ნინო თოფურია, მაკა ლომიძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

წარმოდეგენილია პროგრამული პროდუქტები, რომლებიც გამოიყენება ინფორმაციული უსაფრთხოების სფეროში არსებული მართვის ამოცანების გადასაწყვეტად. განხილულია სისტემა „COBRA" და კომპანიის ინფორმაციული უსაფრთხოების პოლიტიკის მართვის პროგრამული კომპლექსი „КОНДОР+". ეს პროგრამები შეტანილი ინფორმაციის საფუძველზე ავტომატურ რეჟიმში ახდენენ ანგარიშგებების ფორმირებას, რომელიც შეესაბამება ISO17799 სტანდარტის მოთხოვნებს.

საკვანძო სიტყვები: ინფორმაციული უსაფრთხოება, ინფორმაციული უსაფრთხოების დაცვის პროგრამული საშუალებები, ISO17799 სტანდარტი.

1. შესავალი

ორგანიზაციაში საკუთარი ინფორმაციის უსაფრთხოების დაცვა, როგორც წესი, წარმოადგენს საერთო მართვის განუყოფელ ნაწილს. სისტემური მიზანმიმართული მოქმედების აუცილებლობა მით უფრო მატულობს, რაც მაღალია ორგანიზაციაში ბიზნეს-პროცესების ავტომატიზაციის დონე. ორგანიზაციის ქვეშ იგულისხმება ნებისმიერი ფირმა, საწარმო, კომპანია, დაწესებულება, უწყება, რომელსაც გააჩნია ფინანსური რესურსები და აქვს საკუთარი ორგანიზაციული-საშტატო სტრუქტურა. ინფორმაციის სახით არსებული არამატერიალური აქტივები ასეთ პირობებში თამაშობენ ერთ-ერთ ძირითად როლს კონკურენტუნარიანობის ამაღლებისა და ბიზნესის განვითარების კუთხით.

ინფორმაციული უსაფრთხოება ასევე მნიშვნელოვანია არამარტო ორგანიზაციის სტრატეგიული განვითარებისა და ძირითადი პროდუქტის შესაქმნელად, არამედ ბიზნეს-პროცესების ისეთი ცალკეული მიმართულებებისათვის, როგორებიცაა კომერციული მოლაპარაკებები, კონტრაქტის პირობები, ფასების პოლიტიკა და სხვ.

ამას გარდა, ორგანიზაციის ინფორმაციული ნაკადის შემადგენელი შეიძლება იყოს არა მარტო კომერციული, არამედ სახელმწიფო მნიშვნელობის საიდუმლო, ასევე სხვა სახის კონფიდენციალური ინფორმაცია (საბანკო ანგარიშები, სამედიცინო, სანოტარო, საადვოკატო, სადაზღვევო, საგამოძიებო, სასამართლო, გაშვილების საიდუმლო, კომპანიების ინტელექტუალური საკუთრება და სხვ.)

