სამართლებრივ-საძიებო ავტომატიზებული სისტემის უსაფრთხოების უზრუნველყოფა

ოთარ შონია, იოსებ ქართველიშვილი, ლევან ყოლბაია

საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

ნაშრომში წარმოდგენილია სახელმწიფო დაწესებულებებში და კერძო სტრუქტურებში ნორმატიულ-სამართლებრივი დოკუმენტების მართვისა და საქმიანი პროცესების ინტეგრირებული ავტომატიზებული სისტემის დაცვა, მისი ნორმალური პროცესის ფუნქციონირებაში შემთხვევითი და მიზანმიმართული ჩარევისაგან, ინფორმაციის მოპარვის მცდელობისაგან, მისი კომპონენტების მოდიფიცირებისა ან ფიზიკური განადგურებისაგან, სხვადასხვა საგანგაშო ზემოქმედების განეიტრალების შესაძლებლობა, უსაფრთხოების უზრუნველყოფის აუცილებლობა.

საკვანძო სიტყვები: ნორმატიულ-სამართლებრივი დოკუმენტები. სამართლებრივ-საძიებო ავტომატიზებული სისტემები. უსაფრთხოების უზრუნველყოფა.

1. შესავალი

უკანასკნელ ხანებში კომპიუტერულ ქსელებში (სადენიანი და უსადენო) უსაფრთხოება და მომსახურების ხარისხი უაღრესად მნიშვნელოვანი და აქტიური კვლევის საგანი გახდა, რისი მიზეზიც მონაცემთა პაკეტების გადაცემის მზარდაჭერის მზარდი მოთხოვნაა [1,2]. ადეკვატური უსაფრთხოების გარეშე ორგანიზაციები თავს აარიდებენ კომპიუტერულ ქსელების გამოყენებას.

უსაფრთხოების საკითხები კომპიუტერულ ქსელებში მნიშვნელოვანი დაბრკოლებაა ასეთი ქსელების ფართოდ ადაპტირების მიზნით. შესაბამისად, მსგავსი კომპიუტერული ქსელების უსაფრთხოება მნიშვნელოვანი სფეროა, რაც რეაგირებას მოითხოვს, თუკი ასეთი ქსელები ფართოდ იქნება გამოყენებული. აუცილებელია, რომ აღნიშნული სფეროს მკვლევარებმა მოახდინონ ღია პრობლემების იდენტიფიცირება და უზრუნველყონ შესაბამისი გადაწყვეტილებები ამ პრობლემებისთვის.

უსაფრთხოება უაღრესად მნიშვნელოვანი საკითხია კომპიუტერულ ქსელებისათვის, ვინაიდან გარემოში გავრცელებული საკომუნიკაციო სიგნალები ხელმისაწვდომია დასაჭერად. აქედან გამომდინარე, კომპანიებმა და ინდივიდუალურმა მომხმარებლებმა უნდა შეიცნონ პოტენციურად არსებული პრობლემები და მიიღონ შესაბამისი ზომები.

ნებისმიერ სისტემას, რომელსაც დაცვა სჭირდება, გააჩნია სისუსტეები ან ხარვეზები, რომელთა ნაწილს ან ყველას ერთად ამოირჩევს თავდამსმხმელი ობიექტად. შესაბამისად, სისტემის უსაფრთხოების მექანიზმების შექმნის ერთ-ერთი მიდგომაა იმ საფრთხეებისა და სავარაუდო თავდასხმების განხილვა, რომელთა წინაშე დგას სისტემა, იმის გათვალისწინებით, რომ სისტემას ხარვეზები გააჩნია. უსაფრთხოების მექანიზმებმა უნდა უზრუნველყოს სისტემის უსაფრთხოება მოცემული საფრთხეების, თავდასხმებისა და ხარვეზების გათვალისწინებით.

უნდა აღინიშნოს, რომ კომპიუტერული ქსელების მარშრუტიზაციის ოქმები სპეციფიკაციებში არ განსაზღვრავს რაიმე სახის პრევენციულ ღონისძიებებს ან უსაფრთხოების მექანიზმებს. ამდენად, კომპიუტერული ქსელების მარშრუტიზაციის ოქმების უსაფრთხოება გადაუდებელ აუცილებლობად იქცა ქსელის გაშვების სტიმულირებისა და გამოყენების სფეროს გაფართოებისთვის.

