ინფორმაციული უსაფრთხოების სამსახურის ანალიტიკის სისტემა

გულნარა ჯანელიძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

თანამედროვე პერიოდში კომპიუტერული ქსელი წარმოადგენს პროგრამებისა და მოწყობილობების დიდ განაწილებულ სისტემას, რომლის ძირითადი დანიშნულებაა ინფორმაციის გაცვლა. კომპიტერული ქსელი კომპანიის ბიზნესის განვითარების შესანიშნავი საშუალებაა. დაცულობის სისტემატური ანალიზი კომპიუტერული ქსელების უსაფრთხოების სისტემის აუცილებელი ელემენტია. ამდენად, ინფორმაციულ-ანალიტიკური ქვესისტემა ინფორმაციის დაცვის სისტემის მნიშვნელოვან კომპონენტს წარმოადგენს, ხოლო ანალიტიკური საქმიანობა კონფიდენციალურ ინფორმაციაზე არაუფლებრივი ქმედებების გამოვლენასა და სიტუაციის შეფასებაში მდგომარეობს. სტატიაში წარმოდგენილია ინფორმაციულ-ანალიტიკური სამსახურის ამოცანები და მათ გადასაჭრელად შემოთავაზებულია ანალიზის ჩატარებისა და კვლევის მიმართულებები. ასევე დამუშავებულია თანამედროვე ინფორმაციულ-ანალიტიკური სისტემა და წარმოდგენილია უსაფრთხოების სისტემის საბაზო ფუნქციები, რომელსაც უზრუნველყოფს შემოთავაზებული სისტემა.

საკვანძო სიტყვები: ინფორმაციულ-ანალიტიკური სისტემა, უსაფრთხოების სისტემა.

1. შესავალი

ინფორმაციულ-ანალიტიკურ სფეროს მნიშვნელოვანი ადგილი უჭირავს ადამიანის საქმიანობაში. თანამედროვე პერიოდში მეტად აქტუალურია ანალიტიკური ტექნოლოგიების გამოყენება, რომელიც საწყისი ინფორმაციის გადამუშავების საფუძველზე მაღალი ხარისხის ახალი ცოდნის მიღების საშუალებას იძლევა. ინტერნეტის შექმნა და განვითარება ფასდება როგორც ტრადიციული ტექნოლოგიების ერიდან რეალურ დროში რეალიზებული ტექნოლოგიების ერაში გიგანტური ნახტომი. თანამედროვე ყოფაში ინტერნეტი მთელი ინდუსტრიაა, რომელიც ელვისებურად შეიჭრა ადამიანის საქმიანობის ყველა სფეროში[1].

თანამედროვე ეტაპზე ინტერნეტის ბიზნეს-სექტორი ვითარდება საკმაოდ მაღალი ტემპებით, რაც განპირობებულია, უპირველესად, ინფორმაციული ტექნოლოგიების განვითარების დონით. რაც უფრო სწრაფად ვითარდება ინფორმაციული გეოსტრუქტურა, მით უფრო უჩნდებათ კომპანიებს ახალი ინფორმაციული ტექნოლოგიებით მანიპულირების შესაძლებლობები თავიანთი ბიზნესის სრულყოფის მიზნით. ნებისმიერი სახის კომერციული საქმიანობა მიმდინარეობს რისკებით. ელექტრონულ ბიზნესში რისკების სიტუაციების დონე პროცენტულად გაცილებით აღემატება ტრადიციულ ბიზნესში რისკების დონეს, რაც ძირითადად დაკავშირებულია ინტერნეტ-სივრცის ინტენსივობასთან. ამდენად, ბიზნესის სტრატეგიულ განვითარებაზე პასუხისმგებელმა პირმა სარისკო სიტუაციების შეფასებისა და პროცენტული მაჩვენებლის შემცირებისათვის უნდა გამოიყენოს ანალიტიკური მეთოდები.

