SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL2 No4
DECEMBER 2018

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 01-04 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

INFORMATION WARFARE-ABKHAZIA AND GEORGIA

Natalia Patarkatsasvhili, Elene Zakashvili, Ani Dekanosidze
Ivane Javakhishvili Tbilisi State University

ანოტაცია-ოცდამეერთე საუკუნეში საინფორმაციო ომი მნიშნელოვანი და აქტუალური საკითხია, ამიტომ ვთვლით , რომ ჩვენი თემა ,,ინფორმაციული ომი-აფხაზეთი და საქართველო'' აღწერს რეალობას ისტორიული ფაქტების საფუძელზე და საკმაოდ მწვავე პრობელამასაც სვამს- ურთიერთობას ქართველებსა და აფხაზებს შორის.

Annotation-Information warfare in the 21st century is very important and actual subject, so we think our theme ,, Information Warfare-Abkhazia and Georgia'' describes reality based on historical facts and also points out a big problem- relationship between Abkhazians and Georgians.

საკვანძო სიტყვები- ინფორმაციული ომი, საბჭოთა კავშირი, საქართველო, აფხაზეთი, კირილიცა, ქართული გრაფიკა, ჩატეხილი ხიდი

თანამედროვე მსოფლიოში ყველაზე დიდი სიმდიდრე, სტრატეგიული მნიშვნელობის რესურსი, გავრცელებული "იარაღი" და გააზრებული პიარსვლა ინფორმაციაა - ძალა, რომელიც მოსახლეობის რწმენაზე, ღირებულებებსა და შეხედულებებზე ახდენს ზემოქმედებას, ცვლის და აფორმირებს მას ისე, როგორც ეს საინფორმაციო ომში ჩართულ სახელმწიფოებს აწყობთ. საინფორმაციო ომის მასშტაბები ინდივიდებს შორის დაწყებული კონფლიქტიდან გიგანტ სახელმწიფოებს შორის გამწვავებულ დაპირისპირებამდე იცვლება, შედეგი კი ყოველთვის ძლიერის, ანუ იმის მხარესაა, ვინც საინფირმაციო სტრატეგია მოქნილად აწარმოა. ტერმინი ,,ინფორმაციული ომი'' დღეს ძალზედ აქტუალურია, ამას არაერთი სტატია, ნაშრომი თუ მოხსენება მოწმობს რომელიც ბოლო ოცი წლის განმავლობაშია შექმნილი. გლობალიზაციის ეპოქაში ძნელია აკონტროლო ინფორმაციის მიღებისა და გავრცელების საშუალებები, ამიტომ ნებისმიერ ომს, წარმოებულს იარაღითა და სამხედრო ტექნოლოგიებით, წლების განმავლობაში სასურველი და მიზანმიმართული ინფორმაციით მომზადებული ნიადაგი უდევს საფუძვლად.

,, დღეს ინფორმაციული ომის ჟამი დგას, კალმით ანუ სიტყვით ბრძოლის დრო.'' [1]

პოსტმოდერნულ მსოფლიოში საინფორმაციო ომის მსვლეობა იმდენად ხილულია, რამდენადაც კალაპოტში მდინარის დინება, თუმცა წარსულიდან შემორჩენილი,

[1] ილია II - სრულიად საქართველოს კათოლიკოს-პატრიარქი_ საშობაო ეპისტოლე 2013 http://sibrdzne.ge/index.php?swavleba_id=23431&amonaridi=23441

გაცვეთილი და გაყვითლებული ფურცლები კარგად შეფუთულ, უხილავ და დამღუპველ საინფორმაციო ომზე მოგვითხრობს, ეპოქაზე რომელსაც სათავეში ,,დიდი ბელადი'', სტალინი ედგა- კაცი, რომელმაც კარგად იცოდა ინფორმაციის ძალისა და მნიშნელობის ფასი. ამის ნათელი დასტურია აფხაზური ენის ქართულ შრიფტზე გადაყვანის რეალური ისტორია, რეალური რადგან მის შესახებ მხოლოდ ფაქტია ცნობილი, ხოლო რა ედო საფუძლად მხოლოდ მაშინაა გასაგები როდესაც საქართველოს შსს არქივში დაცულ სრულიად საიდუმლო მასალებს ვეცნობით, რომლის მიხედვითაც ირკვევა უდამწერლობო ერს რა მიზნით და რა ინსტრუმენტებით შეუქმნეს დამწერლობა. დამწერლობა რომელიც ერის იდენტობის მაგისტრალური ხაზია.

,, 1937 წლის 4-5 დეკემბერი, ქ. სოხუმი, ნ. მარის სახელობის აფხაზური კულტურის ინსტიტუტი.

თათბირს ესწრება 4 რუსი, 23 აფხაზი და 6 ქართველი.

განხივლის თემა-აფხაზური დამწერლობის ქართულ გრაფიკაზე გადაყვანა.

გადაწყვეტილება-დამწერლობის სამი ვარიანტის შეჯერებით, ქართველებს დაევალათ შეექმნათ გრაფიკა აფხაზი მოსახლეობისათვის.''

ეს იმ ფაქტის მოკლე აღწერაა, რომელიც კარგად დაგეგმილი პროპაგანდის ნაწილი იყო, კერძოდ 1936-41 წლებში საბჭოთა კავშირი შეუდგა ტრიადიდან (მამული, ენა სარწმუნოება) ერთ-ერთი უმნიშვნელოვანესი ნაწილის- ენის სათავისოდ გამოყენებას, ერების საბოლოოდ რუსიფიკაციისათვის მათი ენების რუსულ, ე.წ კირილიცაზე გადაყვანას. ამ დროს აზერბაიჯანელების, ყაზახების, ტაჯიკებისა და სხვა მრავალის ენათა გრაფიკასთან ერთად, აფხაზური დამწერლობის გრაფიკის ცვლილებაც მოხდა, მაგრამ არა კირილიცაზე, არამედ ქართულზე. საბჭოთა კავშირის მიერ გატარებულ სეპარატისტულ და ეროვნული იდენტობის წამშლელ სტრატეგიას მიაწერდნენ და უარეს შემთხვევაში ახლაც მიაწერენ საქრთველოს აფხაზთა მიმართ, კერძოდ მათი დამწერლობის ცვლილებას 1938 წელს. ამ არასწორი და ხშირად დამღუპველი ინფორმაციის გავრცელებას და შესაბამისად, ეროვნული მნიშვნელობის საინფორმაციო ომის წაგებას კი სწორედ, რეალური ისტორიების არ ცოდნა უდევს საფუძვლად. გავრცელებულ ნარატივებს იმის შესახებ, რომ ქართველები ძალისმიერი და მიზანმიმართული ხრიკებით ცდილობდნენ აფხაზთა ,,დამონებას'' და ამისათვის მათ დამწერლობას იყენებდნე სრულიად აბათილებს საქართველოს შსს სპეც. არქივში დაცული მასალები და ამაზევე საუბრობს აფხაზოლოგი თეიმურაზ გვანცელაძე წერილში ,,აფხაზური სამწიგნობრო ენის ქართულ გრაფიკაზე გადაყვანის ისტორიიდან.'' წითელმა სახლემწიფომ, რომელმაც ყველანაირი მატერიალური, არამატერიალური, საკრალური, პროფანული თუ აბსტრაქტული

იარაღი საკუთარ სამსახურში ჩააყენა ნუთუ არ იცოდა, რომ აფხაზური დამწერლობა ქართული გრაფიკის იყო? იმპერიამ იცის რას ფიქრობ ძილის წინ და გამორიცხულია არ სცოდნოდა რას აკეთებდა 16 წელი საქართველო აფხაზეთის „წინააღმდეგ''. ეს იმ საინფორმაციო ომის დასაწყისი იყო, რომლის ტრაგიკულ შედეგებსაც დღემდე ვიმკით, როგორც აფხზი ასევე ქართელი ერი. საბჭოთა კავშირმა შთააგონა აფხაზ ხალხს ქართველთა მტრული დამოკიდებულების, მათზე დომინირების, ძალადობისა და დამორჩილების არასწორი ტენდენცია, და ამით აფხაზეთისათვის ყველაზე ახლოს მდგომი, მონათესავე და მისთვის საუკეთესო ქართული გრაფიკის რუსული კირილიცათი შეცვლას შეუწყო ხელი. ესეც ინფორმაციული ომის მოგებისთვის საჭირო, წინ გადადგმული ნაბიჯი იყო სტალინისთვის, აფხაზ ხალხს მიაწოდეს ბელადის სასურველი ინფომაცია-ქართველთა იმპრეიული მიზნების შესახებ.

1954 წელს სსრკ-მ საკუთარ მიზანს მიაღწია და აფხაზური კვლავ რუსულ გრაფიკაზე გადაიყვანა. ამან ხელი შეუწყო აფხაზებსა და ქართველებს შორის შუღლის ჩამოგდებას, დამწერლობის იმდენად გართულებას (64 ასო ოთხი შრიფტი), რომ თავად აფხაზებიც ივიწყებენ მას და რუსულ ენას იყენებენ. ყველაზე მნიშვნელოვანი, რასაც კრემლმა მიაღწია არის შემდეგი- აფხაზეთის აბრებზე, სხვადასხვა დაწესებულებზე მთლიანად გაქრა ქართული ასოები. დღეს თითქმის ყველაფერი რუსულადაა, აფხაზურიც კი მცირეა ქვეყნის ტერიტორიაზე. რეალურად ხდება აფხაზური ტოპონიმების შეცვლა რუსულის ხარჯზე.

სსრკ-ს დაშლის და თითქმის ერთსაუკუნოვანი განვლილი გზის მიუხედავად ვერ აღდგა კავშირი საქართველოსა და აფხაზებს შორის. რუსეთმა ხელოვნურად შექმნა ჩატეხილი ხიდის სინდრომი, რომელიც კიდევ უფრო მწვავდება და თითქოსდა არ არსებობს არავითარი საშუალება ხიდის აღსადგენად. აგრეთვე გააღრმავეს დაშორების ტენდენცია , რომელიც დღესაც ყელში უჭერს ქართველ ხალხს და ახრჩობს, თუმცა აფხაზთა გონებამდე თუ გულებამდე სათანადოდ ჯერ კიდევ ვერ აღწევს, რადგან დღესდღეისობითაც რუსული პროპაგანდა სწორედ დროში გაწერილი საინფორმაციო ომის ნაწილია.

ვფიქრობთ, ერთადერთი თუ არა ერთერთი გზა არის დიალოგი და ორივე მხრიდან თითო აგურის დადება, რომ ხიდმა კვლავ დაიწყოს გამთლიანება. ყველასათვის ცნობილია, რომ საქართველოში ორი სახელმწიფო ენაა: ქართული და აფხაზური(აფხაზეთის ტერირორიაზე). აქედანაც მტკიცდება, რომ ქართველებს არ სურთ აფხაზური ენის/ იდენტობის „გაქართულება“, არამედ კავშირის აღდგენა და ურთიერთობების განახლება.

გამოსავალი ცხადია, რომ საინფორმაციო ომში ჩაბმა და მისი უკუგებაა სწორედ სპეც არქივში დაცული მასალების ტირაჟირებით, სადაც კარგად ჩანს რომ ქართულ ალფავიტზე აფხაზურის გადაყვანა არა ქართველთა, არამედ კრემლის ინიციატივა

იყო გათვლილი სწორედ დაპირისპირებაზე ქართველებსა და აფხაზ ძმებს შორის, რომლის განმუმხტველად დიდი რუსეთი მოგვევლინებოდა. ეს იყო შედეგი საინფორმაციო ომისა და ამ დოკუმნეტების პოლიტიკური კონტექსტით წარდგინებისა.

ბიბლიოგრაფია

1. თამარ ბელქანია -,,სტალინური კულტУРА!''-გამომცემლობა აზრი. თბილისი 2016
2. თეიმურაზ გვანცელაძე ,, აფხაზური სამწიგნობრო ენის ქართულ გრაფიკაზე გადაყვანის ისტორიიდან'' http://www.amsi.ge/istoria/div/gvanc.html

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 05-39 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

INFLUENCE OF INFORMATION WAR ON MEDIA COVERAGE DURING THE FOUR-DAY CONFRONTATION OF ARMENIA-AZERBAIJAN IN 2016

(CASE STUDY)

Aptsiauri Elene,
Ivane Javakhishvili Tbilisi State University

ხელმძღვანელი: მაია ტორაძე

ასოცირებული პროფესორი

აბსტრაქტი. ჰიბრიდული ომის ელემენტების, განსაკუთრებით კი, საინფორმაციო ომების, გამოყენებამ უკანასკნელ პერიოდში მასშტაბური ხასიათი შეიძინა და სამხედრო, სახელმწიფოებრივი თუ სხვა მიზნების მიღწევის კარგ საშუალებად იქცა. ეს კი მედიისთვის სერიოზული საფრთხეა, რათა, აქტიურად მიმდინარე საინფორმაციო ომის პირობებში, არ იქცნენ დაპირისპირებული მხარეების იარაღად.

ნაშრომის მიზანია საინფორმაციო ომის გავლენის კვლევა სამი ქართული და ერთი რუსული ტელემაუწყებლის („რუსთავი 2,“ „იმედი,“ „საზოგადოებრივი მაუწყებელი,“ „RT“) კონტენტზე.

სომხეთ - აზერბაიჯანს შორის შეიარაღებული კონფლიქტი უახლოეს წარსულში მოხდა და დღესაც აქტუალურია, მისი ანალიზისა და კვლევის სამეცნიერო ნიმუშები კი, ძალზე ცოტაა. მოვლენების ამ რაკურსით კვლევა პირველად ჩატარდა და გარკვეული შედეგები მოგვცა მომავალში მედიაგაშუქების დასახვეწად.

კვლევის პერიოდში შევისწავლეთ 16 საინფორმაციო გამოშვება და 9 სიუჟეტი, რომლის საკვლევადაც გამოვიყენეთ რაოდენობრივი და თვისებრივი კონტენტ-ანალიზი. კვლევა დაეყრდნო ფრეიმინგის თეორიას.

კვლევის შედეგად მივედით შემდეგ დასკვნამდე, რომ ქართული მედიის შემთხვევაში, ადგილი ჰქონდა არა საინფორმაციო ომის ზეგავლენას, არამედ საკითხის არც თუ ისე სიღრმისეულად გაშუქებას, რადგან ფოკუსირება ძირითადად ფაქტების აღწერასა და მხარეების ოფიციალური პოზიციების დაფიქსირებაზე იყო გადატანილი, აქტიურად მიმდინარე საინფორმაციო ომი კი უყურადღებოდ დარჩა; ხოლო „RT-ის” შემთხვევაში იყო ნეგატიური გაშუქება და საინფორმაციო ომის ნიშნები.

საკვანძო სიტყვები: საინფორმაციო ომი, საინფორმაციო ომის გავლენა მედიაგაშუქებაზე, საერთაშორისო სტანდარტები საომარი მოქმედებების გაშუქების

დროს, სომხეთ-აზერბაიჯანის 2016 წლის დაპირისპირება, კვლევა ქართულ და რუსულ მედიაში.

Abstract. Elements of hybrid warfare, especially Information wars, are used very often in recent years. Information wars are a good way to achieve military, state or other goals. This fact is a serious threat to the media in order to keep the guns in the hands of the opposing parties during an active news war.

The purpose of the work is to research the impact of news war on the content of three Georgian and one Russian TV broadcaster ("Rustavi 2," "Imedi," "Public Broadcasting," "RT")

Armed conflict between Armenia and Azerbaijan has been in the near past and is still relevant today. Scientific samples of his analysis and research are very few. The survey was conducted for the first time and gave us some results in the future to improve media coverage.

During the research period, we studied 16 news outlets and 9 stories, which we used in quantitative and qualitative content analysis. The study relied on the theory of Framing .

As a result of the survey we came to the conclusion that the Georgian media did not have an impact on the Information war and the issue was not covered in depth. The focus was mainly on the description of the facts and the official position of the parties, and the active information war remained unattended; And in the case of "RT" there is negative coverage of the issue and information war signs.

KEYWORDS: Information war, Influence of information war on media coverage, international standards in coverage of military actions, confrontation between Armenia and Azerbaijan in 2016, research in Georgian and Russian med

შესავალი

კვლევის აქტუალობა და მნიშვნელობა

ისტორია აჩვენებს, რომ ლოკალური კონფლიქტების გავლენა მსოფლიოში მიმდინარე გლობალურ პროცესებზე ძალზედ მაღალია. ისეთი კონფლიქტებიც კი, რომლებიც, ერთი შეხედვით, მხოლოდ პატარა ქვეყნებისთვისაა საფრთხის შემცველი, გლობალური საინფორმაციო გარემოსთვის რეალურად მნიშვნელოვან ცვლადს წარმოადგენს. ასეთი ლოკალური კონფლიქტის მაგალითია კავკასიის რეგიონში მდებარე მთიანი ყარაბაღი, რომელსაც ხშირად „გაყინული კონფლიქტის“ სახელით მოიხსენიებენ.