2. ძირითადი ნაწილი

თანამედროვე პირობებში სახელმწიფო დაწესებულებებში და კერძო სტრუქტურებში სამართლებრივ-საძიებო ავტომატიზებული სისტემების ინფორმაციული რესურსების მართვის ეფექტური მექანიზმების შექმნა, შეუძლებელია ინფორმაციული უსაფრთხოების სამეცნიერო დასაბუთების და დაბალანსებული პოლიტიკის პრაქტიკულად განხორციელების გარეშე.

ამ დაწესებულებებში ინახება და მუშავდება დიდი რაოდენობის სხვადასხვა მონაცემები, რომლებიც დაკავშირებულია არა მარტო მათი საქმიანობის წარმართვასთან, არამედ სხვადასხვა კვლევითი და კონსტრუქციული პროექტების განხორციელებასთან, პერსონალის პირადი მონაცემების დამუშავებასთან, სახელმწიფო, კომერციული, პირადი და სხვა სახის კონფედენციალური ინფორმაციის შენახვასთან.

მაღალი ტექნოლოგიების სფეროში დანაშაულების ზრდამ განაპირობა მოთხოვნები სახელმწიფო და კერძო დაწესებულებების სამართლებრივ-საძიებო სისტემების მიმართ გამოთვლითი ქსელების რესურსების დაცვის კუთხით. აქტუალური გახდა საკუთარი უსაფრთხოების სისტემის შექმნის აუცილებლობა, რაც გულისხმობს სამართლებრივ-ნორმატიული ბაზის არსებობას, უსაფრთხოების კონცეფციის ფორმირებას, სპეციალური ღონისძიებების შემუშავებას, უსაფრთხოების მიზნით პროცედურების დაგეგმვას, პროექტირებას, ინფორმაციის დასაცავი ტექნიკური საშუალებების რეალიზებას [3]. ყველა ზემოთ ჩამოთვლილი სისტემური კომპონტები განსაზღვრავს ინფორმაციული უსაფრთხოების დაცვის ერთიან პოლიტიკას.

სახელმწიფო თუ კერძო დაწესებულებების სამართლებრივ-საძიებო სისტემაში ინფორმაციის დაცვის სპეციფიკა მდგომარეობს იმაში, რომ ეს დაწესებულებები ხასიათდებიან მუდმივად ცვალებადი პერსონალით, მომხმარებელთა ფართო წრით, საჭირო ინფორმაციის მიღების მსურველთა უზარმაზარი რაოდენობით და მათ შორის „დამწყები კიბერ კრიმინალების“ აქტიური ზრდით.

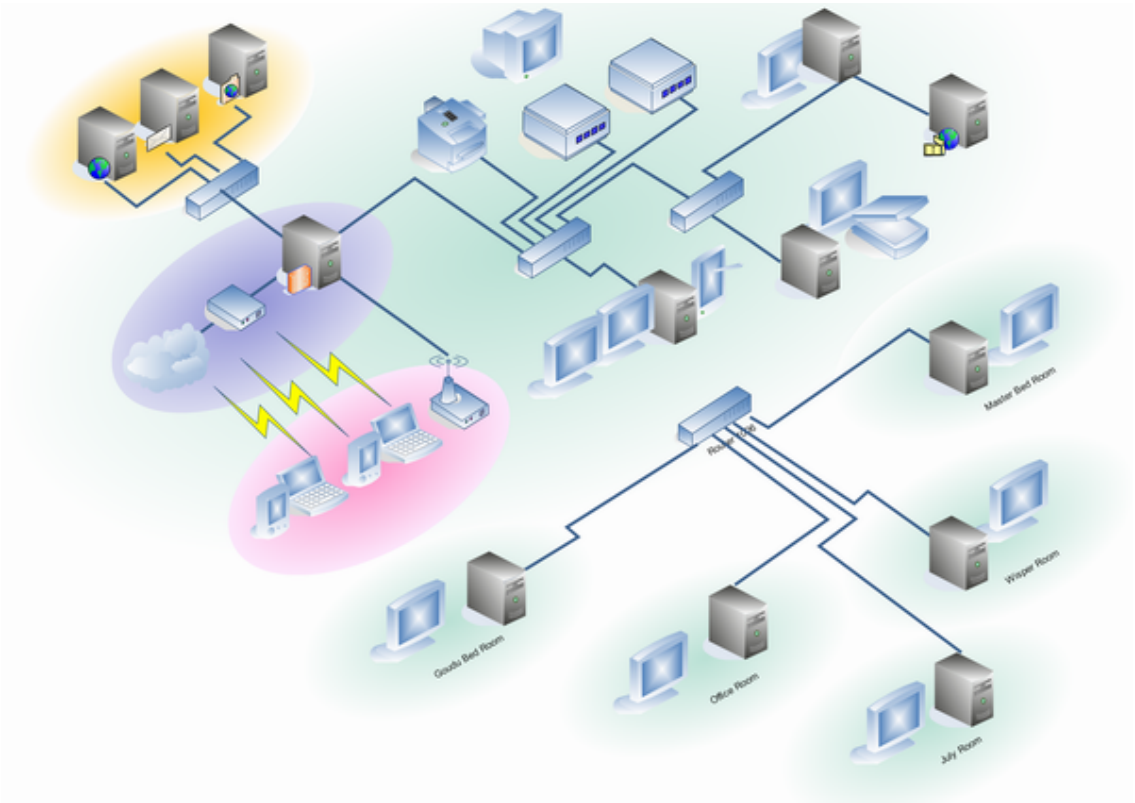
სახელმწიფო თუ კერძო დაწესებულებები, როგორც ინფორმატიზაციის ობიექტი, გამოირჩევა მრავალპროფილური საქმიანობით, დაფინანსების წყაროს მრავალფეროვნებით, დამხმარე ქვედანაყოფებისა და სერვისების არსებობით (მშენებლობა, წარმოება, სამეურნეო საქმიანობა), საგანმანათლებლო მომსახურების ბაზარზე მუდმივი ადაპტაციით, შრომის ბაზრის მოთხოვნების ანალიზით, ზემდგომ ორგანიზაციებთან ელექტრონული ურთიერთქმედების აუცილებლობით, თანამშრომლებისა და მომხმარებელთა სტატუსების ხშირი ცვალებადობით.