2. ძირითადი ნაწილი

ინფორმაციული უსაფრთხოების ანალიტიკის სპეციფიკა შემდგომში მდგომარეობს:

1. ანალიტიკა წარმოებს თანამედროვე, პროგრესული ტექნოლოგიების გამოყენებით;
2. წარმოადგენს ანალიტიკის დარგობრივი ფორმის სიმბიოზს. ფორმირდება შემდეგი ელემენტებისაგან:
   - ინტერნეტ-ტექნოლოგიების ანალიტიკა;
   - მარკეტინგული საქმიანობა, მათ შორის ინტერნეტ-მარკეტინგი;
   - ეკონომიკური საქმიანობის ანალიტიკა;
   - კანონმდებლობის შესწავლაზე ორიენტირებული ანალიტიკური საქმიანობა;
   - ანალიტიკა და მარკეტინგი მართვის სფეროში;
   - სოციალური ანალიტიკის ასპექტები, რომელშიც მოიაზრება საკადრო საკითხებთან დაკავშირებული, საზოგადოებრივი აზრის შესწავლის, ინტერნეტის აუდიტის საკითხები.

უსაფრთხოების სამსახური სავალდებულო სტრუქტურული ქვედანაყოფია განსაკუთრებით მსხვილ კომპანიებში. მათ წინაშე მდგომ მრავალ ამოცანათა შორის შეიძლება გამოვყოთ კომერციული საიდუმლოს შენახვასთან და ასევე, კონკურენტების მხრიდან არასამართლებრივი ქმედებების შეჩერებასთან დაკავშირებული ამოცანები, კერძოდ:

- კომერციული საიდუმლოს შემცველი ინფორმაციის დაცვის უზრუნველყოფა;
- კომერციული საიდუმლოს სამართლებრივი, ორგანიზაციული და ინჟინერ-ტექნიკური დაცვის მიზნით შესასრულებელი სამუშაოების ორგანიზება;
- სპეციალური საქმეთაწარმოების ორგანიზება, რომელიც გამორიცხავს კომერციული საიდუმლოს შემცველი ინფორმაციის არასანქცირებულად მიღებას;
- კომერციული საიდუმლოს შემცველ ინფორმაციაზე უსაფუძვლო დაშვების და წვდომის შეჩერება;

– კონფიდენციალური ინფორმაციის გაჟონვის შესაძლო არხების გამოვლენა და ლოკალიზება როგორც ყოველდღიურ საქმიანობაში, ასევე ექსტრემალურ სიტუაციებში.

– მარკეტინგული სიტუაციების და არასამართლებრივი ქმედებების შეფასება როგორც ბოროტმზრახველების, ასევე კონკურენტების მხრიდან [2].

ზემოაღნიშნული ამოცანების გადასაწყვეტად მნიშვნელოვანია უსაფრთხოების რეჟიმის დარღვევის ანალიზი, ასევე კონკურენტებისა და სხვა ორგანიზაციების, კლიენტების, პარტნიორების შესახებ ინფორმაციის შეგროვება და ანალიზი. ამდენად, ანალიტიკური სამუშაოები უსაფრთხოების სამსახურის ერთ-ერთ ძირითად რგოლს წარმოადგენს. იგი მოიცავს ანალიზის ჩატარებისა და კვლევის მთელ რიგ მიმართულებებს, რომელთაგან მნიშვნელოვანია:

– სხვადასხვა ტიპის ობიექტებთან მუშაობის სპეციფიკის განსაზღვრა;

– ობიექტთა შორის კავშირებისა და დამოკიდებულებების გამოვლენა;

– კომერციული ხასიათის გარე წყაროებთან მუშაობა;

– არასტრუქტურირებელ ინფორმაციასთან მუშაობა;

– კომპანიის კლიენტებთან დაკავშირებული რისკების შეფასება;

– ანალიზის ობიექტებისა და შედეგების დავგუფება;

– მონაცემთა ანალიზისათვის მისაღები ფორმით, ასევე შედეგების სქემებისა და დიაგრამების სახით წარმოდგენა;