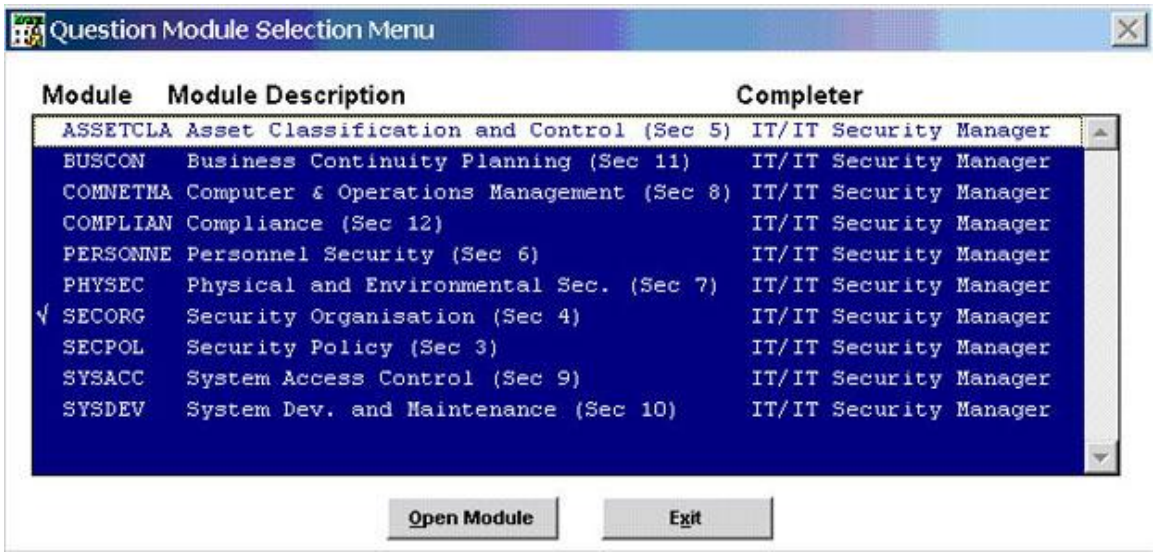
2. ძირითადი ნაწილი

ორგანიზაციაში ინფორმაციული უსაფრთხოების უზრუნველყოფა შესაძლებელია სხვადასხვა ტიპის პროგრამული პაკეტებით. პრაქტიკულად ყველა თანამედროვე პროგრამულ პროდუქტს აქვს „ჩაშენებული" საშუალებები, რომლებსაც შეუძლიათ მკაცრად განსაზღვრონ ამა თუ იმ მომხმარებლის უფლებები, გამიჯნონ ინფორმაციასთან მიმარვა, გაანაწილონ სისტემური რესურსების გამოყენების წესები და შემოიტანონ სხვა შეზღუდვები, რომლებიც უზრუნველყოფს ინფორმაციული უზრუნველყოფის პოლიტიკის რეალიზაციას.

უფრო განვითარებული პროგრამული პროდუქტების კონცეფცია კი ეფუძნება ინტერაქტიულ ინტელექტუალურ ანალიზს და უსაფრთხოების პოლიტიკის სრულყოფილებას. იგულისხმება, რომ მენეჯერს თავდაპირველად შეაქვს სისტემაში (პასუხობს დასმულ შეკითხვებს) ყველა აუცილებელი ინფორმაცია, რომელიც ასახავს ინფორმაციული უსაფრთხოების მდგომარეობას ორგანიზაციაში.

შედეგად ღებულობს დეტალურ ანგარიშგებას ინფორმაციული უსაფრთხოების მდგომარეობის და საერთაშორისო სტანდარტებთან შესაბამისობის შესახების, რეკომენდაციებს მოქმედი უსაფრთხოების პოლიტიკის დახვეწაზე და სხვა ანგარიშებს. ამგვარად, პროგრამული უზრუნველყოფა საშუალებას იძლევა ერთ პროცესში მოექცეს ორგანიზაციის შესახებ პირველადი ინფორმაციის მოგროვება, ინფორმაციული უსაფრთხოების უზრუნველყოფის ფაქტობრივი დონის ანალიზი, დოკუმენტაციის შემუშავება და მართვის მეთოდების ადაპტაცია განსაზღვრულ მოთხოვნებთან (მაგალითად, ISO 17799 სტანდარტთან).

ერთ-ერთი ასეთი პროდუქტია სისტემა „COBRA", რომელიც შექმნა ბრიტანულმა კომპანიამ „C&A Systems Security Ltd." მას აქვს ორი ვარიანტი: შემოკლებული ვერსია შეიცავს მოდულს „COBRA ISO17799 Consultant". სრულ ვერსიაში წარმოდგენილია რისკების ანალიზის დამატებით საშუალებები "Risk Consultant" და სპეციალური მოდული „Module Manager". ამ საშუალებებით შესაძლებელია ინფორმაციული უსაფრთხოების მდგომარეობის შესახებ საკუთარი ცოდნის ბაზების შექმნა და მათი მოდიფიკაცია საჭიროების შემთხვევაში. სისტემის საბაზო მოდულის დანიშნულებაა შეაფასოს, თუ რამდენად შეესაბამება ინფორმაციული უსაფრთხოების მდგომარეობა ISO17799 სტანდარტის მოთხოვნებს. პირველ ეტაპზე მუშაობას იწყებს მოდული „Question Module". ესაა შეკითხვების ნაკრები, რომელიც აღწერს პერსონალის უსაფრთხოებას, უწყვეტი მუშაობის დაგეგმვას, უსაფრთხოების პოლიტიკას და ა.შ. (ნახ.1).