სომხეთ - აზერბაიჯანის დაპირისპირებას დიდი ისტორია აქვს. მისი დაწყების ზუსტ თარიღზე დღემდე დავობენ. 1994 წელს ცეცხლის შეწყვეტის შეთანხმებას მოეწრა ხელი. ამის შემდეგ შეიარაღებული შეტაკებები ხშირად ხდებოდა, თუმცა, მათ შორის, 2016 წლის ოთხდღიანი ომი ყველაზე ფართომასშტაბიანი აღმოჩნდა. ამასთან, მასში შერწყმული იყო ძველი და ახალი თაობის ომის სახეობები, ანუ, სამხედრო მოქმედებების პარალელურად, აქტიურად მიმდინარეობდა საინფორმაციო ომიც. „ამ დაპირისპირებამ კიდევ ერთხელ აჩვენა, რომ თანამედროვე მსოფლიოში ინფორმაციული და კიბერ ომი საბრძოლო მოქმედებების განყოფელ ნაწილად იქცა (CyberHouse, 2016).“

ბუნებრივია, კონფლიქტი, რომელიც რეგიონის შემადგენლობაში შემავალ ქვეყანაში ხდება, სახიფათოა სხვა სახელმწიფოებისთვისაც. არსებობს არაერთი მიზეზი თუ რატომ არის სომხეთ-აზერბაიჯანის დაპირისპირება საქართველოსთვის მნიშვნელოვანი. ყარაბაღი საქართველოსთან ტერიტორიულად ახლოსაა - თითქმის იმავე მანძილითაა დაშორებული თბილისიდან, როგორც ბათუმი (ნამჩავაძე, ბ., 2016). ამასთან, ბ. ნამჩავაძის აზრით, იმის გამო, რომ სომხეთი და აზერბაიჯანი საქართველოს მსხვილი ეკონომიკური პარტნიორები და საგარეო ვაჭრობითა და ტურიზმით დაკავშირებული ქვეყნებია, შესაძლებელია, კონფლიქტს მოჰყვეს ინვესტიციებისა და ქვეყნის ეკონომიკური განვითარების ტემპის შემცირება; საქართველოს ენერგო ინფრასტრუქტურის მიზანში ამოღების საფრთხეებსა და ბაქო–ჯეიჰანის ნავთობსადენთან დაკავშირებულ რისკებზე საუბრობს სომხეთში არსებული რეგიონული კვლევების ცენტრის დირექტორი რიჩარდ გირაგოსიანი (გირაგოსიანი, რ., 2017); ასეთივე საფრთხედ მიიჩნევა სომხეთში მდებარე მეწამულის ატომური ბირთვული ელექტოსადგურის თუნდაც შემთხვევით დაზიანება[1]; ანალიტიკოსი ლ. გოგოლაძე თვლის, რომ ამ ყველაფერმა შეიძლება ეთნიკური დაპირისპირებაც გამოიწვიოს საქართველოს ტერიტორიაზე (გოგოლაძე ლ., 2016), რადგან, თუ საქსტატის 2014 წლის საყოველთაო აღწერის მონაცემებს გადავხედავთ, ვნახავთ, რომ, ეროვნებით ქართველი მოსახლეობის შემდეგ, ყველაზე დიდი დიასპორა სწორედ სომხეთსა და აზერბაიჯანს ჰყავს (ქვეყნის მაცხოვრებელთა 6,3% აზერბაიჯანელია, 4,5 კი - სომეხი[2]). კონფლიქტოლოგი ზაზა ცოტნიაშვილი კი სიტუაციის დიდ რელიგიურ დაპირისპირებაში გადაზარდასაც არ გამორიცხავს. ასევე ყურადღებას ამახვილებს აზერბაიჯანისთვის პაკისტანის, როგორც ბირთვული სახელმწიფოს მხარდაჭერაზე[3].

ანალიტიკოსთა მოსაზრებით, „საქართველო არის ზუსტად კონფლიქტის შუაში და, მისი გვერდის ავლით, ვერც რუსეთი - სომხეთს და ვერც თურქეთი - აზერბაიჯანს

[1] https://www.youtube.com/watch?v=NVwGzTDd8UA;
[2] http://census.ge/ge/mosakhleobis-2014-tslis-sakoveltao-aghtseris-dziritadi-shedegebi-zogadi-informatsia/201#.WyAfeoozbIW;
[3] https://www.youtube.com/watch?v=NVwGzTDd8UA.

სახმელეთო და საჰაერო დახმარებას ვერ გაუწევენ". ამიტომ ჩნდება განსაკუთრებული საფრთხე საქართველოს, როგორც სატრანზიტო მაგისტრალის გამოყენებისა (გოგოლაძე, ლ.,2016). საგულისხმოა ისიც, რომ რუსეთი და სომხეთი არიან კოლექტიური უსაფრთხოების ხელშეკრულების ორგანიზაციის წევრები (CSTO), რომელიც ითვალისწინებს სამხედრო პარტნიორობას, რის საფუძველზეც ნებისმიერ წევრ ქვეყანაზე ძალადობა ყველა მათგანაზე შეტევად აღიქმება[4].

ჩვენი კვლევის აქტუალობა სწორედ იმაში მდგომარეობს, რომ საინფორმაციო ომების პირობებში (ნებისმიერი კონფლიქტის დროს) საქართველოსთვის სასიცოცხლოდ მნიშვნელოვანია ობიექტური ინფორმაციის ფლობა და საზოგადოების დაცვა პროპაგანდისტული ზეგავლენისაგან. სწორედ ამიტომ, აუცილებელია მედიის სტანდარტების მიხედვით მუშაობა, მით უფრო, რომ უკვე აღარ არსებობს ლოკალური და გლობალური კონფლიქტები. საჭიროა, დავაკვირდეთ და განვიხილოთ შეცდომები, შემდეგ კი განვლილ გაკვეთილებზე ვისწავლოთ და მომავალში გავაუმჯობესოთ გაშუქების ხარისხი.

კვლევის მიზანი

კვლევის მიზანია დაკვირვების გზის დავადგინოთ, რამდენად მოახდინა გავლენა საინფორმაციო ომმა მედიის მუშაობაზე ამ კონფლიქტში და დაარღვეს თუ არა (და როგორ) ჟურნალისტებმა საყოველთაოდ აღიარებული მედიასტანდარტები ომის გაშუქების დროს.

კვლევის სიახლე

ომი უახლოეს წარსულში მოხდა და მისი ანალიზის, კვლევის სამეცნიერო ნიმუშებიც მცირედ მოიპოვება. აღნიშნული მოვლენების ამ რაკურსით კვლევა პირველია და შესაბამისად გარკვეულ შედეგებს მოგვცემს მომავალში მედიაგაშუქების დასახვეწად.

საკვლევი კითხვები

კვლევის დაწყებამდე შემუშავდა შემდეგი კითხვები:

- რა სიხშირით შეიქმნებოდა მედიაში სომხეთ-აზერბაიჯანის კონფლიქტი და რამდენჯერ იყო იგი საინფორმაციო გამოშვების დღის მთავარი თემა?
- ირღვეოდა თუ არა ომის მიმდინარეობისას ომის გაშუქების საყოველთაოდ აღიარებული საერთაშორისო სტანდარტები და ნორმები?
- რა წყაროებს ეყრდნობოდნენ ქართველი ჟურნალისტები, ვინ იყო მათი პირველწყარო?

[4] https://en.wikipedia.org/wiki/Collective_Security_Treaty_Organization;

- ხომ არ ექცეოდნენ გავლენის ქვეშ ჟურნალისტები უშუალოდ ადგილზე მუშაობის დროს?
- მსჯელობდნენ თუ არა საკითხის გაშუქებისას საქართველოსთვის არსებულ საფრთხეებზე?
- შეექმნებოდა თუ არა საბრძოლო მოქმედებების პარალელურად მიმდინარე საინფორმაციო ომი?

ამ კითხვებზე პასუხის გასაცემად შევისწავლეთ შემდეგი ტელეკომპანიები: „იმედი“ და „რუსთავი 2,“ რომლებიც შეირჩა რეიტინგის მიხედვით;[5] „საზოგადოებრივი მაუწყებელი,“ როგორც ეროვნული ტელემაუწყებელი და „Russia Today,“ რუსული პროპაგანდისტული ტელევიზია, რომელიც არაერთ ქვეყანაში მაუწყებლობს და, პოლიტიკური მიზნების მიღწევას - რუსეთის იდეოლოგიის დამკვიდრებას - ყალბი ინფორმაციების, ე.წ. „Fake News“-ების, გავრცელებით ცდილობს.

საკვლევ პერიოდად განისაზღვრა 2016 წლის 2-5 აპრილი, საბრძოლო მოქმედებების მიმდინარეობის პერიოდი. ასევე გაანალიზებულია 2016 წლის, 31 დეკემბრის, შემაჯამებელი გადაცემები, იმის დასადგენად, თუ რამდენად სერიოზულად და მნიშვნელოვნად აღიქვამს მედია ამ კონფლიქტს და უბრუნდება თუ არა გარკვეული დროის შემდეგ მის განხილვას. გაანალიზდა ქართული ტელეარხების 16 მთავარი საინფორმაციო გამოშვება და RT–ის 9 სიუჟეტი.

საკვლევი კითხვებიდან გამომდინარე, ჩამოყალიბდა ჰიპოთეზა:

- მედიასაშუალებები, საინფორმაციო ომის მიმდინარეობისას, ექცეოდნენ გარკვეული ძალების ზეგავლენის ქვეშ და არღვევდნენ ომის გაშუქების სტანდარტებს.

კვლევის მეთოდოლოგია

კვლევა განხორციელდა მედიის კვლევის ერთ-ერთი მეთოდის - **შემთხვევის ანალიზის** მიხედვით, გამოვიყენეთ მისი ორი ტიპი: აღწერითი, საკითხის შესასწავლად და კვლევითი - მედიასაშუალებებზე დაკვირვებისა და საინფორმაციო ომის შესაძლო გავლენის კვლევისათვის (Yin, R.K.,1994).

გამოყენებულია **რაოდენობრივი და თვისებრივი კონტენტ-ანალიზი.**

ყარაბაღის კონფლიქტის ანალიზის დროს **კლიპინგის** მეთოდით დავთვალეთ საკვლევ ობიექტებში მასალების რაოდენობა, ქრონომეტრაჟი და რიგითობა, რამაც მოგვცა

[5] http://www.bm.ge/ka/article/tvmr-2017-wlis-yvelaze-reitinguli-televiziebi/16418.

გარკვეული მონაცემები შინაარსობრივი ანალიზის გასაკეთებლად. რაც თავის მხრივ დაგვეხმარა, დაგვედგინა, ირღვეოდა თუ არა საინფორმაციო ომის გავლენით გაშუქების სტანდარტები, რა წყაროებს ეყრდნობოდნენ ჟურნალისტები, ადგილზე ჰყავდათ თუ არა საკუთარი წარმომადგენლები, იყო თუ არა აღქმული საქართველოსთვის არსებული საფრთხეები.

სიუჟეტების ტონალობის განსაზღვრისა და გავლენის შეფასებისთვის გამოვიყენეთ **ტონალობის ანალიზი**, რომლის მიხედვითაც დავაკვირდით ტელევიზიებს, თუ როგორ იყვნენ განწყობილები რომელიმე მხარის მიმართ - „პოზიტიურად," „ნეგატიურად" თუ „ნეიტრალურად." ანალიზის ეს ფორმა, სუბიექტურ შეფასებას იყენებს, მასალის შინაარსში ობიექტების მიმართ გამოხატული კეთილგანწყობის ან არაკეთილგანწყობის განსაზღვრისთვის (მიქელსონი, დ., გრიფინი, ტ.,ლ., 2005).

კვლევის სრულყოფისათვის ასევე გამოვიყენეთ თვისებრივი კვლევის მეთოდის - **სიღრმისეული ინტერვიუს** ნახევრად სტრუქტურირებული ფორმა, რამაც საშუალება მოგვცა მოგვეძიებინა სხვა მნიშვნელოვანი და უცნობი დეტალები, უკვე არსებული მასალების გარდა. ამ გზით შესაძლებელია ისეთი მონაცემების შეგროვება, რომელიც საშუალებას იძლევა შევადაროთ მიღებული მონაცემები (Weerakkody, N., 2009).

ინტერვიუები ჩავატარეთ კონფლიქტის ზონაში მომუშავე 4 ჟურნალისტთან და 3 ექსპერტთან, რომლებიც დაკავებულნი არიან კონფლიქტების, საინფორმაციო ომებისა და კიბერ უსაფრთხოების თემატიკაზე მუშაობით.

კვლევა დაეყრდნო **ფრეიმინგის თეორიას,** რომელიც „წარმოადგენს, იმას თუ როგორ, რა კონკრეტული იდეით არის დაწერილი და მოწოდებული ესა თუ ის ამბავი, შეიცავს საორიენტაციო ჰედლაინებს, სპეციფიკურ, საჭირო სიტყვებსა და ა.შ." (კაპელლა და ჯეიმსონი, 1997).

ფრეიმების დახმარებით, რომლებიც საშუალებას გვაძლევს გამოვავლინოთ გარკვეული ზეგავლენა, გავაანალიზეთ თუ რამდენად იცავდნენ ჟურნალისტები ზოგიერთ სტანდარტს, ასევე რამდენად ხშირად ახსენებდნენ რომელიმე მხარეს ან მათ მედიასაშუალებებსა თუ ომის არატრადიციულ ფორმებს.

კვლევის ფარგლებში მომზადდა **სატელევიზიო გადაცემაც.**

თავი I - ლიტერატურის მიმოხილვა

1.1. ომის თანამედროვე ფორმა: საინფორმაციო ომი და მისი შემადგენელი ფუნქციური სფეროები

ჰიბრიდული ომის ელემენტების გამოყენებამ, უკანასკნელ პერიოდში, პიკს მიაღწია. მათ შორის ყველაზე ხშირად საინფორმაციო ომები გვხვდება. სტაინის შეფასებით, ჩვენ ვართ ინფორმაციული საუკუნის შუა ეტაპზე, რომელმაც, ახალი მიზნები და შესაძლებლობები მოიტანა. ეს 21-ე საუკუნის ომის ფორმებს ცვლის, მაგრამ, მიუხედავად იმისა, რომ ომში ტყვიები სხვა მეთოდებით ჩანაცვლდა, საბოლოო მიზანი მაინც იგივე დარჩა - მოწინააღმდეგის დაპყრობა (Stein, G. J. 1995).

დ. ძიძიშვილი აღნიშნავს, რომ მკვლევრები ჯერ კიდევ ბოლომდე ვერ თანხმდებიან საინფორმაციო ომის ზუსტი დეფინიციის, შემადგენლობისა და ელემენტების შესახებ. ერთი ნაწილი მხოლოდ მედიაპლატფორმებს მოიაზრებს, მეორეს კი მიაჩნია, რომ „მისი ელემენტები არა საშუალებები, არამედ ხერხებია, მაგალითად: დეზინფორმაცია, ჭორების გავრცელება, ფსიქოლოგიური ზემოქმედება, შთაგონება, მითების შექმნა და ა.შ.“ (ძიძიშვილი, დ. 2015).

ტერმინს, პროფესორი დევიდ ალბერტი ნაშრომში - Defensive Information Warfare, მოიხსენიებს, როგორც „ყოვლისმომცველს,“ რომელიც განსხვავებულ ღონისძიებებს მოიცავს და ამ ღონისძიებებს ჰყოფს, როგორც შედარებით ძველი (კონკურენცია, კონფლიქტი, ომი) და ახალი (პროპაგანდისტული კამპანია, რომელიც მოიცავს მედია ომს, ანუ თავდასხმებს მეთაურებზე (ფიზიკური და არაფიზიკური), ასევე მათ საინფორმაციო წყაროებსა და კომუნიკაციის საშუალებებზე) წარმომავლობის მქონედ (ALBERTS, D.S., 1996).

კიდევ ერთი ავტორთა ჯგუფი საუბრობს ომის ამ ფორმის წარსულ დროსთან კავშირზე, რაზეც მეტყველებს ისიც, რომ ინფორმაცია სამხედრო ოპერაციების ძირითადი ნაწილი იყო საუკუნეების განმავლობაში. სამხედრო ლიდერები აღიარებდნენ მის მნიშვნელოვან როლს, როგორც ბრძოლის ველზე ხელშემწყობ ფაქტორს, ამიტომ ყოველთვის ცდილობდნენ მოეპოვებინათ გადამწყვეტი ინფორმაცია მოწინააღმდეგის შესახებ (Alberts, D.S., Garstka, J.J., Hayes, R.E., Signori, D.A., 2001). ამაზე მიანიშნებს ჩინელი სამხედრო სტრატეგისა და თეორტიკოსის სუნ-ძის (ძვ.წ.აღ. 543 – 495) ნაშრომი „ომის ხელოვნება.“ ის, მტრის გეგმებში ჩაწვდომასთან ერთად, გვთვაზობს მისით მანიპულირებისა და დასუსტების უამრავ ხერხს. გამარჯვების მოსაპოვებლად, კი, როგორც ტრადიციულ, ასევე არატრადიციული ძალების გამოყენებას (სუნ-ძი, 2016).