სამართლებრივ-საძიებო სისტემის უსაფრთხოების დაცვაზე მნიშვნელოვან გავლენას ახდენს – ინფორმაციული გარემოს არქიტექტურა და ინფორმაციულ რესურსებზე ხელმისაწვდომობის უფლებების მართვა. განვიხილოთ თითოეული დონის სტრუქტურა:

ინფორამციული გარემოს აქრიტექტურაში შედის - ინფრასტრუქტურა, რომელიც უზრუნველყოფს სამართლებრივ-საძიებო სისტემის სერვისების საიმედო, უსაფრთხო და 24 საათიან რეჟიმში ფუნქციონირებას და საინფორმაციო რესურსები, რომლებიც უზრუნველყოფს ნებისმიერ ადგილიდან და ნებისმიერ დროს სამართლებრივ-საძიებო სისტემის საინფორმაციო რესურსებთან მარტივ და საიმედო წვდომას. სადენიანი ქსელური (კომუტატორები, მარშრუტიზატორები და ა.შ.) როუტერისა და კომუტატორების ადმინისტრირება, რომლებიც უზრუნველყოფს როგორც გარე ინტერნეტთან წვდომას, ასევე შიგა რესურსებთან კავშირს. შიგა კომპიუტერული ქსელის სამისამართო სისტემის მენეჯმენტი, შიგა ქსელის თვითოეული სეგმენტის უსაფრთხოების უზრუნველყოფა და დაცვა როგორც გარე ასევე შიდა არასანქცირებული შეღწევისაგან. ასევე უსადენო ქსელური (უსადენო კომუტატორები და მარშრუტიზატორები) - უსადენო როუტერებისა და კომუტატორების ადმინისტრირება, რომლებიც უზრუნველყოფს ინტერნეტით კავშირს მოცილებული მომხმარებლებისათვის. უსადენო ქსელის სამისამართო

სისტემის მენეჯმენტი, მათი უსაფრთხოების უზრუნველყოფა და დაცვა. ასევე მნიშვნელოვანია სერვერების ადმინისტრირება, რომელზეც გაშვებულია ყველა საჭირო საინფორმაციო რესურსის გამართულად და შეუფერხებლად მუშაობისთვის შესაბამისი პროგრამული უზრუნველყოფა. ხდება სერვერების 24 საათიანი მონიტორინგი და ყველა შესაძლო ხარვეზის უმოკლეს დროში აღმოფხვრა და გასწორება. სერვერებზე დაყენებული პროგრამული უზრუნველყოფის პერიოდული განახლება, სარეზერვო კოპირება და დაცვა როგორც გარე, ასევე შიგა არასანქცირებული შეღწევისაგან.