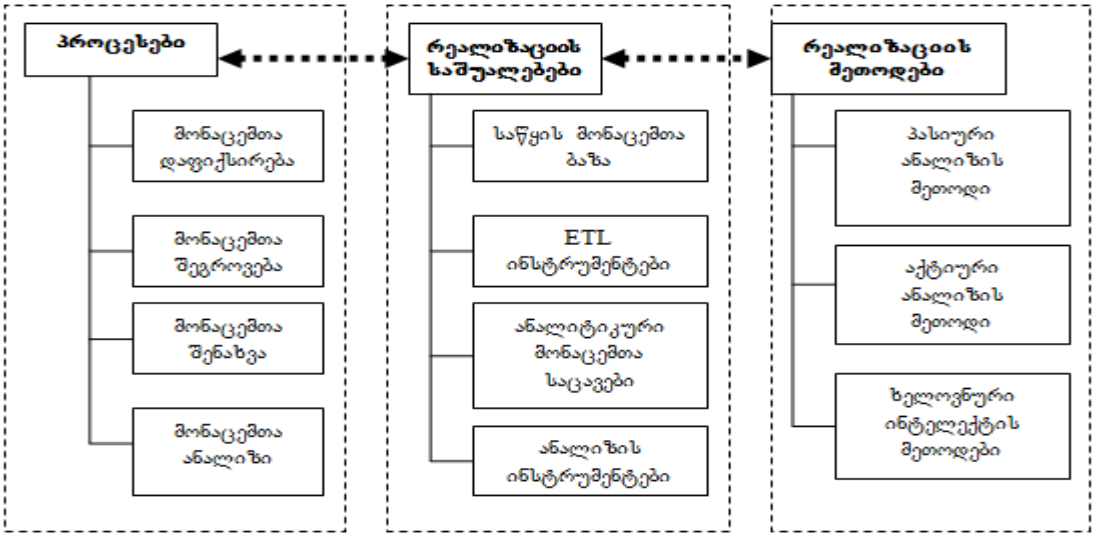
– მონაცემთა უტყუარობისა და ხარისხის შეფასება;

– საკუთარი მოსაზრებების გამოხატვა და ობიექტების ანალიზის შესახებ დასკვნების გამოტანა;

– ანალიზის შედეგების გაფორმება ანგარიშის სახით;

– სპეციალიზებული ანალიტიკური ფუნქციების და სტატისტიკური მეთოდების გამოყენება[3,4].

ინფორმაციული უსაფრთხოების სამსახურის ანალიტიკის სისტემა წარმოდგენილია 1-ელ ნახაზზე.



ნახ.1. ინფორმაციული უსაფრთხოების ანალიტიკის სისტემა

წარმოდგენილი სისტემა უზრუნველყოფს უსაფრთხოების სისტემის საბაზო ფუნქციების რეალიზებას, როგორიცაა: საპრობლემო სივრცის ანალიზი; საკუთარი მონაცემთა ბაზების წარმოება; მონაცემთა გარე წყაროებთან ერთიან სივრცეში მუშაობა; ელექტრონული დოსიეების წარმოება; მონაცემთა ანალიზი როგორც ტრადიციული ცხრილური ანალიზის საშუალებებით, ასევე ვიზუალური ანალიზის მეშვეობით; ინფორმაციის გამოთვლა; არასტრუქტურირებული დოკუმენტების გადარჩევა, დოკუმენტის სქემის აგება და განთავსება მონაცემთა ბაზაში; მოთხოვნათა ფორმირება გრაფიკული საშუალებებით; კლასტერული ანალიზი; სოციალური ქსელების ანალიზი; ანალიზი კარტოგრაფიული ინფორმაციის გამოყენებით; ობიექტთა დუბლიკატების ძიება.

3. დასკვნა

უსაფრთხოების სამსახურის ანალიტიკური სისტემის მეშვეობით დამკვეთი იღებს ინსტრუმენტს, რომელიც სხვადასხვა წყაროდან წარმოდგენილი მრავალფეროვანი ინფორმაციის ანალიზის საშუალებას იძლევა. ამდენად, აღნიშნული სისტემა საშუალებას იძლევა უფრო ეფექტურად იქნას გადაწყვეტილ უსაფრთხოებასთან დაკავშირებული ამოცანები, რომელთაგან მნიშვნელოვანია:

– შიდა ინფორმაციული კვლევების ორგანიზება;

– თანამშრომელთა მონაცემებზე კონტროლის ორგანიზება მათი სამუშაოზე მიღებისას;

– კომერციული საიდუმლოს შემცველ ინფორმაციაზე არასამართლებრივი დაშვების და წვდომის აღმოფხვრა;

– კონფიდენციალური ინფორმაციის გაჟონვის დასაშვები არხების გამოვლენა და ლოკალიზება;

– იურიდიული და ფიზიკური პირების გადახდისუნარიანობის და მათი საგადასახადო ვალდებულებათა დროული შესრულების შესაძლებლობების გამოვლენა.