კვლევითი ორგანიზაცია Rand-მა 2013 წელს ჩაატარა კვლევა, რომელშიც აღნიშნულია, რომ აშშ-ის საჰაერო ძალები კვლავ განსაზღვრავენ საინფორმაციო ომს (IW), როგორც

ელექტრონული ომებისა და კომპიუტერული ქსელების ოპერაციების შემადგენლობას (Porche, I. R., Paul, C., York, M., და სხვ., 2013). საბოლოოდ, როგორც შმიტი წერს, ძირითადად, ყველა მკვლევარი მაინც მიდის იმ დასკვნამდე, რომ საინფორმაციო ომი, ეს არის ქმედებები, რომლებიც ზიანს აყენებს მოწინააღმდეგის ინფორმაციას, საინფორმაციო სისტემებს და ამავდროულად იცავს საკუთარს (Schmitt, M.N., 2002); სწორედ იმ გარემოში, სადაც ინფორმაციის ფლობა, გავრცელება ან მისით მანიპულირება განსაკუთრებით მნიშვნელოვანია[6], საინტერესოა Rand-ის სქემაც, სადაც ომი ჩაშლილია შემადგენელი ფუნქციური სფეროების მიხედვით:

ელექტრონული ომი (EW) - ელექტრონული თავდასხმები და თავდაცვა, ომის დროს დახმარება და სპექტრის მართვა-კონტროლი;

კომპიუტერული ქსელის ოპერაციები (CNO) - ინფორმაციის საკუთარი სარგებლობისთვის გამოყენება და დაცვა;

ქსელური ოპერაციები - ინფორმაციის უზრუნველყოფა;

ელექტრომაგნიტური სპექტრის ოპერაციები (EMSO) - სპექტრის მართვა, განაწილების სიხშირე;

საინფორმაციო ოპერაციები (IO) - ელექტრონული ომი, სამხედრო ხრიკები, ფსიქოლოგიური, საიდუმლო და კომპიუტერული ქსელის ოპერაციები;

სიგნალების დაზვერვა (SIGIN) - შეგროვება და მათი დახშობა;

სამხედრო ინფორმაცია, მხარდაჭერის ოპერაციები (MISO) - კოორდინაცია სამხედრო ინფორმაციის მხარდაჭერის ოპერაციებზე;

(ცალკე განიხილება **ყოფილი ფსიქოლოგიური ოპერაციები (PSYOP) -** ემოციებზე ზეგავლენა, ამოცანებისა და ქცევების მოფიქრება);

საზოგადოებასთან ურთიერთობის ოპერაციები - ძალებზე, პოპულაციებზე ყურადღების გამახვილება;

ცოდნის მართვა - შექმნა, ორგანიზება, გამოყენება და გადაცემა (Porche, I. R., Paul, C., York, M., და სხვ., 2013).

მოლანდერის, რიდლისა და უილსონის მიხედვით, მიუხედავად იმისა, რომ საინფორმაციო ომს არ აქვს წინა ხაზი, პოტენციური ბრძოლის ველი ყველგან გვხვდება (Molander, R.C., Riddile, A.S., Wilson, P. A.). ამ მოსაზრებას ამტკიცებს ტეილორიც და ამბობს, რომ ომი მოიცავს ყველა ფრონტს, მათ შორის - ახალ ამბებს, ჟურნალისა და

[6] https://en.oxforddictionaries.com/definition/information_war.

გაზეთის სვეტებს, საერთაშორისო რადიოსიგნალებს, მუდმივ რეჟიმში, სატელევიზიო და ინტერნეტსივრცეს. თანამედროვე მსოფლიოში მედიის მართვა და მისით მანიპულირება ბრძოლის გადამწყვეტი ფორმაა, რომლითაც დღეს ომებში გამარჯვება მიიღწევა (Tylor, A., 2001).

აქამდე არსებული კონფლიქტების ანალიზის საფუძველზე შეგვიძლია, დავუშვათ, რომ ომის გაშუქების სტანდარტების დაუცველობით არსებობს მაღალი ალბათობა იმისა, რომ ჟურნალისტი მოექცეს ყალბი ინფორმაციის (დეზინფორმაციის, პროპაგანდის) ზეგავლენის ქვეშ და განიცადოს საინფორმაციო ომის გავლენა.

1.2. საერთაშორისო სტანდარტები საომარი მოქმედებების გაშუქების შესახებ

მეცნიერები მეორე მსოფლიო ომის დროს არსებული მანიპულირების მეთოდებისგან ბევრად უფრო დახვეწილ მეთოდად მიიჩნევენ თანამედროვე ეპოქის პროპაგანდისტულ სტრატეგიებს. ჟურნალისტებს კი კონფლიქტში მთავარ მოთამაშეებად ხედავენ იმ გარემოში, სადაც მეომარი მხარეები და მთავრობები მათ აღიქვამენ, როგორც არამხოლოდ იარაღს, არამედ პროპაგანდის მანქანას (Gjelten,T., 1998).

ნოიმენი და ფამი სამშვიდობო ჟურნალისტიკას კატალიზატორის ფუნქციის მქონედ მიიჩნევენ და საუბრობენ იმაზე, რომ ბოლო ოთხი ათწლეულის განმავლობაში მედიაკრიტიკოსები, მშვიდობის აქტივისტები და პროფესიული მედია ასოციაციები ჟურნალისტებს სთხოვენ, ხელი შეუწყონ ჟურნალისტიკას ამ მიმართულებით (Neumann, R., Fahmy, S., 2016). ამას ემსახურება ომისა და მშვიდობის გაშუქების ინსტიტუტის (Institute For War & Peace Reporting) მიერ შემუშავებული „მშვიდობის გაშუქების ექვსი სავალდებულო წესი ჟურნალისტებისთვის:

- კონფლიქტში გარკვევის ვალდებულება - განვითარების ისტორიის, არსის, მოგვარების შესაძლო გზები გამოკვლევა. ომის კანონების, კონფლიქტოლოგიისა და კონფლიქტების მშვიდობიანი მოგვარების პროცესების ცოდნა.
- სამართლიანად გაშუქება - ბალანსის დაცვა, „მნიშვნელოვანი კომპლექსური საკითხების, სხვადასხვა ინტერესთა ჯგუფებისა თუ ქვეჯგუფების შეხედულებების გაშუქება.“
- კონფლიქტის წინაპირობასა და მიზეზებზე საუბარი - მხარეების ლეგიტიმური და მცდარი უკმაყოფილებების გაჟღერება.
- ადამიანური მხარის წარმოჩენა (ნებისმიერ მხარეს მყოფთა) - „დაბალანსებულად, პროფესიონალურად, ძალდატანების გარეშე.“ ეს ვალდებულება განისაზღვრება, როგორც რესპონდენტების, ისე აუდიტორიის მიმართ.
- სამშვიდობო ინიციატივების გაშუქება (მშვიდობის დამყარებისა და შერიგებისკენ გადადგმული ნაბიჯების) იმავე რაოდენობით, რა რაოდენობითაც

შეუქდება კონფლიქტის გამწვავება. ასევე საჭიროა მტრულად განწყობილ მხარეთა შორის წყაროების მოძებნა, განსაკუთრებით კი ისეთი წყაროების, რომლებიც „გასცდებიან მოვლენათა მარტივი ბიპოლარული ინტერპრეტირების ფარგლებს.“

- საკუთარი გავლენის აღიარება - ჟურნალისტებს გააზრებული უნდა ჰქონდეთ, რომ მათი მომზადებული მასალა გავლენას ახდენს კონფლიქტზეც და ადამიანთა ცხოვრებაზეც. მნიშვნელოვანია ისიც, რომ „ფრთხილად იყვნენ, რათა არ მოხდეს მათი ბოროტად გამოყენება რომლიმე მხარის მიერ ან ძალადობის წამქეზებლად“ (ომისა და მშვიდობის გაშუქების ინსტიტუტი, 1999).

ჟენევის 1949 წლის 12 აგვისტოს კონვენციების დამატებითი ოქმის, საერთაშრისო შეიარაღებული კონფლიქტების მსხვერპლთა დაცვის შესახებ (I ოქმი, 1977 წლის 8 ივნისი), მე-3 ნაწილის, მე-3 თავის, 79-ე მუხლის მიხედვით, შეიარაღებული კონფლიქტის რაიონში მომუშავე ჟურნალისტები არ სარგებლობენ რაიმე განსაკუთრებული უფლებითა თუ პრივილეგიით, ისინი განიხილებიან, როგორც ჩვეულებრივი სამოქალაქო პირები[7]

თავი - II. კონფლიქტის შესახებ

2.1. სომხეთ - აზერბაიჯანის დაპირისპირების ისტორია

როგორც საზოგადოებრივი მაუწყებლის სიუჟეტში[8] აღნიშნავენ, ყარაბაღის კონფლიქტს ისტორიულ-კულტურული ფესვები აქვს, რაც გასული საუკუნის ბოლოდან იწყება და რომელსაც დღემდე ეთნიკურად სომეხი სეპარატისტები მართავენ.

მთიანი ყარაბაღი საბჭოთა პერიოდში აზერბაიჯანის შემადგენლობაში იყო, თუმცა მოსახლეობის დიდ ნაწილს ეთნიკურად სომხები შეადგენდნენ (გადახაბაძე, ე., 2016).

1988 წლის 22 თებერვალს კონფლიქტი შეიარაღებულ დაპირისპირებაში გადაიზარდა და სომხეთის კონტროლირებადი გახდა არა მხოლოდ მთიანი ყარაბაღი, არამედ აზერბაიჯანელებით დასახლებული მიმდებარე რაიონებიც, რესპუბლიკის 20%, წერს გაბიევი. რთულ ეკონომიკურ ვითარებაში აღმოჩენილმა მხარეებმა ერთმანეთის მოქალაქეებს ეთნიკურად დევნაც დაიწყეს, რის შედეგადაც ათასობით ადამიანმა დაკარგა საცხოვრებელი ადგილი და იძულებით გადაადგილებულ პირთა რაოდენობამ (განსაკუთებით აზერბაიჯანელი მოსახლეობა) ერთ მილიონს მიაღწია (გაბიევი, ხ., 2003).

[7] https://bit.ly/2CQfwpN;

[8] https://www.youtube.com/watch?v=K89AnlsogQQ .

საზოგადოებრივი მაუწყებლი, 2016 წლის 10 აპრილის სიუჟეტში, განიხილავს ცეცხლის შეწყვეტის შეთანხმებას, რომელიც 1994 წელს გაფორმდა. ამ დროისთვის ყარაბაღზე კონტროლი, სომხეთის მიერ მხარდაჭერილ სეპარატისტებს ჰქონდათ დამყარებული და მთიანი ყარაბაღი დამოუკიდებელ რესპუბლიკად იყო გამოცხადებული. აზერბაიჯანული მხარე მიიჩნევს, რომ ომი არა სომხეთთან, არამედ რუსეთთან წააგეს, ასევე აპროტესტებენ სომხეთშიც, არ მოსწონთ, რომ აზერბაიჯანისთვის იარაღის ნომერ პირველი მიმწოდებელი მათი ტრადიციული სამხედრო პარტნიორი - რუსეთია.[9].

სომხეთ-აზერბაიჯანის კონფლიქტის დარეგულირების მიზნით, 1994 წელს **ეუთოს** ბუდაპეშტის სამიტზე რუსეთის, ამერიკისა და საფრანგეთის წარმომადგენლობის თავმჯდომარეობით, ჩამოყალიბდა **მინსკის ჯგუფი**[10].

1994 წლის შემდეგ გარკვეული ინციდენტები სომხეთსა და აზერბაიჯანს შორის სულ ხდებოდა, ვკითხულობთ საგარეო ურთიერთობა საბჭოს ვებგვერდზე, თუმცა 2016 წლის 2-5 აპრილს იყო ყველაზე მწვავე დაპირისპირება[11] და „გაყინულმა კონფლიქტმაც“ ლღობა დაიწყო.

ბრორსი ამბობს, რომ სიტუაცია სწორედ მაშინ გამწვავდა, როდესაც სომხეთისა და აზერბაიჯანის პირველი პირები (სერჟ სარქისიანი და ილჰამ ალიევი) საკუთარ ქვეყნებში აშშ-ის ბირთვული უსაფრთხოების სამიტიდან ბრუნდებოდნენ (Broers, L.,2016).

დაპირისპირების უეცარი აფეთქების მიზეზად ორივე მხარე განსხვავებულ და ურთიერთსაწინააღმდეგო ვერსიას ასახელებს, აღნიშნავენ აჰმედბეილი და კარაპეტიანი (აჰმედბეილი, ს., კარაპეტიანი, ა.,2016).

2.2. საინფორმაციო ომი სამარი მოქმედებების პარალელურად

ოთხდღიანი ომის დროს აქტიურად მიმდინარეობდა საინფორმაციო ომიც - წერს Cyber House[12]. მხარეები ავრცელებდნენ დეზინფორმაციას, როგორც საკუთარი წარმატების, ასევე მოწინააღმდეგის წარუმატებლობის შესახებ, აყალბებდნენ ინფორმაციასა და მონაცემებს, ურთიერთბრალდებების ფონზე შეცდომაში შეჰყავდათ საზოგადოება (Cyber House, 2016).

[9] https://www.youtube.com/watch?v=K89AnlsogQQ ;
[10] https://www.osce.org/minsk-group/108306 ;
[11] https://www.cfr.org/interactives/global-conflict-tracker#!/conflict/nagorno-karabakh-conflict;

[12] https://bit.ly/2FQ1fyO;

დამოუკიდებელი, არაკომერციული თურქული კვლევითი ცენტრის - AVIM[13]-ის შეფასებით, სტატიაში ვკითხულობთ, რომ ომის ადრეულ ეტაპზე სომხურმა მედიამ (მათ შორის, სოციალურმა) დაიწყო ინფორმაციის გავრცელება, რომ 50-60 ISIS-ის მებრძოლი გადავიდა აზერბაიჯანში არმიაში გასაწევრიანებლად. ეს ბრალდება კი შეიძლება გავიგოთ, როგორც პროპაგანდა, რომელსაც აქვს პოტენციური უარყოფითი შედეგები გრძელვადიან პერსპექტივაში. გარდა ამისა, პროპაგანდისტული ნაბიჯი იყო ისიც, რომ მედიამ ყურადღება გაამახვილა აზერბაიჯანში ადამიანთა უფლებების დარღვევებზე, რასაც გააკრიტიკებდა დასავლეთი და ალიევს წარმოაჩენდა, როგორც კორუმპირებულ დესპოტს (TUNCEL, T. K.,2016).

კომახია აღნიშნავს, რომ აზერბაიჯანელებმა შეტევები დაიწყეს ყარაბაღისა და სომხეთის საინფორმაციო საიტებსა და სოციალურ მედიაზე, რასაც საპასუხოდ აზერბაიჯანის სამთავრობო საიტებზე შეტევა მოჰყვა. „ამის მტკიცებულებად სომხეთის მხარემ ის ფაქტი მოიყვანა, რომ „სომეხი მოხალისეებით სავსე ავტობუსი „თვითმკვლელმა დრონმა“ ააფეთქა და შვიდი ადამიანის სიცოცხლე შეიწირა. სომხური მხარის შეფასებით, ავტობუსის ადგილმდებარეობის დადგენა, სავარაუდოდ, საკომუნიკაციო ხაზებზე განხორციელებული კიბერ შეტევის შედეგად მოხდა (კომახია, მ., 2016).

Cyber House - ის სტატიაში ვკითხულობთ, რომ სომხურმა ჰაკერულმა დაჯგუფებებმა DDOS შეტევებით გაითიშეს აზერბაიჯანის სამთავრობო (gov.az) და საინფორმაციო (apa.az, irevanaz.com, anarim.az, aze.az.) საიტები, გატეხეს აზერბაიჯანის პრეს-სააგენტოს ვებგვერდი და მოსკოვში აზერბაიჯანის საელჩოს ტვიტერის გვერდიც (Broers, L., 2016).

მკვლევარი ინგილიზიანი წერს, რომ ამავე დღეს გავრცელდა პრეზიდენტ ალიევის განცხადება ცეცხლის შეწყვეტის შესახებ, რაც შეფასდა გონივრულ პოლიტიკურ-სამხედრო ტაქტიკურ ნაბიჯად, რომლის მიზანიც გლობალური საინფორმაციო ომის წარმოება და ყარაბაღის სამხედრო მაღალჩინოსნებისთვის გაუგებრობის შექმნა იყო. ფაქტია, რომ ამ მეთოდმა იმუშავა, რადგან დასავლეთის საინფორმაციო გამოშვებებმა და ლიდერებმა სწრაფი რეაგირება მოახდინეს და სომხეთს ბრალი დასდეს ბრძოლის გაგრძელებაში, თუმცა რეალურად ბრძოლა არც შეწყვეტილა, პირიქით, პრეზიდენტის ამ განცხადებას მალევე მოჰყვა აზერბაიჯანის თავდასხმები ყარაბაღის სამხრეთ ნაწილებზე (Ingilizian, M., 2016).

Cyber House-ში ვკითხულობთ, რომ 4 აპრილს სომხურმა ჰაკერულმა დაჯგუფებამ გამოაქვეყნა 25 000 აზერბაიჯანელი ჯარისკაცის პირადი მონაცემები, რომელიც მათი ერთ-ერთი სამთავრობო საიტის (სახელი არ დაკონკრეტებულა) გატეხვით მოიპოვეს. ამის საპასუხოდ აზერბაიჯანელმა ჰაკერებმა სომხეთში არსებული რუსეთის საელჩოს ტვიტერი გატეხეს და გამოაქვეყნეს განცხადება, რომ რუსეთი უსამართლოდ იჭერს

[13] http://avim.org.tr/en/Yorum/A-SHORT-ASSESSMENT-OF-THE-4-DAY-WAR-IN-KARABAKH .

სომხეთის მხარეს და ემხრობა ცეცხლის შეწყვეტას, რადგან სომხეთი მარცხდება მათ მოახერხეს გაეთიშათ სომხეთის სამთავრობო პორტალებიც, ეროვნული ბანკის, ეროვნული უსაფრთხოების სამსახურის, ენერგეტიკისა და ეკონომიკის სამინისტროს გვერდები. მიუხედავად იმისა, რომ სომხური მხარე ადასტურებს შეტევების რეალურობას, უარყოფენ თურქი და აზერბაიჯანელი ჰაკერების მიერ მიყენებულ ზიანს.