შესაძლებელი რომ იყოს ინფორმაციაზე წვდომის კონტროლი, აუცილებელია როგორც აპარატურული, ისე პროგრამული საშუალებების ეფექტურად ფუნქციონირება. 1-ელ ნახაზზე ნაჩვენებია, თუ როგორ უნდა იყოს გამართული ინფორმაციული ინფრასტრუქტურა სხვადასხვა ორგანიზაციებში, აპარატურული და პროგრამული საშუალებების ნაკრების გამოყენებით.



ნახ.1. საინფორმაციო რესურსებისა და სხვადასხვა სერვისების მხარდაჭერის სტრუქტურა

მოკლედ დავახასიათოთ საინფორმაციო რესურსების სტრუქტურაში გამოყენებული თითოეული კომპონენტი:

- Proxy სერვისი – სახელმწიფო და კერძო დაწესებულებების ლოკალურ ქსელში არასანქცირებული ვებგვერდების ფილტრაცია „transparent proxy" ტექნოლოგიით, მისი ადმინისტრირება და გამართული მუშაობა;
- E-mail სერვისი - თანამშრომლებისა და მომხმარებლების ელ-საფოსტო სერვისის ადმინისტრირება და გამართულად მუშაობის უზრუნველყოფა. ელ-საფოსტო დაგზავნის სიების შექმნა, მათი განახლება და მხარდაჭერა.

- DNS სერვისი - დომენური სახელების (პირველადი და მეორადი) ადმინისტრირება და გამართული მუშაობა:
- Web სერვისი - კუთვნილ დომენურ სახელებზე დაფუძნებული ვებგვერდების უსაფრთხოება, ადმინისტრირება და გამართული ფუნქციონირება;
- მონაცემთა ბაზები - ვებგვერდებისათვის საჭირო SQL მონაცემთა ბაზების უსაფრთხოება, ადმინისტრირება და გამართული ფუნქციონირება;
- File სერვისი - SFTP და ფაილური სერვერის ადმინისტრირება და მისი გამართული ფუნქციონირების უზრუნველყოფა;
- სარეზერვო კოპირება - სერვერებზე არსებული ვებგვერდების, ფაილების, მონაცემთა ბაზების პერიოდული სარეზერვო კოპირების უზრუნველყოფა;

სამართლებრივ-საძიებო სისტემის უსაფრთხოების დაცვის ერთ-ერთ მნიშვნელოვან მეთოდია ინფორმაციულ რესურსებზე ხელმისაწვდომობის უფლებების მართვა. როგორც წესი, გამოიყენება რამდენიმე პროგრამული პროდუქტი და ინფორმაციული სისტემა. თითოეულს გააჩნია რეგისტრაციის და უფლებების ადმინისტრიების საკუთარი სისტემა. ასეთი სისტემების მართვისთვის აუცილებელია ე.წ. ადმინისტრატორები, რომელთა ფუქნციაა მომხმარებლის კატეგორიისა და მათი უფლებების განსაზღვრა.

სახელმწიფო და კერძო დაწესებულებების სამართლებრივ-საძიებო ინფორმაციულ სისტემაზე წვდომის უფლება ეძლევათ, როგორც თანამშრომლებს ასევე სპეციალური უფლებამოსილების მქონე პირებს. მათი რაოდენობა მუდმივად ცვალებადია, შესაბამისად, იქმნება ინფორმაციულ რესურსებზე ხელმისაწვდომობის უფლებების მართვის ავტომატიზაციის აუცილებლობა.

ქსელის დაუცველობა „ხაკერს“ აძლევს პოტენციურ საშუალებას არასანქცირებული წვდომისა და ფალსიფიკაციის. საკვლევ სისტემაში უსაფრთხოების დასაცავად გამოყენებულია AAA (Authentication, Authorization, and Accounting) პროტოკოლი, რომელიც ახორციელებს ქსელის მომხმარებლის აუტენტიფიკაციის, ავტორიზაციისა და აღრიცხვის შესაძლებლობას.

1. აუტენტიფიკაცია - ითხოვს პიროვნებისგან დამტკიცებას, რომ ის ნამდვილად წარმოადგენს ქსელის მომხმარებელს (მაგალითად: მომხმარებლის სახელის და პაროლის შეყვანა);

2. ავტორიზაცია - აუტენტიფიკაციის შემდეგ, ავტორიზაცია იღებს გადაწყვეტილებას თუ რომელ რესურსზე აქვს წვდომის უფლება მომხმარებელს და რომელი მოქმედებების შესრულებაა ნებადართული;

3. აღრიცხვა - აფიქსირებს ჩანაწერების სახით მომხმარებლის მონაცემზე წვდომის დროსა და ინფორმაციას მისი ქმედებების შესახებ.