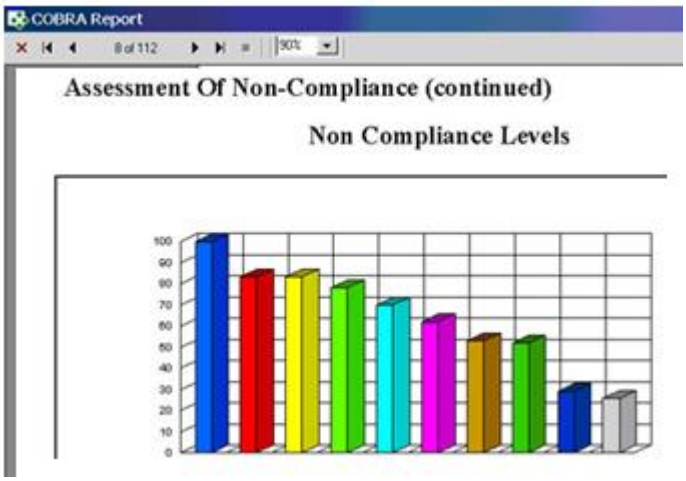


ნახ.1. სისტემა "COBRA"-ს შეკითხვების ჯგუფი

ასეთი სახით შეტანილი ინფორმაციის საფუძველზე მიიღება ანგარიში ინფორმაციული უსაფრთხოების მდგომარეობის შესახებ, რომელიც შედგება ხუთი ნაწილისაგან: შესავალი; შესრულებული სამუშაოს ძირითადი მიმართულებების ჩამონათვალი; არა შესაბამისობის დონის შეფასება; ორგანიზაციული ღონისძიებების ჩამონათვალი, რომელთა რეალიზაციაც აუცილებელია სტანდარტების მოთხოვნების შესასრულებლად და დასმული შეკითხვებისა და მონაცემების ჩამონათვალი.

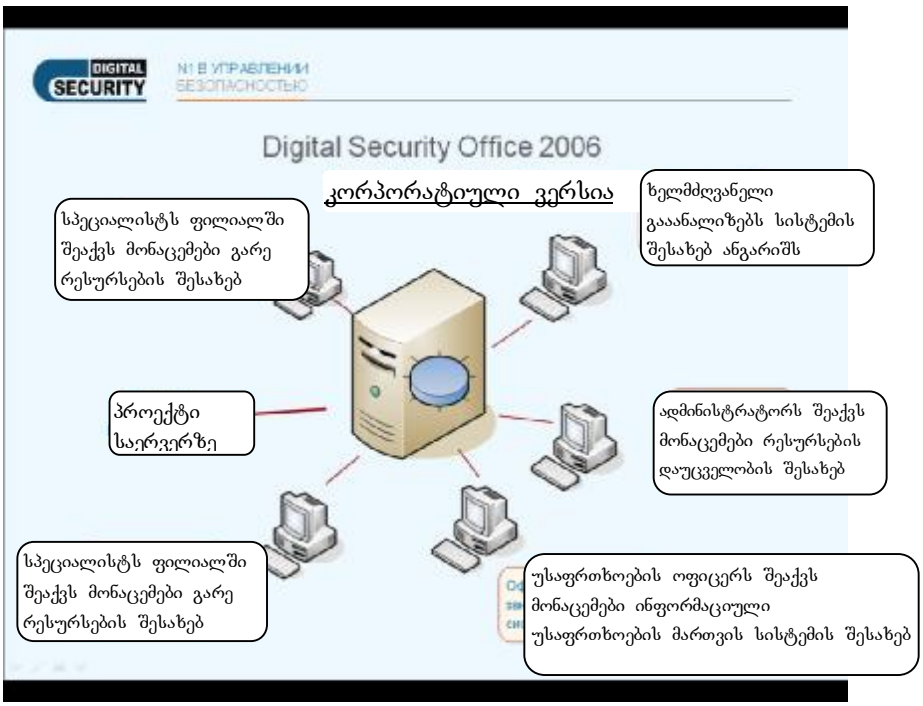
ტექსტური ნაწილის გარდა, ანგარიშში შეიძლება ჩართული იყოს გრაფიკები, რომლებიც ნათლად ასახავს სტანდარტის მოთხოვნების შესრულების დონეს (ნახ.2).