ომი 5 აპრილს დასრულდა, თუმცა მცირე შეტაკებები 9 აპრილამდე გრძელდებოდა. ერთმანეთის მიმართ ურთიერთბრალდებები და საინფორმაციო ომი ცეცხლის შეწყვეტის შემდეგაც არ დასრულებულა. სომხეთ-აზერბაიჯანის „დაპირისპირებამ კიდევ ერთხელ აჩვენა, რომ თანამედროვე მსოფლიოში ინფორმაციული და კიბერ ომი, საბრძოლო მოქმედებების განუყოფელ ნაწილად იქცა“ (Cyber House, 2016).

III თავი. კვლევა, ძირითად

მიგნებები

3.1. ზოგადი რაოდენობრივი შედეგები

2016 წლის 2 აპრილიდან 5 აპრილის ჩათვლით, დავაკვირდით 4 ტელემაუწყებელის მთავარ საინფორმაციო გამოშვებებს (გამონაკლისები: RT-ის ვებგვერდზე განთავსებული სიუჟეტები, რადგან მთლიანი საინფორმაციო გამოშვებები არ მოიპოვება. ნაწილი იყო მხოლოდ კადრები და არა სიუჟეტები, თუმცა ამას კვლევის დასაწყისში დასახული მიზნებისთვის ხელი არ შეუშლია და გარკვეული ტენდენცია მაინც გამოიკვეთა; 3 აპრილის „იმედის“ 5-საათიანი საინფორმაციო გამოშვება გაანალიზდა, რადგან ამ დღეს 20 საათიანი ქრონიკის ნაცვლად გადიოდა ანალიტიკური გადაცემა) და ასევე 3 ქართული ტელემაუწყებლის წლის შემაჯამებელ გადაცემას. ჯამში ყარაბაღის კონფლიქტის მიმდინარეობის ამსახველი 5 დღიანი მონიტორინგის შედეგად 42 მასალა გაანალიზდა, რომელთა საერთო ხანგრძლივობამ 1 სთ. 52 წთ. და 55 წმ. შეადგინა.

საკვლევ პერიოდში საკითხს ყველაზე მეტი 15 მასალა „რუსთავი 2-მა“ მიუძღვნა, როგორც რაოდენობრივად, ასევე ხანგრძლივობითაც (53წთ. და 42 წმ.); შემდეგი იყო „იმედი” 12 მასალითა და 23 წთ. და 6 წმ. ხანგრძლივობით; “RT,” რომელმაც 1-ით მეტი (8) მასალა მოამზადა, ვიდრე „საზოგადოებრივმა მაუწყებელმა“ (7), თუმცა ქრონომეტრაჟში გახლდათ მნიშვნელოვანი სხვაობა: ამ უკანასკნელმა 26 წთ და 24 წმ. დაუთმო კონფლიქტს, “RT”კი 9 წთ და 43 წმ.

ცხრილი N 1.

ტვ	მასალების რაოდენობა	ქრონომეტრაჟი	რიგითობა
რუსთავი 2	15	53 წთ. 42 წმ.	1-ლი, 2,3 აპრილი; მე-4 , 4 აპრილი; მე-6, 5 აპრილი,
იმედი	12	23წთ. 6წმ.	1-ლი, 2,3 აპრილი; მე-3, 4 აპრილი; მე-5, 5 აპრილი; 31 დეკემბერი- გადაცემის 28წთ და 58 წმ-დან.
საზოგადოებრივი მაუწყებელი	7	26 წთ. 24 წმ.	1-ლი, 2,4 აპრილი; II ბლოკის 1-ლი 3 აპრილი; მე-4 ,5 აპრილი;
RT	8	9წთ. და 43 წმ.	

ასევე გავაანალიზეთ სიუჟეტთა რიგითობა საინფორმაციო გამოშვებებში (“RT“-ის გარდა). საბრძოლო მოქმედებების დაწყების პირველი ორი დღე, „რუსთავი 2-ისა“ და „იმედის“ გამოშვებებში, პირველ სიუჟეტად იყო წარმოდგენილი, ხოლო საზოგადოებრივი მაუწყებლის შემთხვევაში, მხოლოდ 2, 4 აპრილს გავიდა პირველ სიუჟეტად. რაც შეეხება წლის შემაჯამებელ გადაცემებს, კონფლიქტის, ცხელი წერტილებისა და პოლიტიკური საკითხების მიმოხილვის დროს, მხოლოდ „იმედმა“ გაიხსენა მომხდარი.

3.2.კონტენტ-ანალიზი

3.2.1. მონაცემთა ანალიზი სტანდარტებით მუშაობის თვალსაზრისით

კვლევის დასაწყისში ჩამოყალიბებულ მეორე, მესამე და მეოთხე საკვლევ კითხვებზე პასუხის გასაცემად გადავწყვიტეთ აღნიშნულ მედიასაშუალებებზე განსაზღვრულ პერიოდში დაკვირვება (2-5 აპრილის მთავარი საინფორმაციო გამოშვებები და 31 დეკემბრის შემაჯამებელი გამოშვება) ჩაგვეტარებინა კონტენტ-ანალიზის მეთოდითაც, რათა დაგვედგინა, რამდენად მოახდინა საინფორმაციო ომმა და მისმა ელემენტებმა გავლენა მედიის მუშაობაზე; ირღვეოდა თუ არა და როგორ ომის მიმდინარეობისას ომის გაშუქების საერთაშორისო, საყოველთაოდ აღიარებული სტანდარტები და ნორმები, რა წყაროებს ეყრდნობოდნენ ქართველი ჟურნალისტები, ჰყავდათ თუ არა მედიასაშუალებებს ადგილზე გაგზავნილი ჟურნალისტები, იყო თუ არა მსჯელობა საქართველოსთვის არსებულ საფრთხეებზე და იყო თუ არა დაცული - მშვიდობა - კონფლიქტის გაშუქების თანაფარდობა.

ცხრილი N2. 1-ლი სტანდატი კონფლიქტის (ისტორიის, არსისა და მოგვარების შესაძლო გზების) ცოდნა

ტვ	**2 აპრილი**	**3 აპრილი**	**4 აპრილი**	**5 აპრილი**	**31/ XII**
რუსთავი 2	ისტორია და მოგვარების გზები.	ისტორია მოკლედ.	დღის მიმოხილვა.		
იმედი	ისტორია (მცირედ).	ისტორიის და წინა დღეების მიმოხილვა.	მიმდინარე დაპირისპირების მიმოხილვა.	ჩართვები ადგილებიდან სადაც იყო საბრძლო მოქმედებები. მსხვერპლის გაშუქება; ყარაბაღის აზერბაიჯანული მხარის სამხედროების დასაფლავების კადრები;	კონფლიქტის არსი.
საზოგადოებრივი მაუწყებელი	ისტორია.	ისტორიისა და მიმდინარე ამბების მიმოხილვა.	ისტორიისა და მიმდინარე ამბების მიმოხილვა.	წარსულის მიმოხილვა.	
RT					

„რუსთავი 2-ისა “ და „იმედის“ ეთერში 2 და 3 აპრილის გამოშვებაში მიმოხილულია კონფლიქტის ისტორია, მოგვარების შესაძლო გზები. შემდეგი 2 დღე კი ძირითადად მიმდინარე ამბებს ეთმობა.

„საზოგადოებრივი მაუწყებლის“ 2 აპრილის გადაცემაში ისტორია წარმოდგენილია მოგვარების გზები კი - არა. 3 აპრილს მიმდინარე ამბების მიმოხილვაა, თუმცა სტუმართან საუბარი, გარკვეულწილად, მოიცავს ისტორიასაც. 4 აპრილს საუბრობენ, როგორც ძველ დაპირისპირებაზე, ასევე მიმდინარეზე და მოგვარების გზად განიხილავენ საქართველოს, როგორც შუამავლის როლს.

ცხრილი N3. მე-2 სტანდარტი - მხარეთა ბალანსი

ტვ	**2 აპრილი**	**3 აპრილი**	**4 აპრილი**	**5 აპრილი**	**31/XII**
რუსთავი 2	დაბალანსებულია.	დაბალანსებულია.	აზერბაიჯანი, სომხეთი.	დაბალანსებულია.	
იმედი	ძირითადად აზერბაიჯანული პოზიცია .	დაბალანსებულია.	აზერბაიჯანი, სომხეთი.	დაბალანსებულია.	აზერბაიჯანი.
საზოგადოებრივი მაუწყებელი	ყარაბაღის ერთ მაცხორებელთან ინტერვიუ.	დაბალანსებულია.	აზერბაიჯანი, სომხეთი.	ყარაბაღი,აზერბაიჯანი.	
RT		აზერბაიჯანული პოზიცია ნაკლებად.		დაბალანსებულია.	

„რუსთავი 2-მა“ 2 აპრილს წარმოადგინა დაბალანსებულად გაშუქებული ინფორმაცია სომხეთისა და აზერბაიჯანის შესახებ, თუმცა მცირე იყო ყარაბაღის წარმომადგენლებზე. 3 და 5 აპრილს სრულად დაბალანსებული იყო. ხოლო 4 აპრილს ძირითადად სომხეთ-აზერბაიჯანის პოზიციები გახლდათ.

„იმედმა“ 2 აპრილს ძირითადად აზერბაიჯანული პოზიცია გააშუქა. 3 და 5 აპრილს დაცული იყო. 4 აპრილს აზერბაიჯანისა და სომხეთის პოზიციები შუქდებოდა. ხოლო 31 დეკემბრის წლის შემაჯამებელი, რამდენიმე წამიანი მიმოხილვა მთლიანად აზერბაიჯანიული მხარის პოზიციებს წარმოადგენდა.

„საზოგადოებრივი მაუწყებელი“ 2 და 4 აპრილს აშუქებდა ორივე მხარეს, 2 აპრილს ყარაბაღიც გააშუქეს, რაც მხოლოდ ერთ მაცხოვრებელთან ინტერვიუთი შემოიფარგლა.

“RT-ის” შემთხვევაში 3 და 5 აპრილს სამივე პოზიცია გაშუქდა, თუმცა 3 აპრილს აზერბაიჯანული - ნაკლებად. საუბრობდნენ, თავდაცვის სამინისტროს ინფორმაციაზე ცეცხლის შეწყვეტის თაობაზე და იქვე ამბობდნენ, რომ ამას სომხეთი უარყოფს და საბრძოლო მოქმედებები კვლავ მიმდინარეობს.

ცხრილი N 4. მე-3 სტანდარტი - წინაპირობა და მიზეზები

ტვ	**2 აპრილი**	**3 აპრილი**	**4 აპრილი**	**5 აპრილი**	**31/XII**
რუსთავი 2	განხილულია.	ურთიერთსაწინააღმდეგო მოსაზრებებია წარმოდგენილი.			
იმედი	საუბრობენ რომ მიზეზები არ არის ცნობილი.		მიმოხილულია მიზეზები და ერთმანეთის დადანაშაულება.		
საზოგადოებრივი მაუწყებელი	წინაპირობა გაშუქებულია, მიზეზები არა.	შუქდება, რომ აზერბაიჯანულმა მხარემ დაიწყო სროლები ყარაბაღის მიმართულებით, რასაც სამხედრო ოპერაციები მოჰყვა.			
RT					

„რუსთავი 2-მა“ კონფლიქტის დაწყების პირველ დღეს, 2 აპრილს ისაუბრა ომის წინაპირობებსა და მიზეზებზე, 3 აპრილს მოქალაქეებისა და ოფიციალური პირების ურთიერთსაწინააღმდეგო მოსაზრებები იყო წარმოდგენილი, ომის დაწყებასთან დაკავშირებით.

„იმედის“ 2 და 4 აპრილის გადაცემაში მხოლოდ დაუდგენელ მიზეზებზე საუბრობდნენ.

„საზოგადოებრივმა მაუწყებელმა“ 2 აპრილს წინაპირობა გააშუქა, მიზეზები - არა. 3 აპრილს სომხური პოზიციიდან საუბრობდნენ, რომ აზერბაიჯანმა დაიწყო სროლა და ამას მოჰყვა სამხედრო ოპერაციები.

“RT-ის” არ განუხილავს მსგავი თემა.

ცხრილი N 5. მე-4 სტანდარტი- დაბალანსებულად გაშუქებული ადამიანური მხარე

ტვ	**2 აპრილი**	**3 აპრილი**	**4 აპრილი**	**5 აპრილი**	**31/ XII**
რუსთავი 2	დაშავებულებსა და დაჭრლებზეა საუბარი.	დაბალანსებულია.	დაბალანსებულია.	დაბალანსებულია.	
იმედი		გაშუქებულია ვიწროდ.		დაბალანსებულია(მსხვერპლსა და მოქალაქეებზე).	
საზოგადოებრივი მაუწყებელი	სომხური მხარის დაღუპულებსა და დაჭრილებზე.				
RT					

„რუსთავი 2-მა“ 2 აპრილს მხოლოდ დაშავებულებსა და დაჭრილებზე ისაუბრა. 3 (დიდი რაოდენობით), 4 და 5 აპრილს სიუჟეტები სავსებით დაბალანსებული იყო.

„იმედზე“ 3 აპრილს ცოტა ისაუბრეს მოქალაქეებზე, რომლებიც ცდილობენ სიმშვიდის შენარჩუნებას. 5 აპრილს კი დაბალანსებულად წარმოადგინეს ცნობები მსხვერპლსა და მაცხოვრებლებზე.

„საზოგადოებრივმა მაუწყებელმა“ 2 აპრილს სომხური მხარის დაღუპულებსა და დაჭრილებზე ისაუბრა.

“RT-ის” გაშუქებულ მასალაში 3 აპრილს მხოლოდ ტექსტში მოიხსენიებს ჟურნალისტი მოქალაქეებთან საუბარს.

ცხრილი N 6. მე-5 სტანდარტი- სამშვიდობო ინიციატივები

ტვ	**2 აპრილი**	**3 აპრილი**	**4 აპრილი**	**5 აპრილი**	**31/ XII**
რუსთავი 2	შუქდება.		შუქდება.	შუქდება.	

იმედი	მოწოდებები ცეცხლის შეწყვეტისკენ.	გაშუქებულია.	გაშუქებულია.	ცეცხლის შეწყვეტის შეთანხმება.	
საზოგადოებრივი მაუწყებელი	გაშუქებულია.	საერთაშორისო ორგანიზაციებისა და რუსეთის მოწოდებები.	გაშუქებულია.	ცეცხლის შეწყვეტის შეთანხმება, მინსკის ჯგუფის დაგეგმილი ვიზიტი კონფლიქტის ზონაში.	
RT		ცეცხლის ცალმხრივი შეწყვეტა.			

„რუსთავი 2-ის“ 2 აპრილის გაშუქებაში ისმის რესპონდენტთა მოწოდებები საერთაშორისო ორგანიზაციის მეტი ჩართულობისკენ. 4 აპრილს კონფლიქტის მოგვარებისკენ მიმართული მოწოდებებია საერთაშორისო საზოგადოებისა და ევროსაბჭოს მიერ. 5 აპრილს აშუქებენ ცეცხლის შეწყვეტასა და სომხეთის პრეზიდენტის მოწოდებას ეუთოს მეტი აქტიურობისკენ, ასევე მინსკის ჯგუფის წევრების ადგილზე ჩასვლასა და მონიტორინგს.

„იმედის“ ეთერში 2, 3 და 4 აპრილის ისმის მოწოდებები ცეცხლის შეწყვეტისკენ. 5 აპრილს შუქდება ცეცხლის შეწყვეტის შეთანხმება.

„საზოგადოებრივი მაუწყებლის“ 2 აპრილის ეთერში წარმოდგენილია რუსეთის მოწოდებები ცეცხლის შეწყვეტის შესახებ, საუბარია მინსკის ჯგუფზეც და გაშუქებულია ქართველი პოლიტიკოსების პოზიციები, ამ კუთხით. 3 აპრილს საერთაშორისო ორგანიზაციები და კვლავ რუსული მხარის მოწოდებები ისმის. 4 აპრილს გაშუქებულია ლავროვის მოწოდებები, თურქეთის მხარის განცხადებები, ეუთოს სამუშაო ჯგუფის შეხვედრა და საქართველოში ნატოს სამოკავშირეო ოფისის ხელმძღვანელის განცხადება. 5 აპრილს - ცეცხლის შეწყვეტის შეთანხმება და მინსკის ჯგუფის თანათავმჯდომარეების ვიზიტი კონფლიქტში ჩარულ მხარეებთან.

“RT” 3 აპრილს აშუქებს ცეცხლის ცალმხრივ შეწყვეტას; ხოლო 5 აპრილს ცეცხლის შეწყვეტა არ შუქდება სრულყოფილად, ამბობენ რომ შეტაკებები შეჩერდა, მაგრამ არტილერიული დაბომბვები გრძელდება და აკეთებენ პროგნოზსაც, რომ ეს კრიზისი შესაძლოა ფართო მასშტაბიან ომში გადაიზარდოს.

3.2.2. ტელემაუწყებლების წყაროები კონფლიქტის გაშუქებისას

საბრძოლო მოქმედებების გაშუქების დროს ტელემაუწყებლები მრავალფეროვან წყაროებს იყენებდნენ. პირველ რიგში გამოვყოთ პირველწყარო. „რუსთავი 2-ს“ პირველივე დღიდან ადგილზე ჰყავდა საკუთარი კორესპონდენტები. „იმედს“ 3 და 5 აპრილს. „საზოგადობრივ მაუწყებელს“ სართოდ არ ჰყოლია, ‘‘RT-გან“ განსხვავებით.

ცხრილი N 7.