მოკლედ მიმოვიხილოთ თითოეული მათგანი:

აუტენტიფიკაცია – კვლევის ობიექტის შემთხვევაში, სისტემის მომხმარებლის ტიპის განსაზღვრის შემდეგ, ხდება მომხმარებლისთვის სახელისა და პაროლის მინიჭება, რომელსაც ახორციელებენ შესაბამისი სტრუქტურის წარმომადგენლები (მაგალითად, კერძო დაწესებულებებში ხელმძღვანელის დავალებით შესაბამისი თანამშრომელი ქმნის მომხმარებლის სახელსა და პაროლს, სახელმწიფო დაწესებულების შემთხვევაში კი - რეგისტრაციის სამსახური, პერსონალის მართვის დეპარტამენტი). თითოეული ტიპის გათვალისწინებით, მომხმარებლის სახელი იქმნება სპეციალური ალგორითმის მიხედვით, რომელიც განთავსდება ბაზაში ცხრილის სახით. ინფორმაცია ეგზავნება სისტემის ადმინისტრატორს. მრავალწლიანმა გამოცდილებამ მკაფიოდ დაგვანახა აუცილებლობა გაძლიერდეს სამართლებრივ-საძიებო სისტემის უსაფრთხოება. მომხმარებელთა ტიპს (თანამშრომელი) განესაზღვრა მართვის ავტომატიზიბულ სისტემაზე მუშაობის უფრო ფართო უფლებები. სწორედ, ამან განაპირობა სხვადასხვა პაროლის შემოღების აუცილებლობა. თანამშრომლების ინფორმაციის დაცულობის ხარისხის გაზრდისთვის განცალკევდა მეილ-

სერვერისა და ავტომატიზებული სისტემის პაროლები, რომლებიც კონტროლირდება შეყვანისას, პროგრამის მიერ. გარდა ამისა, ავტომატურ რეჟიმში, ყოველ სამ თვეში, სისტემა ითხოვს მომხმარებლის პაროლის შეცვლას.

ავტორიზაცია - მომხმარებლის სისტემაში რეგისტრაციის შემდეგ ისაზღვრება თითოეული მომხმარებლის უფლებები სამუშაო ადგილისა და თანამდებობის მიხედვით. უფლებები ჩაწერილია სპეციალურ ცხრილებში, რომელიც ისაზღვრება ადმინისტრატორისა და მომხმარებლის დონეზე.

არსებობს სამი ტიპის მომხმარებელი: თანამშრომელი, სტუმარი, რეგისტრირებული მომხმარებელი. აუტეტიფიკაციის შემდეგ თითოეული მომხმარებლის ტიპის შესაბამისად, შედის მისთვის განკუთვნილ მოდულში. ტიპის განსაზღვრის შემდეგ, მომხმარებებლს უფლება ეძლევა იმუშაოს მისთვის განსაზღვრულ პროგრამული ჯგუფებზე. თანამშრომელი ან რეგისტრირებული მომხმარებელი შედის მხოლოდ მათთვის განკუთვნილ გვერდზე, რომელთაც, თავიანთი მომხმარებლის ტიპის ფარგლებში აქვთ ერთნაირი უფლებები. შესაბამისი დაწესებულების შესაბამის თანამშრომელს, სამუშაო პოზიციის გათვალისწინებით, განესაზღვრება პროგრამულ ჯგუფში და პროგრამულ ბმულზე მუშაობის უფლებები.

უსაფრთხოების დაცვის მიზნით, თითოეული თანამშრომლისთვის, გაწერილია შიდა ქსელის IP მისამართები. თანამშრომელს უფლება ეძლევა სისტემაზე იმუშაოს მხოლოდ შიდა ქსელიდან. მაგალითად, ერთ-ერთი ორგანიზაციის თანამშრომელს უფლება აქვს იმუშაოს დასაშვებ მონაცემების ბმულზე შეცვალოს ინფორმაცია, მაგრამ მას არ აქვს უფლება დაამატოს ან წაშალოს რაიმე სახის ინფორმაცია ბაზიდან. ეს უფლება მინიჭებული აქვს შესაბამისი სამსახურის თანამშრომელს. როგორც ზემოთ აღინიშნა, სამივე მომხმარებლის ტიპის უფლებები გაწერილია სპეციალურ ცხრილებში.