– კონკურენტებისა და ბოროტმზრახველების კომპანიასთან მიმართებით არაუფლებრივი ქმედებების აღმოფხვრა;

– იმ პირთა ჯგუფის გამოვლენა, რომელთათვისაც უნდა შეიზღუდოს კომერციული საიდუმლოს ხელმისაწვდომობა, ასევე აღიწეროს აღნიშნული სახის ინფორმაციის ხელმისაწვდომობის უფლებები სხვადასხვა ჯგუფებისთვის;

– ფიზიკურ და იურიდიულ პირთა შორის სამართლებრივი ურთიერთდამოკიდებულების გამოვლენა;

– ფიზიკურ და იურიდიულ პირთა შორის ქონებრივი ურთიერთდამოკიდებულებების გამოვლენა.

ზემოთქმულიდან გამომდინარე წარმოდგენილი სისტემა ახორციელებს მონაცემებსა და ობიექტებზე სრულ კონტროლს. ამავდროულად იგი საკმაოდ მოქნილია. ანალიზის აქტიური და პასიური მეთოდების გამოყენებით სისტემა აგებს ქსელის თავდასხმების გრაფს. მიღებული გრაფის ანალიზისათვის გამოიყენება ხელოვნური ინტელექტის მეთოდები, რაც მრავალსაფეხურიანი რთული თავდასხმების წინასწარ გათვლის საშუალებას იძლევა.

ლიტერატურა:

1. შონია ო., ჯანელიძე გ., მეფარიშვილი ბ. ინფორმაციული და ქსელური რესურსების უსაფრთხოების ურუნველყოფა, თბ., სტუ, 2009

2. ჯანელიძე გ., მეფარიშვილი ნ. საწარმოს ინფორმაციული რისკების ანალიზი, სტუ შრომები, მართვის ავტომატიზებული სისტემები №2(9), ISSN 1512-3979, თბ., 2010. გვ. 62-66

3. Lam J. Enterprise Risk Management: From Incentives to Controls. John Wiley. ISBN 978-0-471-43000-1. 2003

4. Ежемесячный научно-информационный журнал. В мире науки. ООО ИД «Медиа-Пресса». Ст. 52, Москва, 12-2008.

INFORMATION SECURITY ANALYTICS SYSTEM

Janelidze Gulnara
Georgian Technical University

Summary

The computer network is a great software and hardware distributed system in modern period, main purpose of which is to exchange information. Computer network is a perfect tool for the business development. Regular safety analysis is one of the necessary elements of the computer network security system. Thus, informational-analytical subsystem is the most important link of information security system, and analytical activity consists in revealing of illegal access to the confidential information and the evaluation of situation. In the article there are presented problems of informational-analytical service and there are proposed directions of analysis and research. Also here is processed a modern informational-analytical system and represented basic functions of the proposed security system.

СИСТЕМА АНАЛИТИКИ СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Джанелидзе Гульнара
Грузинский Технический Университет

Резюме

В современном обществе компьютерные сети преставляют собой большую систему программных средств и устройств, назначением которой является обмен информацией. Компьютерные сети - это отличное средство для развития бизнеса компании. Систематический анализ защитности является необходимым элементом системы безопасности компьютерных сетей. Поэтому информационно-аналитическая подсистема является значительным компонентом системы защиты информации, а суть аналитической деятельности заключается в выявлении неправового действия над конфиденциальной информацией и в оценке ситуации. В статье преставлены задачи информационно-аналитической службы, для их решения предложены направления проведения анализа и исследований. Также разработана современная информационно-аналитическая система и представлены базовые функции, обеспечиваемые предложенной системой.