ტელევიზია	საკუთარი კორესპონდენტები
რუსთავი 2	2-დან - 5 აპრილამდე
იმედი	3, 5 აპრილი
საზოგადოებრივი მაუწყებელი	არ ჰყოლია
RT	ჰყავდა

რაც შეეხება ზოგადად წყაროებს, „რუსთავი 2-მა“ გამოიყენა: დაპირისპირებული მხარეების ოფიციალური პოზიციები, მათი მედიასაშალებები და მცხოვრებლები, რუსეთის პოზიცია, ქართველი პოლიტიკოსებისა და სამხედრო ექსპერტების, ასევე ეუთოს, ევოკავშრის, ნატოს ვარაუდები, შეფასება - მოწოდებები.

„იმედი“ იყენებდა: მხარეებისა და მოქალაქეების ოფიციალურ პოზიციებს, საერთაშორისო ორგანიზაციებისა და სხვა სხვადასხვა ქვეყნების პოლიტიკოსთა და ექსპერტთა კომენტარებს, ასევე სააგენტო ინტერფაქსს, BBC, აზერბაიჯანულ სააგენტოზე დაყრდნობით BBC-ისა და BBC ის რუსული ბიუროს ცნობებს.

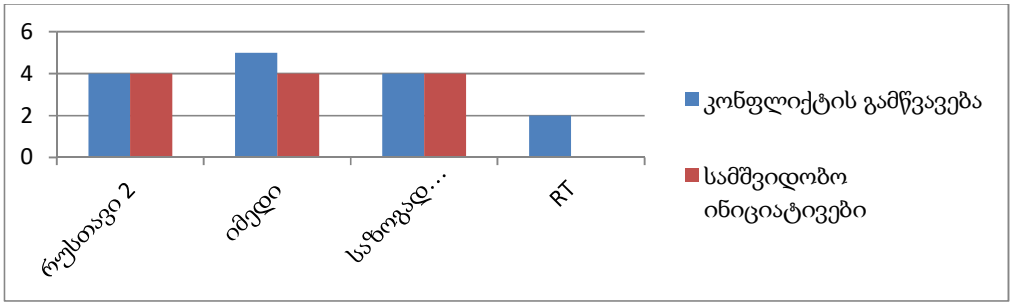
„საზოგადოებრივი მაუწყებელი“ იყენებდა: რუსეთის, აზერბაიჯანისა და სომხეთის ოფიციალურ პოზიციებსა და მედიას, ყარაბაღის თავდაცვის სამინისტროს, აზერბაიჯანის სამოქალაქო წრეებს, ქართველ ექსპერტებს, საერთაშორისო ორგანიზაციებს.

“RT” იყენებდა: დაპირისპირებული მხარეების ოფიციალურ პოზიციებს, მაცხოვრებლებს, სომხური მხარის სამხედრო პირებს.

3.2.3. კონფლიქტისა და სამშვიდობო ინიციატივების დაბალანსებული გაშუქება და მსჯელობა საქართველოსთვის არსებულ საფრთხეებზე

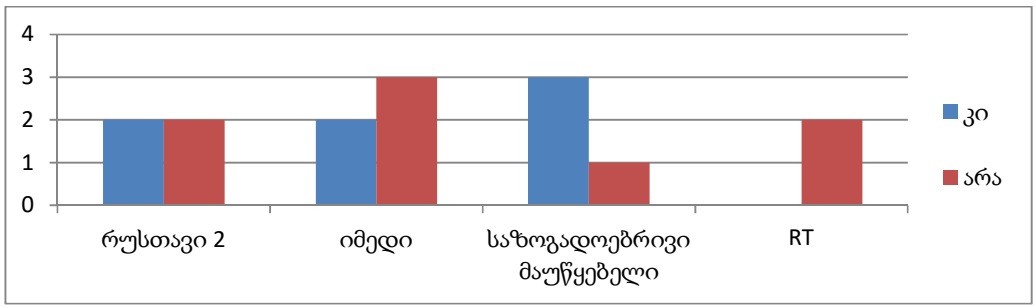
კონფლიქტის გამწვავებისა და სამშვიდობო ინიციატივების თანაფართობა დაცულია „რუსთავი 2-ის“ და „საზოგადოებრივი მაუწყებლის ეთერში, ასევე „იმედის შემთხვევაშიც თუ 31 დეკემბრის მიმოხილვას არ ჩავთვლით. “RT“-მ 2-ჯერ გააშუქა კონფლიქტის გამწვავება, სამშვიდობო ინიციატივები კი არცერთხელ.

დიაგრამა N 1.კონფლიქტისა და სამშვიდობო ინიციატივების გაშუქება



რაც შეეხება მსჯელობას საქართველოსთვის არსებულ საფრთხეებთან დაკავშირებით, „რუსთავი 2-მა“ 2 და 4 აპრილს იმსჯელა, „იმედმა“ 3, 4 აპრილს და „საზოგადოებრივმა მაუწყებლმა 2, 3 და 4 აპრილს.

დიაგრამა N 2. საქართველოსთვის არსებულ საფრთხეებზე მსჯელობა



3.3.მედიის ფრეიმები

ფრეიმინგის თეორიის დასადასტურებლად, კონტენტ-ანალიზით დადგინდა საკვანძო სიტყვების გამოყენების სიხშირე, რომლებსაც მედია იყენებდა საკითხის გაშუქების დროს.

ცხრილი N 8.

კოდირების სიტყვები	რუსთავი 2	იმედი	საზოგადოებრივი მაუწყებელი	RT	სულ
კონფლიქტი	30	42	35	5	**112**
ომი	9	4	7	2	**22**
ფრონტის ხაზი	12	3	5	1	**21**
ესკლაცია	11	5	8		**24**
დეესკალაცია	2	2	2		**6**
საბრძოლო მოქმედებები	22	12	26	7	**67**
აზერბაიჯანმა დაიწყო საბრძოლო მოქმედებები	6	5		2	**13**
სომხეთმა დაწყო საბრძოლო მოქმედებები	5	3	1	1	**10**
ცეცხლის შეწყვეტა	22	14	26	4	**66**
მსხვერპლი	18	2	12	1	**33**
სტაბილიზაცია	2		1	1	**4**
2016 წლის კონფლიქტის მიზეზები	2		1		**3**
რუსეთი	38	11	19		**68**
საქართველო	15	17	23		**55**
სომხეთი	82	37	52	5	**176**
აზერბაიჯანი	107	64	62	8	**241**
ყარაბაღი	68	27	40	9	**144**
სომხეთის ოფიციალური პოზიცია	5	7	4		**16**
აზერბაიჯანის ოფიციალური პოზიცია	17	11	13	3	**44**
აზერბაიჯანული მედია	5	1	1		**7**
სომხური მედია	8		2		**10**
ყარაბაღის მედია	1				**1**
რუსული მედია	2				**2**
მინსკის ჯგუფი	4	5	6		**15**
ორი მხარე	9	3	6	2	**20**
პროპაგანდა	2				**2**
საინფორმაციო ომი	1				**1**
ურთიერთსაპირისპირო მონაცემები	10	4	5		**19**
ჰიბრიდული გამოწვევები		1			**1**

საბრძოლო მოქმედებების გაშუქების დროს მედიამ ყველაზე ხშირად დაპირისპირების გამოსახატავად გამოიყენა სიტყვა „კონფლიქტი“ 122-ჯერ, ხოლო ომი 22-ჯერ, რაც მიუთითებს იმაზე, რომ ისინი ცდილობდნენ სიტუაციის, რაც შეიძლება ნეიტრალური ტერმინით შეფასებას. თუმცა იგივეს ვერ ვიტყვით, ესკალაცია - დეესკალაციის შემთხვევაში.

აზერბაიჯანისა და სომხეთის მოხსენიების თანაფარდობა საბრძოლო მოქმედებების დაწყებაში თითქმის ყველა ტელევიზიას დაბალანსებული აქვს. სომხეთის ოფიციალური პოზიცია ყველაზე მეტჯერ ახსენა „იმედმა,“ აზერბაიჯანის კი „რუსთავი 2-მა.

კონფლიქტის მიზეზებზე დიდი ყუადღების გამახვილება მედიამ არ ჩათვალა საჭიროდ, რაც მსგავსი საკითხების გაშუქების ერთ-ერთი სტანდარტია, 2-ჯერ ახსენა „რუსთავი 2-მა“ და ერთხელ „საზოგადოებრივმა მაუწყებელმა.“

ცეცხლის შეწყვეტა საკმაოდ დიდი რაოდენობით, 66- ჯერ, ახსენეს. „საზოგადოებრივმა მაუწყებელმა,“ ეს ტერმინი გამოიყენა 26-ჯერ, რაც ხშირი გამოყენებაა, თუ გავითვალისწინებთ მის ქრონომეტრაჟს.

რუსეთი ჯამში 68-ჯერ ახსენეს, მათ შორის ყველაზე მეტჯერ „საზოგადოებრივმა მაუწყებელმა“ 19-ჯერ. აქედან რუსულ მედიას საუბარი 2 -ჯერ შეეხო „რუსთავი 2-ის“ ეთერში.

3.4. ყარაბაღის 2016 წლის 4 დღიანი კონფლიქტის ტონალობის ანალიზი

ტონალობის განსაზღვრაში დაგვეხმარა კოდირების ანკეტა, რომელიც მოიცავს, როგორც წამყვანის, ასევე ჟურნალისტებისა და რესპონდენტების ტექსტებს. სიუჟეტის ტონალობა 100 ქულიან შკალაზე ფასდება. ნეგატიურ ფრაზებად განისაზღვრა: „ომი“, „ფრონტის ხაზი“, „ესკალაცია“, „აზერბაიჯანმა საბრძოლო მოქმედებები დაიწყო“, „სომხეთმა საბრძოლო მოქმედებების დაწყო“. პოზიტიურად: „დეესკალაცია“, „ცეცხლის შეწყვეტა“, „სიტუაციის სტაბილიზაცია“, „კონფლიქტის მოგვარების გზა“, „სამშვიდობო მოლაპარაკებები/ინიციატ

ივები“. ნეიტრალურად: „კონფლიქტი“, „2016 წლის კონფლიქტის მიზეზები“, „მინსკის ჯგუფი“, „პროპაგანდა“, „საინფორმაციო ომი“, „ჰიბრიდული გამოწვევები“.

ცხრილი N 9. ტონალობის ანალიზი

ტონალობა	რუსთავი 2	იმედი	საზოგადოებრივი მაუწყებელი	RT
ნეგატიური	43	20	21	10
პოზიტიური	26	20	30	3
ნეიტრალური	49	52	47	5

„რუსთავი 2-ის“ სიუჟეტებში ნეგატიური ფრაზები გამოყენებული იყო 43-ჯერ, პოზიტიური 26-ჯერ, ხოლო ნეიტრალური 49-ჯერ. „იმედის“ ეთერში ნეგატიური 20-ჯერ, პოზიტიური 20-ჯერ, ნეიტრალური 52-ჯერ. „საზოგადოებრივი მაუწყებლის“ ეთერში ნეგატიური 21-ჯერ, პოზიტიური 30-ჯერ, ნეიტრალური კი 47-ჯერ. “RT-ის” შემთხვევაში კი ნეგატიური 10-ჯერ (მართალია ცეცხლის შეწყვეტა სხვა ტელევიზიებთან ჩაითვალა პოზიტიურად, თუმცა ამ შემთხვევაში “RT-ს“ ნეგატიურ კონტექსტში ჰქონდა გამოყენებული), პოზიტიური 3-ჯერ და ნეიტრალური 5-ჯერ.

მონაცემთა დაჯამების შედეგად დადასტურდა, რომ სომხეთ-აზერბაიჯანის შეიარაღებული დაპისირპირების გაშუქების ტონალობა ჩვენ მიერ შესწავლილ ქართულ მედიასაშუალებებში ნეიტრალურია (148 ნეიტრალური მესიჯი), ხოლო RT -ის შემთხვევაში - ნეგატიური (10 ნეგატიური მესიჯი).

3.5. კონფლიქტის ზონაში მომუშავე ჟურნალისტებისა და ექსპერტების სიღრმისეული ინტერვიუების ანალიზი

კითხვარი მომზადდა - „მშვიდობის გაშუქების ექვსი სავალდებულო წესი ჟურნალისტებისთვის“ - სტანდარტებზე დაყრდნობით. სიღმისეული ინტერვიუსთვის შეირჩა 8 რესპონდენტი, რომლებიც საკვლევ პერიოდში მუშაობდნენ კონფლიქტის ზონაში: დავით ქაშიაშვილი (“რუსთავი 2,” ყარაბაღის აზერბაიჯანული მხარე), დავით კაკულია (რუსთავი 2, ყარაბაღის სომხური მხარე, ჟურნალისტმა არ ისურვა ინტერვიუს ამ მიმართულებით ჩაწერა), გურამ როგავა („იმედი,“ ყარაბაღის სომხური მხარე), სოფო მთივლიშვილი („იმედი,“ ყარაბაღის სომხური მხარე), დავით ცაგარელი („იმედი“ ყარაბაღის სომხური მხარე). ასევე 3 ექსპერტი - დავით ძიძიშვილი (თავდაცვის ინსტიტუციური აღმშენებლობის სკოლის წარმომადგენელი), ზაზა ცოტნიაშვილი (კონფლიქტოლოგი), ირაკლი ალადაშვილი („კვირის პალიტრის“ სამხედრო მიმომხილველი და ჟურნალ - „არსენალის“ რედაქტორი).

სიღმისეული ინტერვიუების მომზადების დროს შემუშავდა ორი განსხვავებული კითხვარი ორი მიზნობრივი ჯგუფის წევრებისთვის. ჟურნალისტებს მივაწოდეთ შემდეგი 8 კითხვა: იცნობთ თუ არა აღნიშნულ სტანდარტებს კარგად და თუ იყენებთ მათ პრაქტიკაში? უშუალოდ ამ ომში თუ იყენებდით? იცავდით თუ არა ადგილზე

მუშაობის დროს სტანდარტებს (თუ - კი, რამდენად რთული იყო)? როგორ შეაფასებთ თქვენს მუშაობას, რა შეცდომები დაუშვით და შეიძლებოდა არ დაგეშვათ? ვინ იყო პირველწყარო? რუსული მედია წყაროდ თუ გამოგიყენებიათ? ეძებდით თუ არა მხარეებს შორის წყაროებს, რომლებიც გასცდებოდნენ მოვლენათა მარტივი ბიპოლარული ინტერპრეტირების ფარგლებს? რომელიმე მხარეს თუ უცდია თქვენი ბოროტად გამოყენება არასწორი ინფორმციის მოწოდების ან რაიმე მსგავსი მეთოდით? რატომ არ აშუქებდით აქტიურად მიმდინარე საინფორმაციო ომს?

ექსპერტებს კი დავუსვით შემდეგი 5 კითხვა: როგორ უნდა იმუშაონ ჟურნალისტებმა საინფორმაციო ომის პირობებში, რომ არ დაარღვიონ სტანდარტები და არ იქცნენ, რომელიმე მხარის იარაღად? ჰქონდა თუ არა გავლენა საინფორმაციო ომს მედიაგაშუქებაზე აღნიშნული კონფლიქტის დროს? რა სტანდარტები დაირღვა მედიაში ჟურნალისტების მიერ? იყო თუ არა საკითხის მიკერძოებული გაშუქება? თქვენი შეფასებით, რა შეიძლება იყოს მიზეზი იმისა, რომ საინფორმაციო ომი მედიასივრცეში („რუსთავი2,“ „იმედი,“ „საზოგადოებრივი მაუწყებელი,“ “RT”) საერთოდ (თუ არ ჩავთვლით „რუსთავი 2-ის“ ერთ-ერთ სიუჟეტში ერთხელ ნახსენებ ტერმინს) არ გაშუქებულა?

ჟურნალისტებიდან აღნიშნულ სტანდარტებს სრულად ან ნაწილობრივ იცნობდა ყველა ჟურნალისტი, გარდა ერთისა (დ. ცაგარელი), თუმცა, მისი თქმით, ყველა მათგანი მის მასალებში დაცული იყო.

საკუთარი მუშაობის შეფასების, დაშვებული შეცდომების შესახებ „რუსთავი 2-ის“ ჟურნალისტმა (რომელიც მუშაობდა აზერბაიჯანულ მხარეს, დ. ქაშიაშვილი) მოგვიყვა, რომ ისინი გარკვეული დროით დააკავეს და მხოლოდ მაშინ გაათავისუფლეს, როდესაც დარწმუნდნენ, რომ ეს მედიასაშუალება მათ კონფლიქტს არასწორად, არაობიექტურად არ გააშუქებდა. „იმედის“ჟურნალისტს, ს. მთივლიშვილს (მუშაობდა ყარაბაღის სომხურ მხარეს) მიაჩნია, რომ პროდიუსერმა დაუშვა დიდი შეცდომა, რადგან მას ადგილზე თემის მოკვლევისთვის ძალიან მცირე დრო ჰქონდა.

დაფიქსირდა ჟურნალისტების საკუთარი ინტერესებისთვის გამოყენების მცდელობის ფაქტიც, არასწორი ინფორმციის მიწოდებისა თუ რაიმე მსგავსი მეთოდით, „რუსთავი 2-ის“ და „იმედის“ ჟურნალისტის (სომხურ მხარეს მომუშავე) შემთხვევაში. როგორც „იმედის“ ჟურნალისტი (ს. მთივლიშვილი) აღნიშნავს, სომხური მხარე ცდილობდა, მოეხდინა ფსიქოლოგიური ზეწოლა (და არა მხოლოდ ფსიქოლოგიური) -„ჩვენი გადაადგილების ტრაექტორიის ზედმიწევნით გაგება და შეცდომაში შეყვანა სურდათ, ასევე მოინდომეს ჩვენი ნამუშევარის გადაწერა, რომ რომელიმე სომხური ტელევიზიის ეთერში გაეშვათ.“

საინფორმაციო ომის პირობებში მუშაობისთვის, ექსპერტების ინტერვიუებში შემდეგი პოზიციები გამოიხატა: ობიექტურობა, 3 დამოუკიდებელი წყაროს ცნება, კავშირი კონფლიქტში მონაწილე ქვეყნების მედიასაშუალებებთან და რედაქციასთან, ისეთი თემის გაშუქებაზე უარის თქმა, რომელშიც პასუხებზე მეტი კითხვებია (დ. ძიძიშვილი).