აღრიცხვა - სისტემის მომხმარებლის მიერ შესრულებული ქმედებები და შესრულების დრო აღირიცხება სპეციალურ ცხრილში, რომლის ყოველდღიურ ანალიზს აკეთებს სისტემის ადმინისტრატორი. აღრიცხვადი ქმედებებია: მომხმარებლის პირადი მონაცემების ცხრილში ინფორმაციის დამატება, წაშლა, რედაქტირება; რეგისტრაციების ცხრილში ინფორმაციის დამატება, წაშლა, რედაქტირება; შესაბამისი უფლებამოსილების მქონე პირის მიერ ფაილების ატვირთვა, ატვირთვის დრო, ფაილის სახელი, IP მისამართი და მომხმარბელის მიერ ფაილების ჩამოტვირთვის დრო, ფაილის სახელი, IP მისამართი.

3. დასკვნა

ტექნოლოგიური სიახლეების პერიოდში, როდესაც მიმართულება განიცდის სწრაფ განვითარებას, აუცილებელია სამართლებრივ-საძიებო სისტემის უსაფრთხოების უწყვეტი განახლების პროცესის უზრუნველყოფის ხელშეწყობა. სწორედ ამ ამოცანის წინაშე დგანან სახელმწფიო და კერძო დაწესებულებების სამართლებრივ-საძიებო მართვის ავტომატიზებული სისტემები მუდმივად.

პრაქტიკაში უწყვეტ სამუშო ციკლს ექვემდებარება დაცვის მექანიზმების გაძლიერება და კიდევ უფრო ინოვაციური მეთოდების დანერგვა. თავის მხრივ, უახლესი მეთოდებისა და იდეების შემუშავება და მათი პრაქტიკული გამოყენება, ნათლად დაგვანახვებს მეთოდების დადებით მხარეებსა და მის ნაკლოვანებებს. სიტუაციური ანალიზის საფუძველზე ხდება მეთოდების გაძლიერება სხვადასხვა მიმართულებით და უფრო მეტად სრულყოფა დაცვის მეთოდებისა არსებული მომენტისთვის.

ლიტერატურა:

1. გოგიჩაიშვილი გ., ოდიშარია კ., შონია ო. (2008). ინფორმაციის დაცვა ავტომატიზებულ სისტემებში. სტუ, თბილისი, „ტექნიკური უნივერსიტეტი"

2. შონია ო., შეროზია თ. (2008). ინფორმაციული ტექნოლოგიები და უსაფრთხოება. სტუ, თბილისი, „ტექნიკური უნივერსიტეტი"

3. შონია ო., ქართველიშვილი ი., ყოლბაია ლ. (2014). ნორმატიულ-სამართლებრივი დოკუმენტების მართვისა და საქმიანი პროცესების ავტომატიზებული სისტემის დამუშავება და უსაფრთხოების უზრუნველყოფა. სტუ-ს შრ.კრ. „მართვის ავტომატიზებული სისტემები", № 1(17), თბილისი, გვ.59-63.

LEGAL-SEARCH AUTOMATED SYSTEM SECURITY GUARANTEES

Shonia Otar, Kartvelishvili Ioseb, Kolbaia Levan

Georgian Technical University

Summary

During the technical innovation period, when the direction, experiencing rapid development, it's necessary to provide legal-search system security continuous renewal process promotion. This is the task that the public and private institutions legal-search automated management system facing constantly. In practice continuous employment cycle is subject strengthening security mechanism and introduction more innovative methods. In turn, the latest methods and ideas development and their practical application clearly demonstrate the positive and negative sides of the method. On the basis of situational analysis happens strengthen of method in different direction and improve further the protection of the existing methods.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРАВОВО-ПОИСКОВОГО АВТОМАТИЗИРОВАННОГО СИСТЕМЫ

Шония О., Картвелишвили И., Колбая Л.

Грузинский Технический Университет

Резюме

В период технологических новшеств, когда направление подвергается быстрому развитию, обязательно обеспечение беспрерывного содействия обновлению процесса безопасности правово-поисковой системы. Именно перед этой задачей стоят постоянно правово-поисковые автоматизированные системы. На практике беспрерывному трудовому циклу подчинены усиления защитных механизмов и еще более-ускорения иновационных методов. В свою очередь, выработка новейших методов и идей и их практическое использование явно покажут положительные стороны и недостатки. На основании ситуационного анализа происходит усиление методов в разном направлении и еще более-усовершенствование методов защиты в данном моменте.