ასეთი პროგრამული პროდუქტების რიცხვს ასევე მიეკუთვნება კომპანიის ინფორმაციული უსაფრთხოების პოლიტიკის მართვის პროგრამული კომპლექსი „КОНДОР+". იგი შექმნილია სანკტ-პეტერბურგის ფირმა "Digital Security"-ის მიერ და სისტემა „COBRA"-ს ანალოგიურია.



ნახ.2. სისტემა "COBRA"-ს მიერ სტანდარტის მოთხოვნების შესრულების ხარისხის მაჩვენებელი გრაფიკი

მე-3-ე ნახაზზე ასახულია Digital Security Office სისტემის მუშაობის პროცესი:



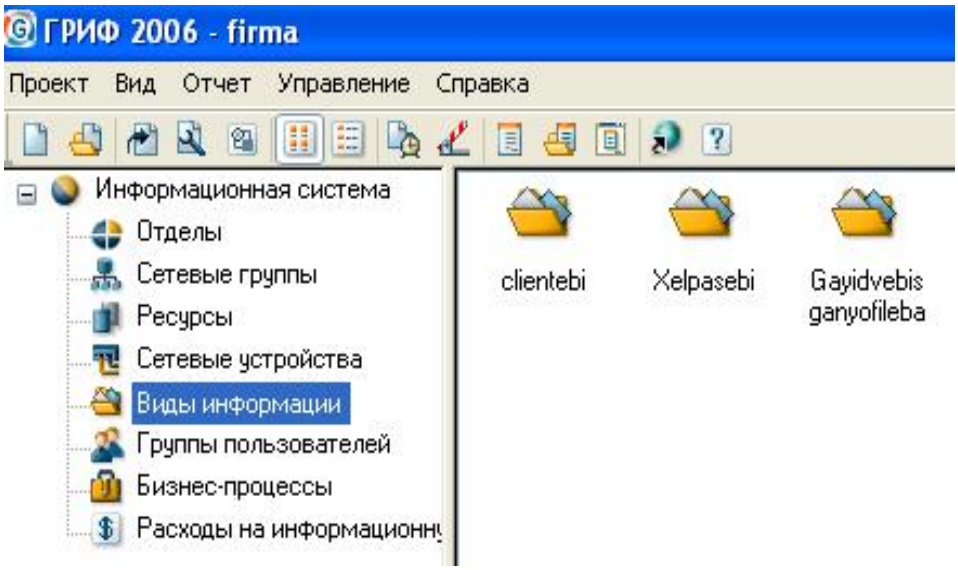
ნახ.3. Digital Security Office სისტემის მუშაობის პროცესი

მოცემული პროგრამული კომპლექსი, მოიცავს ოთხ ფუნქციონალურ მოდულს:

- „პროექტი" – განკუთვნილია ინფორმაციული უსაფრთხოების მდგომარეობის შესახებ ინფორმაციის შესაგროვებლად;
- „ანგარიშები" – განკუთვნილია შეგროვებული მონაცემების საფუძველზე ინფორმაციული უსაფრთხოების დეტალური ანალიზისათვის;
- „დიაგრამები/სტატისტიკა – განკუთვნილია ინფორმაციული უსაფრთხოების მდგომარეობის შემაჯამებელი ანალიზისათვის;