რაც შეეხება უშალოდ ამ ომს, ერთ-ერთი ექსპერტის, ირაკლი ალადაშვილის აზრით, საინფორმაციო ომი ქართულ მედიაზე ნაკლებად მოახდენდა გავლენას, იმიტომ, რომ ქართული მედია ამ დროს შედარებით ყველაზე ობიექტური შეიძლება ყოფილიყო.

დ. ძიძიშვილი ფიქრობს, რომ „ყველაზე ხშირად ირღვეოდა კონფლიქტის შინაარსში გარკვევის ვალდებულება, რადგან ჟურნალისტების გარკვეული ნაწილი კარგად არ იცნობდა იმ ვითარებას, რამაც გამოიწვია კონფლიქტი და მისი შემდგომი ესკალაცია. ასევე იშვიათი იყო სამართლიანი გაშუქებისა და ადამიანური მხარეების წარმოჩენის შემთხვევები. გარდა ამისა, ხშირად ვრცელდებოდა ოფიციალური სამთავრობო ინფორმაცია გადამოწმებისა და შესაბამისი ფაქტების წარმოდგენის გარეშე.“

ქართულ მედიას ორი ექსპერტი - ზ. ცოტნიაშვილი და ი. ალადაშვილი ნეიტრალურად მიიჩნევს და ახასიათებს, როგორც მხარეების ოფიციალური პოზიციების გამშუქებლებს; ზ. ცოტნიაშვილი ამბობს, რომ რომ “RT” აქტიურად არ ახორციელებდა კონფლიქტის ესკალაციას. დ. ძიძიშვილი და ი. ალადაშვილი კი ეთანხმებიან მის პროპაგანდისტულ მიზნებს, მოცემულ შემთხვევაში.

ტელეარხების მხრიდან საინფორმაციო ომის უყურადღებოდ დატოვების ფაქტზე რამდენიმე მოსაზრება გამოითქვა:

- რესურსების შესაძლო დაზოგვა (ზ. ცოტნიაშვილი);
- არა საკმარისი დრო ანალიზისა და დეტალურად გაშუქებისთვის (ი. ალადაშვილი);
- ე.წ. უფრო ცხელი ნიუსების სიმრავლე, რომელებმაც ამბავი გადაფარეს. ასევე „მედია ხშირად თავად ხდება საინფორმაციო ომის იარაღი და მისთვის მომგებიანი არ არის აღნიშნული ფაქტების გაშუქება; ამ საკითხზე საუბრისას უნდა აღინიშნოს მედიაგანათლებისა და მედიის მუშაკთა პროფესიონალიზმის როლიც. ხშირად მოუმზადებელი ჟურნალისტებისა და კონტენტზე პასუხისმგებელი პირების კომბინაცია ქმნის იმ გარემოს, სადაც საინფორმაციო ომის სპეციალისტები თავს შესანიშნავად ართმევენ მათზე დაკისრებულ მოვალეობებს, რაც ქართული მედიის კონტექსტში ყველაზე ხშირი ფაქტორია“ (დ. ძიძიშვილი).

3.6. გადაცემა - „საინფორმაციო ომი და მედია“

გარდა კვლევის ტრადიციული მეთოდებისა, გადავწყვიტეთ საინფორმაციო ომისა და მედიის კვლევის თემაზე, დამატებით, მოგვემზადებინა გადაცემა (ქრონომეტრაჟი 34 წთ და 19 წმ), სადაც კომპეტენტური პირები ისაუბრებდნენ (დავით ქუტიძე - ფაქტ-მეტრის რედაქტორი, დავით ძიძიშვილი - თავდაცვის ინსტიტუციური აღმშენებლობის სკოლის წარმომადგენელი, თამაზ ჩიქვანაია - ჟურნალისტი და საინფორმაციო სააგენტო რეპორტიორის დირექტორის მოადგილე). გადაცემაში წარმოდგენილია, როგორც საინფორმაციო ომისგან მომდინარე საფრთხეები (მათ შორის, მედიაჭრილში), ასევე განხილულია რუსული საინფორმაციო ომი და რუსული მედია, ქართულ სივრცეში. გადაცემის ინტერნეტ-მისამართი: https://www.youtube.com/watch?v=vAs32S3Dzck&t=30s.

დასკვნა

კვლევის შედეგად პირველ საკვლევ კითხვაზე, თუ რა სიხშირით შუქდებოდა მედიაში კონფლიქტი და რამდენჯერ იყო იგი დღის მთავარი თემა, მივიღეთ შემდეგი შედეგები - ყველაზე დიდი დრო „რუსთავი 2-მა," დაუთმო თემას და მოამზადა 15 მასალა; სამივე ქართული მედიის საინფორმაციო ბადის პირველ ნომრად თემა მოხვდა 4 დღის განმავლობაში 2-ჯერ. სხვა დღეებში კი თემა გადაიფარა სხვა მნიშვნელოვანი ამბებით.

მეორე საკვლევ კითხვაზე, რომელიც შეეხებოდა, ომის მიმდინარეობისას მისი გაშუქების საერთაშორისო, საყოველთაოდ აღიარებული სტანდარტებისა და ნორმების დარღვევას, მივიღეთ შემდეგი შედეგი - ტელევიზიები ნაკლებად საუბრობდნენ კონფლიქტის მოგვარების გზებზე (ქართულ მედიაში - „რუსთავი 2" უფრო საუბრობს ვიდრე სხვები; "RT"- საერთოდ არ საუბრობს). ისინი ძირითადად ფაქტების მიმოხილვით და მხარეების ოფიციალური (სომხეთისა და აზერბაიჯანის) პოზიციების გაშუქებით შემოიფარგლებოდნენ (ქართული მედია). ამასთან, ე.წ. მთიანი ყარაბაღის პოზიცია უფრო მცირე რაოდენობით იყო წარმოდგენილი. უნდა აღვნიშნოთ „იმედის" 2 აპრილისა და 31 დეკემბრის გადაცემები, სადაც ძირითადად აზერბაიჯანული პოზიცია იყო გაშუქებული, რასაც, ამ შემთხვევაში, ვერ ვიტყვით "RT-ზე," აქ „სამივე" მხარე დაბალანსებული იყო (წარმოდგენილი სტანდარტებიდან მხოლოდ ამ სტანდარტს აკმაყოფილებს რუსული მედიის მიერ მომზადებული მასალები). ადამიანური ისტორიები ყველაზე დიდი რაოდენობით „რუსთავი 2-მა" წარმოადგინა, ყველაზე მცირე რაოდენობით კი - „საზოგადოებრივმა მაუწყებელმა." სამშვიდობო ინიციატივებს კი თითქმის ყოველდღე ყველა მედიასაშუალება აშუქებდა გარდა "RT"-სა, რომელიც საუბრობდა მხოლოდ კონფლიქტის გამწვავებაზე. მაშინაც კი, როდესაც

ყველა მედიამ ცეცხლის შეწყვეტის შესახებ განაცხადა, ამ უკანასკნელმა ზედაპირულად მოიხსენია შეტაკებების შეწყვეტა, თუმცა იქვე დაამატა, რომ საარტილერიო დარტყმები ისევ მიმდინარეობდა. „RT“-მ სიტუაცია შეაფასა, როგორც კრიზისის, ფართომასშტაბიან საომარ კონფლიქტში გადაზარდის საფრთხის მქონედ.

ხომ არ ექცეოდნენ გავლენის ქვეშ ჟურნალიტები უშუალოდ ადგილზე მუშობის დროს?- ამ კითხვაზე შევეცადეთ ძირითადად სიღრმისეული ინტერვიუებით გაგვეცა პასუხი, რის შედეგადაც ყველა შემთხვევაში უარყოფითი პასუხი მივიღეთ. ზოგადი დაკვირვების შედეგადაც ეს დადასტურდა.

წარმოდგენილ საკვლევ პერიოდში ყველა ტელევიზიას, გარდა „საზოგადოებრივი მაუწყებლისა“ ადგილზე ჰყავდათ საკუთარი კორესპონდენტი, რომლებიც მრავალფეროვან წყაროებს იყენებდნენ.

საქართველოსთვის არსებული საფრთხეებზე „საზოგადოებრივმა მაუწყებელმა“ ყველაზე დიდი რაოდენობით იმსჯელა. აქვე უნდა აღვნიშნოთ წლის შემაჯამებელი გადაცემაც, სადაც საკითხი მხოლოდ „იმედის“ მიმოხილვაში მოხვდა.

რაც შეეხება კითხვას, საინფორმაციო ომისა გაშუქების შესახებ - დაკვრვების შედეგად ვნახეთ, რომ არცერთმა ტელევიზიამ, საკვლევი პერიოდის განმავლობაში არ გააშუქა აქტიურად მიმდინარე საინფორმაციო ომი, რისი მიზეზიც შესაძლოა ქვეყანაში მიმდინარე „ცხელი“ პოლიტიკური ამბები ანდა ჟურნალისტებისთვის სამუშაოდ მიცემული დროის სიმცირე იყო. საინფორმაციო ომი მხოლოდ ერთხელ ახსენეს „რუსთავი 2-ის“ ერთ-ერთ სიუჟეტში, თუმცა შეგვხვდა მასთან დაკავშირებული რამდენიმე სხვა ტერმინი: პროპაგნდა (რუსეთზე საუბრისას ახსენა „რუსთავი 2-ში“ მიწვეულმა სტუმარმა); ჰიბრიდული გამოწვევები („იმედში“ ერთხელ გაჟღერდა). ხოლო ურთიერთსაპირისპირო მონაცემების/ინფორმაციის გავრცელება, რომელიც საინფორმაციო ომის ერთ-ერთი ნაწილია ჯამში 19-ჯერ გაჟღერდა.

მონიტორინგის შედეგად ჩვენი ჰიპოთეზა - მედიასაშუალებები, საინფორმაციო ომის მიმდინარეობისას, ექცეოდნენ გარკვეული ძალების ზეგავლენის ქვეშ და არღვევდნენ ომის გაშუქების სტანდარტებს - დადასტურდა „RT-ის“ შემთხვევაში, რომლის მედიაგაშუქებაც საერთო სურათისა და ანალიზის მიხედვით ნეგატიური მაჩვენებლისაა. ხოლო ქართული მედიის შემთხვევაში, საქმე გვაქვს არა საინფორმაციო ომის ზეგავლენასთან, არამედ საკითხის არც თუ ისე სიღრმისეულად გაშუქებასთან (თუ არ ჩავთვლით საქართველოსთვის არსებული საფრთხეებზე მსჯელობას), რადგან ფოკუსირება ძირითადად ფაქტების აღწერასა და მხარეების ოფიციალური პოზიციების გაჟღერებაზე იყო გადატანილი. ქართული მედია დროს უთმობდა - საბრძოლო

მოქმედებებს, ადამიანურ ისტორიებს, საქართველოსთვის შესაძლო საფრთხეების გაშუქებას, აქტიურად მიმდინარე საიფორმაციო ომს კი უყურადღებოდ ტოვებდა .

ბიბლიოგრაფია:

1. სუნ-ძი (2016), ომის ხელოვნება, თბილისი: „თეკა&კომპანია“;
2. Weerakkody, N. (2009), Research Methods for Media and Communication, რიდერი (თარგმანი: ნინო მაჭარაშვილი, ეკატერინე ბასილაია; რედაქტირება და კორექტურა: მარი წერეთელი);
3. მიქელსონი, დ., გრიფინი, ტ.,ლ. (2005), „კონტენტ ანალიზის ახალი მეთოდი,“ რიდერი (თარგმანი გერსამია მ.);
4. კაპელა და ჯეიმსონი, 1997, 39 გვ.;
5. ძიძიშვილი, დ. (2015), საინფორმაციო ომი, როგორც საზოგადოებრივი აზრის ფორმირების ფაქტორი, სამაგისტრო ნაშრომი, ილიას სახ. უნივერსიტეტი, თბილისი;
6. Cyber House (2016), ყარაბახის ინფორმაციული და კიბერ ომი, http://bit.ly/2AXVwAu (ბოლო წვდომის თარიღი 26 თებერვალი, 2018);
7. ნამჩავაძე, ბ. (2016), ომი, რომელიც გვეხება, http://forbes.ge/news/1371/omi%2C-romelic-gvexeba (ბოლო წვდომის თარიღი 26 თებერვალი, 2018);
8. გირაგოსიანი, რ. (2017), ომი მთიან ყარაბაღში: რას შეიძლება ნიშნავდეს ის საქართველოსთვის? http://bit.ly/2HMJC11 (ბოლო წვდომის თარიღი 26 თებერვალი, 2018);
9. გოგოლაძე, ლ. (2016), "სომხეთის და აზერბაიჯანის დაპირისპირება შესაძლოა სამხრეთ კავკასიის დიდ ომში გადაიზარდოს," https://www.kvirispalitra.ge/politic/29157-qsomkhethis-da-azerbaijanis-dapirispireba-shesadzloa-samkhreth-kavkasiis-did-omshi-gadaizardosq.html (ბოლო წვდომის თარიღი 26 თებერვალი, 2018);

10. გადაცემა განთიადი, ერთსულოვნება (2016), მთიანი ყარაბაღის კონფლიქტი და საქართველო, https://www.youtube.com/watch?v=NVwGzTDd8UA (ბოლო წვდომის თარიღი 26 მარტი, 2018);
11. მოსახლეობის 2014 წლის საყოველთაო აღწერის ძირითადი მონაცემები, http://census.ge/ge/mosakhleobis-2014-tslis-sakoveltao-aghtseris-dziritadi-shedegebi-zogadi-informatsia/201#.WyAfeoozbIW (ბოლო წვდომის თარიღი 12 ივნისი, 2018);
12. ვიკიპედია, Collective Security Treaty Organization, https://en.wikipedia.org/wiki/Collective_Security_Treaty_Organization (ბოლო წვდომის თარიღი 12 ივნისი, 2018);
13. Stein, G. J. (1995), Information Warfare, https://www.scribd.com/document/129280540/Information-Warfare-by-Prof-George-J-Stein (ბოლო წვდომის თარიღი 6 თებერვალი, 2018);
14. ALBERTS, D.S. (1996), Defensive Information Warfare, http://www.dodccrp.org/files/Alberts_Defensive.pdf (ბოლო წვდომის თარიღი 5 თებერვალი, 2018);
15. Alberts, D.S., Garstka, J.J., Hayes, R.E., Signori, D.A. (2001), Understanding Information Age Warfare, http://www.dtic.mil/dtic/tr/fulltext/u2/a395859.pdf (ბოლო წვდომის თარიღი 6 თებერვალი, 2018);
16. Porche, I.R., Paul, C., York, M., Serena, C.C., Sollinger, J.M., Axelband, E., Min, E.Y., Held, B.J. (2013), REDEFINING INFORMATION WARFARE BOUNDARIES FOR AN ARMY IN A WIRELESS WORLD, https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf (ბოლო წვდომის თარიღი 6 თებერვალი, 2018) ;
17. Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012), The Law of Cyber-Attack, California Law Review, Vol. 100, No. 4,pp. 817-885, http://www.jstor.org.lez.tsu.edu.ge:2048/stable/pdf/23249823.pdf?refreqid=excelsior:7eb9dd3b5a9530b77e2eb94c661a6a0a (ბოლო წვდომის თარიღი 7 თებერვალი, 2018);
18. ოქსფორდის ლექსიკონი, https://en.oxforddictionaries.com/definition/information_war (ბოლო წვდომის თარიღი 15 თებერვალი, 2018);

19. Molander, R.C., Riddile, A.S., Wilson, P. A., Strategic Information Warfare: A New Face of War, https://www.rand.org/pubs/monograph_reports/MR661/index2.html (ბოლო წვდომის თარიღი 14 თებერვალი, 2018);
20. Tylor, A. (2001), Fighting the Information War, Fortnight, No. 391 pp. 12-13, http://www.jstor.org.lez.tsu.edu.ge:2048/stable/pdf/25560135.pdf (ბოლო წვდომის თარიღი 14 თებერვალი, 2018);
21. Gjelten, T. (1998) Professionalism in War Reporting: A Correspondent's View, https://www.carnegie.org/media/filer_public/40/53/40532590-122f-4a48-a470-5c4a2b793c48/ccny_report_1998_ correspondent.pdf (მითითებულია შემდეგ წყაროში - http://www.kas.de/wf/doc/kas_47078-1522-1-30.pdf?161118091728), (ბოლო წვდომის თარიღი 20 თებერვალი, 2018);
22. Elida, K., Jacobsen, U. (2007), Reviewed Work(s): Journalists under Fire: Information War and Journalistic Practice by Howard Tumber and Frank Webster, Journal of Peace Research, Vol. 44, No. 5, p. 641, http://www.jstor.org.lez.tsu.edu.ge:2048/stable/pdf/27640587.pdf?refreqid=excelsior%3A00b7d72cd8bb3da3715146d0bb1d6c04 (ბოლო წვდომის თარიღი 20 თებერვალი, 2018);
23. Rohn, A. (2014), Media Role in The Vietnam War, https://thevietnamwar.info/media-role-vietnam-war/ (ბოლო წვდომის თარიღი 15 მარტი, 2018);
24. Neumann, R., Fahmy, S. (2016), Measuring journalistic peace/war performance: An exploratory study of crisis reporters' attitudes and perceptions , the International Communication Gazette , Vol. 78(3) 223–246, http://journals.sagepub.com.lez.tsu.edu.ge:2048/doi/pdf/10.1177/1748048516630715 (ბოლო წვდომის თარიღი 20 თებერვალი, 2018);
25. ომისა და მშვიდობის გაშუქების ინსტიტუტი (1999), მშვიდობის გაშუქების ექვსი სავალდებულო წესი ჟურნალისტებისთვის, http://reporter.ge/mshvidobis-gashuqebis-eqvsi-savaldebulo-tsesi-zhurnalistebisthvis/ (ბოლო წვდომის თარიღი 12 ივნისი, 2018);
26. ჟენევის 1949 წლის 12 აგვისტოს კონვენციები და მათი დამატებითი ოქმები, https://bit.ly/2CQfwpN (ბოლო წვდომის თარიღი 12 ივნისი, 2018);
27. გადახაბაძე, ე. (2016), შეტაკებები გრძელდება - ყარაბაღის ომის ისტორია, სომხეთისა და აზერბაიჯანის ჯარების შესაძლებლობები და ირანის მუქარა,

https://www.kvirispalitra.ge/msoflio/29198-shetakebebi-grdzeldeba-yarabaghis-omis-istoria-somkhethisa-da-azerbaijanis-jarebis-shesadzleblobebi-da-iranis-muqara.htm (ბოლო წვდომის თარიღი 11 მარტი, 2018);

28. გაბიევი, ხ. (2003), მთიანი ყარაბაღი როგორც გაყინული კონფლიქტების მაგალითი, ჟურნალი ახალი აზრი 2003, N 11, https://bit.ly/2HkXWwL (ბოლო წვდომის თარიღი 11 მარტი, 2018);
29. ეუთო, Who we are, https://www.osce.org/minsk-group/108306 (ბოლო წვდომის თარიღი 28 ივნისი, 2018);
30. Broers, L. (2016), The Nagorny Karabakh Conflict Defaulting to War, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/NK%20paper%2024082016%20WEB.pdf (ბოლო წვდომის თარიღი 13 მარტი, 2018);
31. Global Conflict Tracker (2017), Nagorno-Karabakh Conflict, www.cfr.org/interactives/global-conflict-tracker#!/conflict/nagorno-karabakh-conflict (ბოლო წვდომის თარიღი 13 მარტი, 2018);
32. აჰმედბეილი, ს., კარაპეტიანი, ა. (2016), ყარაბაღის კონფლიქტის ირგვლივ მღელვარება არ იკლებს, http://bit.ly/2FzJjco (ბოლო წვდომის თარიღი 13 მარტი, 2018);
33. კომახია მ. (2016), სომხეთ-აზერბაიჯანის „ოთხდღიანი“ ომი: ვინ წააგო და ვინ მოიგო, https://www.gfsis.org/files/library/opinion-papers/73-expert-opinion-geo.pdf (ბოლო წვდომის თარიღი 13 მარტი, 2018);
34. TUNCEL, T. K. (2016), A SHORT ASSESSMENT OF THE “4-DAY WAR” IN KARABAKH, http://avim.org.tr/en/Yorum/A-SHORT-ASSESSMENT-OF-THE-4-DAY-WAR-IN-KARABAKH (ბოლო წვდომის თარიღი 14 მარტი, 2018);
35. Ingilizian, M. (2016), Azerbaijan’s Incremental Increase On The Nagoro Karabakh Trontline, https://www.bellingcat.com/news/rest-of-world/2016/04/12/detailing-azerbaijans-incremental-increase-in-nagorno-karabaghs-frontline/#_edn1 (ბოლო წვდომის თარიღი 14 მარტი, 2018);
36. Yin, R.K. (1994) ,Case Study Researh - Design and Methods (Second Edition), http://www.madeira-edu.pt/LinkClick.aspx?fileticket=Fgm4GJWVTRs%3D&tabid=3004 (ბოლო წვდომის თარიღი 12 ივნისი, 2018);

37. სამოქალაქო განათლების ლექსიკონი, http://www.nplg.gov.ge/gwdict/index.php?a=term&d=6&t=3606 (ბოლო წვდომის თარიღი 13 ივნისი, 2018);
38. კიბერ სივრცის სამართალი, ტერმინთა განმარტება, http://ilawge.blogspot.com/p/blog-page_11.html (ბოლო წვდომის თარიღი 13 ივნისი, 2018);
39. საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“ (2012), https://bit.ly/2y5FW9F (ბოლო წვდომის თარიღი 13 ივნისი, 2018);
40. ავალიშვილი, ლ., ლომთაძე, გ., ქევხიშვილი, ს. (2016), კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა , https://bit.ly/2jP3t42 (ბოლო წვდომის თარიღი 13 ივნისი, 2018);
41. კვირის პალიტრა (2015), ჰიბრიდული ომი და საქართველო, https://www.kvirispalitra.ge/politic/24177-hibriduli-omi-da-saqarthvelo.html (ბოლო წვდომის თარიღი 13 ივნისი, 2018);
42. ლექსიკონი Collins, https://www.collinsdictionary.com/dictionary/english/hybrid-warfare (ბოლო წვდომის თარიღი 13 ივნისი, 2018);
43. Business Media Georgia (2018), TVMR: 2017 წლის ყველაზე რეიტინგული ტელევიზიები, http://www.bm.ge/ka/article/tvmr-2017-wlis-yvelaze-reitinguli-televiziebi/16418 (ბოლო წვდომის თარიღი 13 ივნისი, 2018);

გაანალიზებული ვიდეოები:

44. https://www.youtube.com/watch?v=7WINmzgPR6Y (ბოლო წვდომის თარიღი 11 მარტი, 2018);
45. https://www.youtube.com/watch?v=58B-ogcyzZU (ბოლო წვდომის თარიღი 11 მარტი, 2018);
46. https://www.youtube.com/watch?v=6rpyxoxdmlI (ბოლო წვდომის თარიღი 11 მარტი, 2018);
47. https://www.youtube.com/watch?v=QrFDTLPruIE (ბოლო წვდომის თარიღი 11 მარტი, 2018);

48. https://www.youtube.com/watch?v=otsWV84rJiU (ბოლო წვდომის თარიღი 11 მარტი, 2018);
49. https://www.youtube.com/watch?v=M9CM3Q45vvk (ბოლო წვდომის თარიღი 11 მარტი, 2018);
50. https://www.youtube.com/watch?v=j3-wJUHtb6s (ბოლო წვდომის თარიღი 11 მარტი, 2018);
51. https://www.youtube.com/watch?v=D7hq_bJ5sFU (ბოლო წვდომის თარიღი 11 მარტი, 2018);
52. https://www.youtube.com/watch?v=7WINmzgPR6Y (ბოლო წვდომის თარიღი 11 მარტი, 2018);
53. http://rustavi2.ge/ka/video/14258?v=2 (ბოლო წვდომის თარიღი 11 მარტი, 2018);
54. http://rustavi2.ge/ka/video/21672?v=2 (ბოლო წვდომის თარიღი 11 მარტი, 2018);
55. http://rustavi2.ge/ka/video/14323?v=2 (ბოლო წვდომის თარიღი 11 მარტი, 2018);
56. http://rustavi2.ge/ka/video/14283?v=2 (ბოლო წვდომის თარიღი 11 მარტი, 2018);
57. http://rustavi2.ge/ka/video/14227?v=2 (ბოლო წვდომის თარიღი 11 მარტი, 2018);
58. http://rustavi2.ge/ka/video/14229?v=2 (ბოლო წვდომის თარიღი 11 მარტი, 2018);
59. https://www.youtube.com/watch?v=S14etZJbsJs (ბოლო წვდომის თარიღი 11 მარტი, 2018);
60. https://www.youtube.com/watch?v=E1QfmVNuW3g (ბოლო წვდომის თარიღი 11 მარტი, 2018);
61. https://www.youtube.com/watch?v=z57AePQ9M4w (ბოლო წვდომის თარიღი 11 მარტი, 2018);
62. https://www.youtube.com/watch?v=YseJRQtL7Kg (ბოლო წვდომის თარიღი 11 მარტი, 2018);
63. https://www.youtube.com/watch?v=p3hmgMiTgr8 (ბოლო წვდომის თარიღი 11 მარტი, 2018);
64. https://www.imedi.ge/ge/video/8498/qronika-8-saatze--4-aprili-2016-tseli (ბოლო წვდომის თარიღი 11 მარტი, 2018);
65. https://www.imedi.ge/ge/video/8504/qronika-8-saatze--5-aprili-2016-tseli (ბოლო წვდომის თარიღი 11 მარტი, 2018);

66. https://www.youtube.com/watch?v=K89AnlsogQQ (ბოლო წვდომის თარიღი 11 მარტი, 2018);
67. ტელეკომპანია „იმედი“ (02.04.2016), საინფორმაციო გამოშვება-ქრონიკა, თბილისი, (მოპოვებულია „იმედის“ არქივში);
68. ტელეკომპანია „იმედი“ (03.04.2016), საინფორმაციო გამოშვება-ქრონიკა, თბილისი, (მოპოვებულია „იმედის“ არქივში);
69. ტელეკომპანია „იმედი“ (31.12.2016), საინფორმაციო გამოშვება-ქრონიკა, თბილისი, (მოპოვებულია „იმედის“ არქივში);
70. აფციაური, ე. (2018), კვლევის ფარგლებში ჩაწერილი გადაცემა - „საინფორმაციო ომი და მედია,“ თბილისი, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, https://www.youtube.com/watch?v=vAs32S3Dzck&t=30s.

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 40-50 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

BLOWFISH და RSA კრიპტოსისტემების ჰიბრიდული მოდელი

ელზა ჯინჭარაძე
საქართველოს ტექნიკური უნივერსიტეტი

აბსტრაქტი. მოცემულ ნაშრომში განხილულია შიფრაციის ცნობილი ორი ალგორითმის RSA (ასიმეტრიული შიფირაციის ალგორითმი) და Blowfish (სიმეტრიული შიფრაციის ალგორითმი) პროგრამული კოდის რეალიზაცია Java პროგრამირების ენის ბაზაზე. ჩატარებული კვლევების საფუძველზე მიღებული შედეგების გათვალისწინებით შექმნილია ჰიბრიდული კრიპტოსისტემის მოდელი, რომელიც ითვალისწინებს RSA და Blowfish სისტემის კომბინაციას და მათი, როგორც ერთი ჰიბრიდული მოდელის პროგრამულ რეალიზაციას.

JAVA პროგრამირების ენაში რეალიზებული პროგრამული პროდუქტის საშუალებით ჩატარებულია ცდები აღნიშნული ალგორითმებისა და მათი კომბინაციით შექმნილი ალგორითმის ეფექტურობაზე, რაც ითვალისწინებს ალგორითმის უსაფრთხოების დონის პარამეტრებს, ალგორითმის დამუშავების დროს, დეშიფრაცია / შიფრაციის დროს და ალგორითმის მიმდინარეობის პროცესში კომპიუტერული რესურსების გამოყენების მახასიათებლებს.

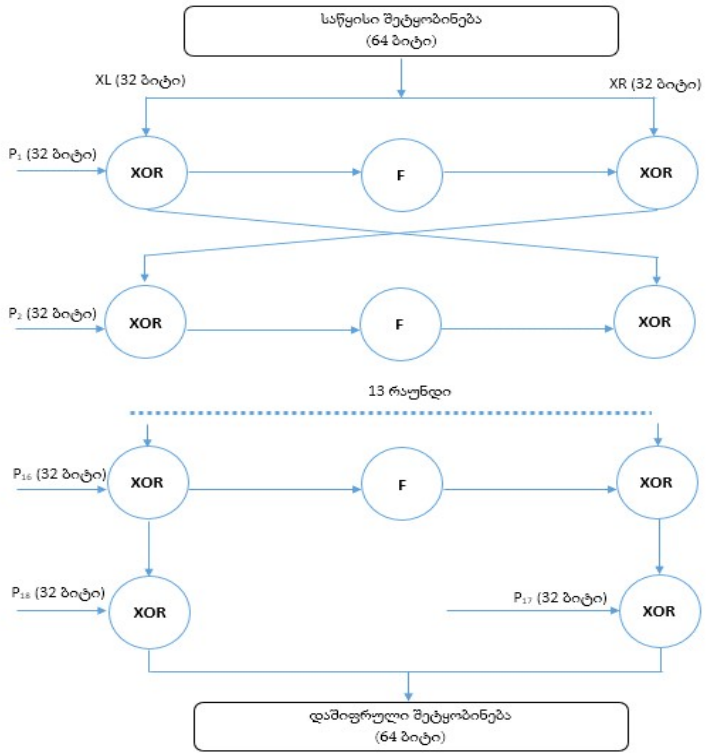
ასიმეტრიული შიფრაციის ალგორითმების ზოგადი მიმოხილვა RSA კრიპტოგრაფიული ალგორითმის მაგალითზე

ალგორითმი Rivest Shamir Adleman ანუ RSA — კრიპტოგრაფიის ასიმეტრიული ალგორითმი (public სიტყვა-გასაღები), მნიშვნელოვან გამოყენებას ჰპოვებს ელექტრონულ კომერციაში, განსაკუთრებით საიდუმლო მონაცემების გაცვლა-გამოცვლისათვის ინტერნეტში [1,2]. კრიპტოსისტემა RSA წარმოადგენს ღია გასაღებიან ალგორითმს, რომელიც შეიძლება გამოყენებული იქნას როგორც ინფორმაციის დასაშიფრად, ასევე ციფრული ხელმოწერის შესაქმნელად. ალგორითმში ღია და საიდუმლო გასაღებებს შორის დამოკიდებულება მოცემულია ცალმხრივი ფუნქციის საშუალებით. ალგორითმი იყენებს ორი ტიპის სიტყვა-გასაღებს: public, ტექსტის დასაშიფრად და private დაშიფრული ტექსტის გასაშიფრად. public სიტყვა-გასაღები ხელმისაწვდომია ყველასთვის ვინც შიფრავს ინფორმაციას, private კი ხელმისაწვდომია მხოლოდ მისთვის ვინც შექმნა ორივე სიტყვა-გასაღები.

RSA კრიპტოგრაფიული ალგორითმის *უარყოფითი* მხარეა მისი შიფრაციის სიჩქარე. ამ ალგორითმის შიფრაციის პროცესი მოითხოვს საკმაოდ დიდ დროს. ასევე, როგორც სხვა ასიმეტრიული ალგორითმების მსგავსად მთავარ უარყოფით მხარეს წარმოადგენს შიფრაციის პროცესში ორი გასაღების გამოყენების ფაქტი. რა თქმა უნდა RSA გვთავაზობს უსაფრთხოების მაღალ დონეს, მაგრამ ამავდროულად არის საკმაოდ ნელი.

სიმეტრიული შიფრაციის ალგორითმების ზოგადი მიმოხილვა Blowfish ალგორითმის მაგალითზე

Blowfish წარმოადგენს სიმეტრიული შიფრაცია/დეშიფრაციის კრიპტოგრაფიულ ალგორითმს. მონაცემთა შიფრაციის ფუნქცია საკმაოდ მარტივია. იგი მიმდევრობით 16-ჯერ წარმატებით გამოიყენება ისეთ აპლიკაციებში, სადაც გასაღების სიგრძე პერიოდულად არ იცვლება. ითვლება, რომ არსებულ შიფრაციის ალგორითმებთან შედარებით Blowfish არის უფრო სწრაფი 32 ბიტიან მიკროპროცესორზე შესრულების დროს.



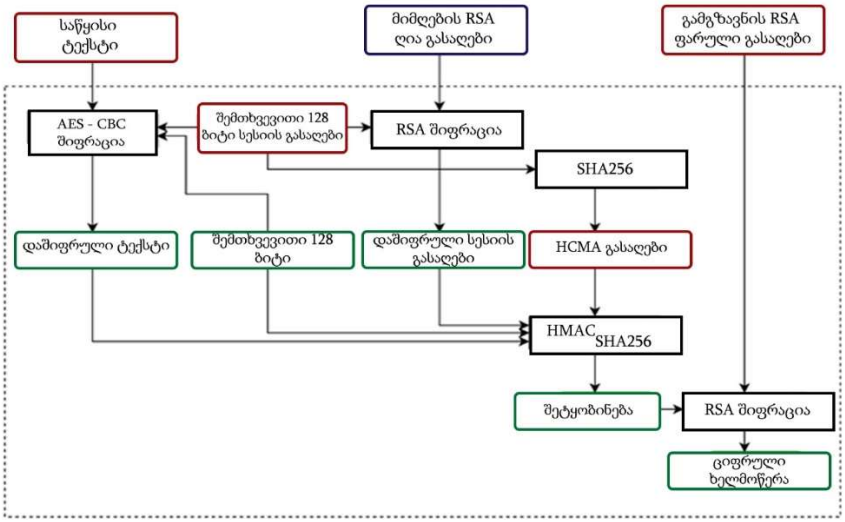
სურათი 1. Blowfish ალგორითმის სტრუქტურა

ამ დროისთვის Blowfish გვთავაზობს შედარებით უფრო მაღალი დონის შიფრაციას, რადგან ჯერჯერობით მასზე განხორციელებული არც ერთი შეტევა არ დასრულებულა წარმატებით. Blowfish არის უფრო სწრაფი ვიდრე DES. თუმცა ამ ალგორითმის სუსტი წერტილია შიფრაციის სუსტი გასაღები.