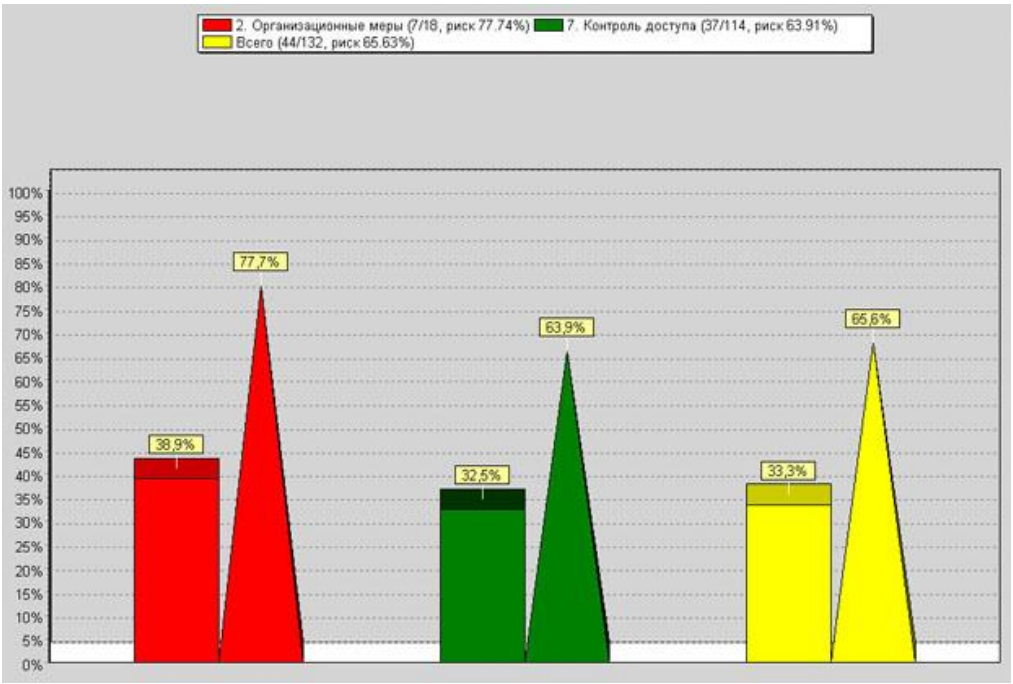
- „რისკების ანალიზი" – განკუთვნილია არსებული რისკების რაოდენობრივად შეფასებისათვის.

მე-4-ე ნახაზზე მოცემულია ამ სისტემის მუშაობის ერთ-ერთი ფრაგმენტი კერძო ფირმის მაგალითზე.



ნახ.4. სიტემა «Гриф»-ის მუშაობის ფრაგმენტი

ასეთი სახით შეტანილი ინფორმაციის საფუძველზე სისტემა ავტომატურად ახდენს შემაჯამებელი სტატისტიკის ფორმირებას, რომელიც წარმოდგენილია დიაგრამის სახით ISO 17799 სტანდარტის თითოეული ნაწილისათვის.



ნახ.5 დარღვევების შესახებ შემაჯამებელი მონაცემების გრაფიკი

3. დასკვნა

ამგვარად, ჩატარებულია ოფისის ინფორმაციული უსაფრთხოების დაცვის ანალიზი პროგრამული საშუალებებით Cobra და "КОНДОР+". შეტანილი ინფორმაციის საფუძველზე მიღებულია ანგარიშგება ინფორმაციული უსაფრთხოების მდგომარეობის შესახებ, რომელიც შეესაბამება ISO17799 სტანდარტის მოთხოვნებს.

ლიტერატურა:

1. ო.შონია, ნ.თოფურია, გ.მაისურაძე „ინფორმაციული უსაფრთხოების სისტემის აგება კორპორაცია Microsoft-ის ტექნოლოგიების გამოყენებით", თბილისი, 2009.

2. С.А. Нестеров, "Анализ и управление рисками в информационных системах на базе операционных систем Microsoft" http://old.intuit.ru/department/itmgt/riskanms/1/

3. С.М. Авдошин, А.А. Савельева, В.А. Сердюк, Технологии и продукты Microsoft в обеспечении информационной безопасности, http://old.intuit.ru/department/security/mssec/

SOFTWARE TOOLS FOR SUPPORTING THE MANAGEMENT OF INFORMATION SECURITY IN THE ENTERPRISE

Nino Topuria, Maka Lomidze
Georgian Technical University

Summary

Article considers the main types software tools used to support the decision of administrative tasks in sphere of information security. Describes the basic functionality of the software systems "COBRA" and "Kondor +". Based on the provided information programs automatically generate reports that meet the international standard ISO 17799.

ПРОГРАММНЫЕ СРЕДСТВА, ПОДДЕРЖИВАЮЩИЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ПРЕДПРИЯТИИ

Топурия Нино, Ломидзе Мака
Грузинский Технический Университет

Резюме

Рассматриваются основные типы программных продуктов, используемых для поддержки решения управленческих задач в сфере информационной безопасности. Описываются основные функциональные возможности программных комплексов "COBRA" и "КОНДОР+". На основе введенной информации программы автоматически формируют как сводную статистику, представляемую в виде диаграмм для каждого раздела стандарта ISO 17799, так и детализированные отчеты об имеющихся несоответствиях.