ჰიბრიდული კრიპტოსისტემების მიმოხილვა

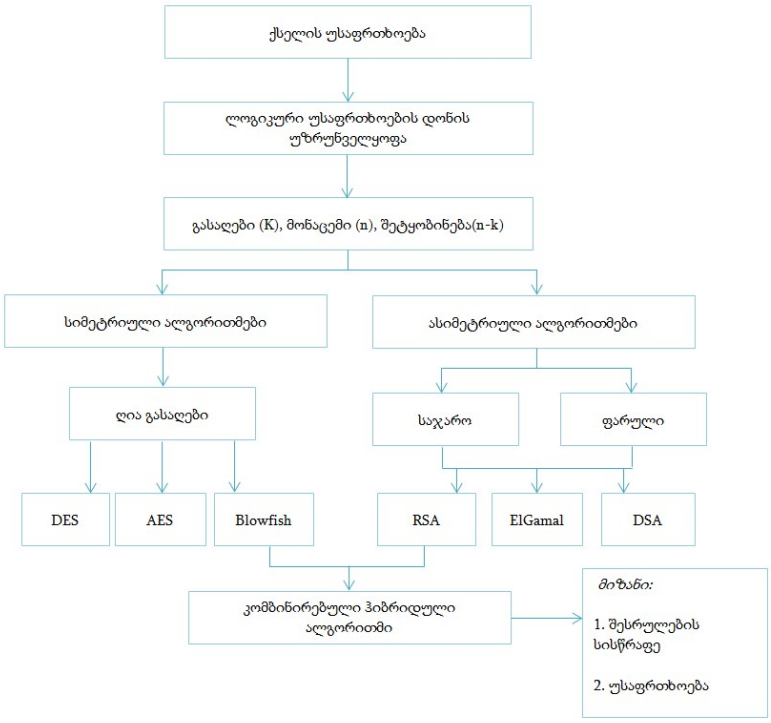
კრიპტოგრაფიაში ჰიბრიდული კრიპოსისტემად ზოგადად მოიხსენიება სისტემა, რომელიც წარმოადგენს ასიმეტრიული და სიმეტრიული შიფრაციის ალგორითმების კომბინაციას [30]. ღია გასაღების კრიპტოსისტემები დაფუძნებულია რთული პრობლემების გამოთვლით სირთულეზე. მაგალითად RSA ემყარება რიცხვის ფაქტორიზაციის პრობლემას (ანუ დიდი რიცხვის დაშლას მარტივ მამრავლებად), ხოლო დიფი-ჰელმანის ალგორითმი ეფუძნება

დისკრეტული ლოგარითმების პრობლემას. მსგავსი სისტემების შემთხვევაში უპირატესობა ენიჭება მოდულით გამრავლების და ახარისხების ოპერაციებს, შესაბამისად გაცილებით მეტი გამოთვლითი სიმძლავრეა საჭირო, ვიდრე სიმეტრიულ სისტემებში. ამიტომ ღია გასაღების კრიპტოსისტემები ძირითადად გამოიყენება, როგორც ჰიბრიდული სისტემები, სადაც ინფორმაციის შიფრაცია/დეშიფრაციისათვის გამოიყენება სწრაფი სიმეტრიული ალგორითმები, ხოლო მისი გასაღების მართვისა და გადაცემისათვის გამოიყენება შედარებით ნელი ასიმეტრიული ალგორითმები.



***სურათი 2**. RSA & AES ჰიბრიდული სქემის მოდელი*

როგორც აღვნიშნეთ, სიმეტრიულ და ასიმეტრიულ ალგორითმებს გააჩნია თავისი დადებითი და უარყოფითი მხარეები. სიმეტრიული ალგორითმების სისტემები არიან საკმაოდ სწრაფი, ვიდრე ასიმეტრიული სისტემები, თუმცა მოითხოვს რომ ფარული გასაღები დაცულად იქნეს გადაცემული შიფრაციის სქემის მეორე მხარისთვის. ხოლო ასიმეტრიული სისტემები უზრუნველყოს ღია გასაღების გაცვლას და საიდუმლო გასაღების უსაფრთხოების დაცვას, თუმცა ეს ხდება სისწრაფის ხარჯზე. სწორედ, ამ პრობლემების აღმოფხვრის მიზნით გამოიყენება ჰიბრიდული ალგორითმები, რაც გულისხმობს შიფრაციის პროცესში სხვადასხვა ტიპის ალგორითმების გამოყენებას.



სურათი 3. ჰიბრიდული კრიპტოსისტემის ზოგადი სქემა

ჰიბრიდული კრიპტოგრაფიული სისტემის ზოგადი იდეა მდგომარეობს იმაში, რომ მოვახდინოთ შემთხვევითი გასაღების გენერირება სიმეტრიული შიფრაციისთვის, ხოლო შემდეგ მოვახდინოთ ამ გასაღების შიფრაცია ასიმეტრიული სისტემისათვის. შემდეგ მიღებული საიდუმლო გასაღებით ხდება საწყისი შეტყობინების შიფრაცია. დეშიფრაციის დროს ხდება შეტყობინების დაშიფვრა საკუთარი საიდუმლო გასაღებით, ხოლო შემდეგ გამოყენება საჯარო გასაღები [31].

Blowfish და RSA ალგორითმების პროგრამული რეალიზაცია და ექსპერიმენტული კვლევის შედეგები

Blowfish და RSA კრიპტოსისტემებზე პროგრამული ექსპერიმენტების ჩატარების, მაქსიმალური გამოყენების დროის, გამოყენებული მეხსიერების შედეგების კვლევის მიზნით შეიქმნა მოცემული სისტემების ალგორითმების პროგრამული რეალიზაცია. ამ მიზნით გამოყენებული JAVA ობიექტზე ორიენტირებული პროგრამირების ენა. თუმცა გამოთვლების სტატისტიკური შედეგების სიზუსტის მიზნით გამოყენებულია არა ვიზუალური ინტერფეისი, არამედ პროგრამასთან კონსოლური მუშაობის რეჟიმი.

ზოგადად შიფრაციის სრული დრო უმთავრესად დამოკიდებულია კონკრეტული ალგორითმის სტრუქტურულ მახასიათებლებზე. ცხრილ 1-ში მოცემულია სხვადასხვა ზომის დასაშიფრი ტექსტზე ჩატარებული შიფრაციისა და დეშიფრაციის ოპერაციები AES

კრიპტოსისტემის გამოყენებით. აქვე უნდა გავითვალისწინოთ, რომ შიფრაციის დროს გამოყენებული გასაღების ზომაა 16 ბიტი.

Blowfish შიფრაცია					
დასაშიფრი ტექსტის ზომა (კილობაიტი)	დასაშიფრი ტექსტის ზომა (ბაიტი)	გასაღების ზომა (ბიტი)	შიფრაციის დრო (ნანოწამი)	დაშიფრული ტექსტის ზომა (ბაიტი)	დეშიფრაციის დრო (ნანოწამი)
32	32710	16	10753053	59241	1984528
64	65420	16	12169867	119493	2743007
128	130840	16	12567266	236670	5602025
256	261680	16	18200673	475738	9356337
512	523360	16	23987822	954280	16802548
1024	1048460	16	35550482	1915678	26062972
2048	2096920	16	43489299	3804367	40463494
4096	4193840	16	62097598	7552059	56950097

ცხრილი 1. Blowfish შიფრაციის სტატისტიკური მაჩვენებლები

მსგავსი სახის ექსპერიმენტი ჩატარდა ასევე **RSA** კრიპტოსისტემაზე, სადაც სხვადასხვა ზომის ფაილების შიფრაციისა და დეშიფრაციის პროცესზე დახარჯული დროის დაკვირვების შედეგად შედეგად მივიღეთ შემდეგი მონაცემები (ცხრილი 2):

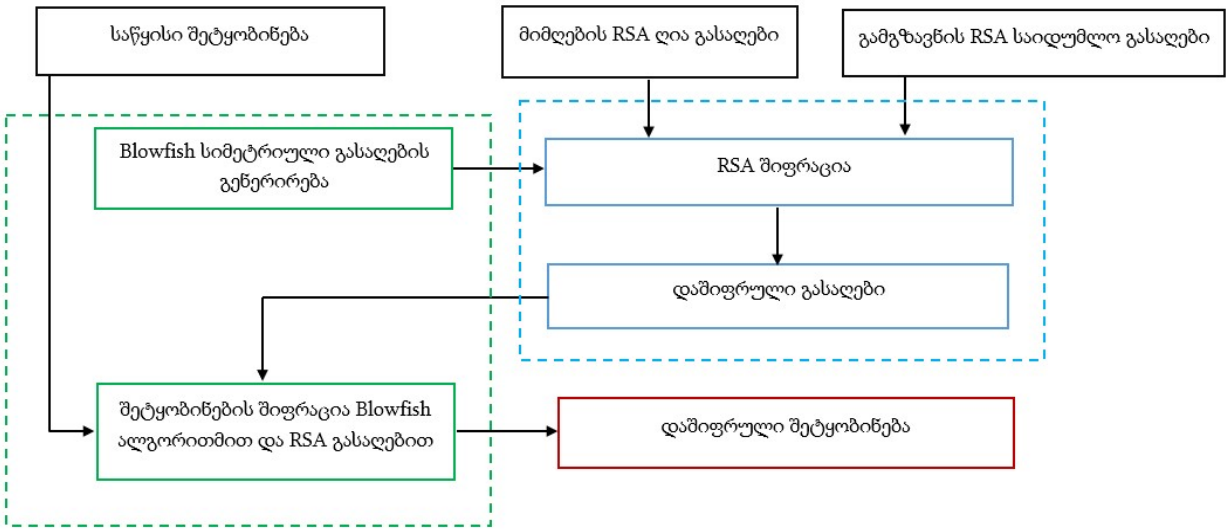
RSA შიფრაცია				
ფაილის ზომა (KB)	საწყისი ფაილის ზომა (Byte)	შიფრაციის დრო (ნანოწამი)	დაშიფრული ტექსტის ზომა	დეშიფრაციის დრო (ნანოწამი)
32	32710	1536637771	118780	55542452
64	65420	3208498484	237689	121344997
128	130840	6149709140	474654	284935252
256	261680	10574937240	946614	671696785
512	523360	20368096461	1896331	1991097468
1024	1048460	41504791208	3795983	6934459468
2048	2096920	89946149790	7586016	27974097086
4096	4193840	181620236481	15179673	121238321204

ცხრილი 2. RSA შიფრაციის სტატისტიკური მაჩვენებლები

Blowfish + RSA სიმეტრიული და ასიმეტრიული კრიპტოსისტემების შედეგად შექმნილი ჰიბრიდული სისტემა

განვიხილოთ ჰიბრიდული კრიპტოსისტემა, რომელიც ზემოთ განხილული Blowfish და RSA კრიპტოსისტემების კომბინაციის საფუძველზე არის შექმნილი. ამ სისტემის იდეა მდგომარეობს შემდეგში. მოცემული სქემის საწყის ეტაპზე ხდება საწყისი ფაილის წაკითხვა. ამავდროულად ხდება RSA ალგორითმის საიდუმლო და ღია გასაღებების ავტომატური გენერირება.

მოცემული სქემის შემდეგ ეტაპზე ავტომატურად გენერირედება Blowfish სიმეტრიული გასაღები, ხოლო მიღებული გასაღები იშიფრება RSA ალგორითმის საშუალებით. აღნიშნული სქემა უზრუნველყოფს Blowfish სისტემის საჯარო გასაღების უსაფრთხოების მაღალ დონეს. RSA ალგორითმის უსაფრთხოების მაჩვენებელი ამცირებს საჯარო გასაღების დეშიფრაციის რისკებს. შესაბამისად ღია გასაღების გაცვლასთან ერთად მოხდება RSA ალგორითმის საიდუმლო გასაღების გაცვლაც. მოცემულ ჰიბრიდულ მოდელში შიფრაციის პროცესი მიმდინარეობს Blowfish ალგორითმის შიფრაციული ალგორითმით, ვინაიდან Blowfish არის მნიშვნელოვნად სწრაფი, ვიდრე RSA ალგორითმი. შესაბამისად, დეშიფრაციის პროცესი შესრულდება შებრუნებული თანმიმდევრობით.



სურათი 3. *RSA + Blowfish კრიპტოსისტემების კომბინაციით მიღებული ჰიბრიდული კრიპოსისტემის ზოგადი არქიტექტურა*

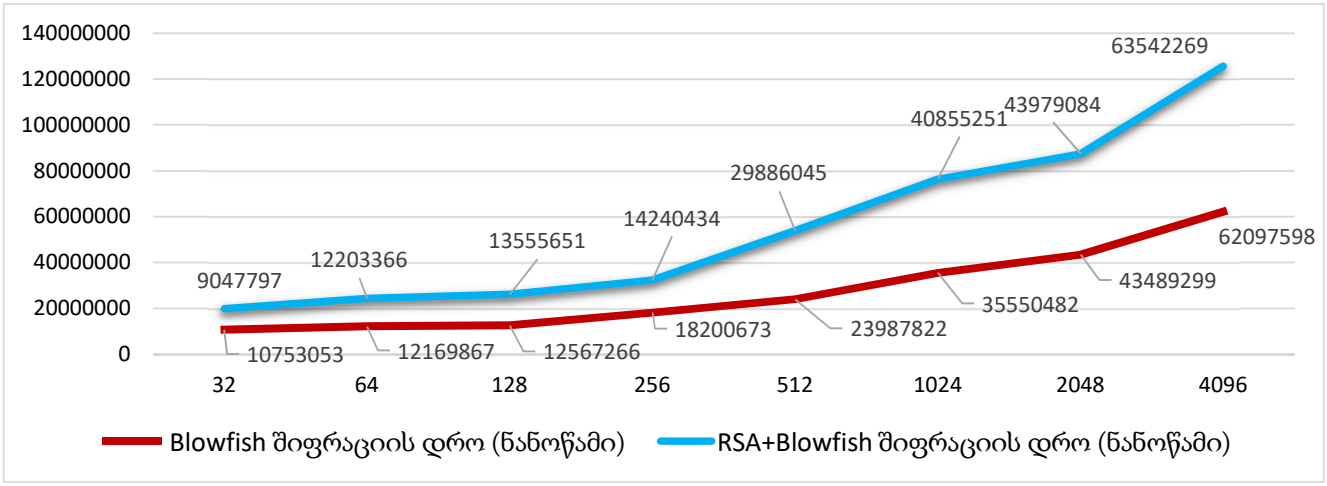
მოცემული სისტემის ალგორითმის Java პლატფორმაში რეალიზებული პროგრამული კოდის გამოყენებით შესრულდა სხვადასხვა ზომის მონაცემებზე შიფრაციისა და დეშიფრაციის პროცესები. (ცხრილი 3).

Blowfish + RSA შიფრაცია				
ფაილის ზომა (KB)	საწყისი ფაილის	შიფრაციის დრო (ნანოწამი)	დაშიფრული ტექსტის ზომა	დეშიფრაციის დრო (ნანოწამი)

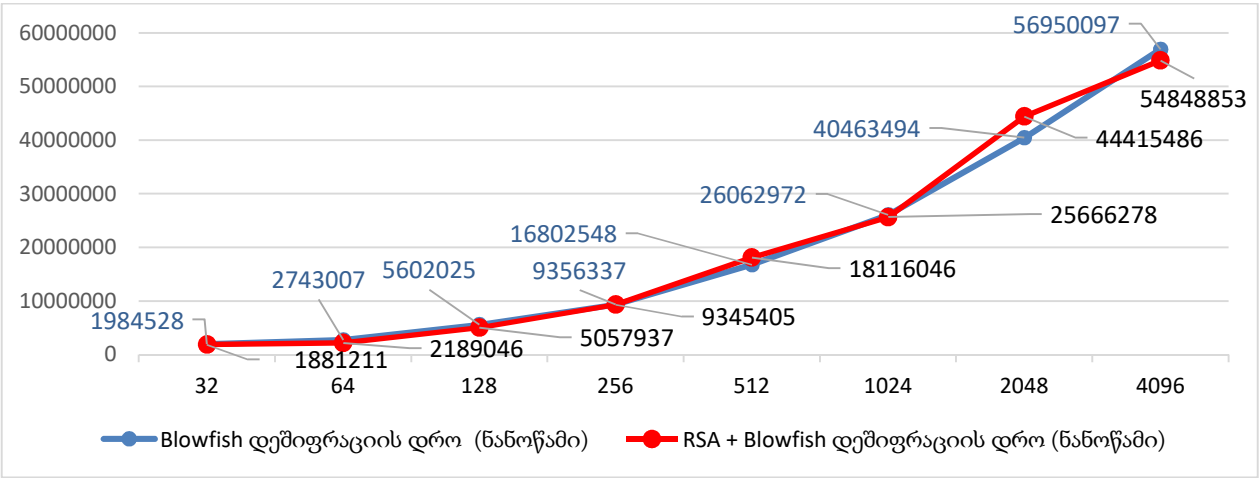
	ზომა (Byte)			
32	32710	9047797	59355	1881211
64	65420	12203366	118428	2189046
128	130840	13555651	237417	5057937
256	261680	14240434	477370	9345405
512	523360	29886045	951418	18116046
1024	1048460	40855251	1898922	25666278
2048	2096920	43979084	3813804	54415486
4096	4193840	63542269	7624638	54848853

ცხრილი 3. Blowfish + RSA ჰიბრიდული კრიპტოსისტემის შიფრაციის პროცესი

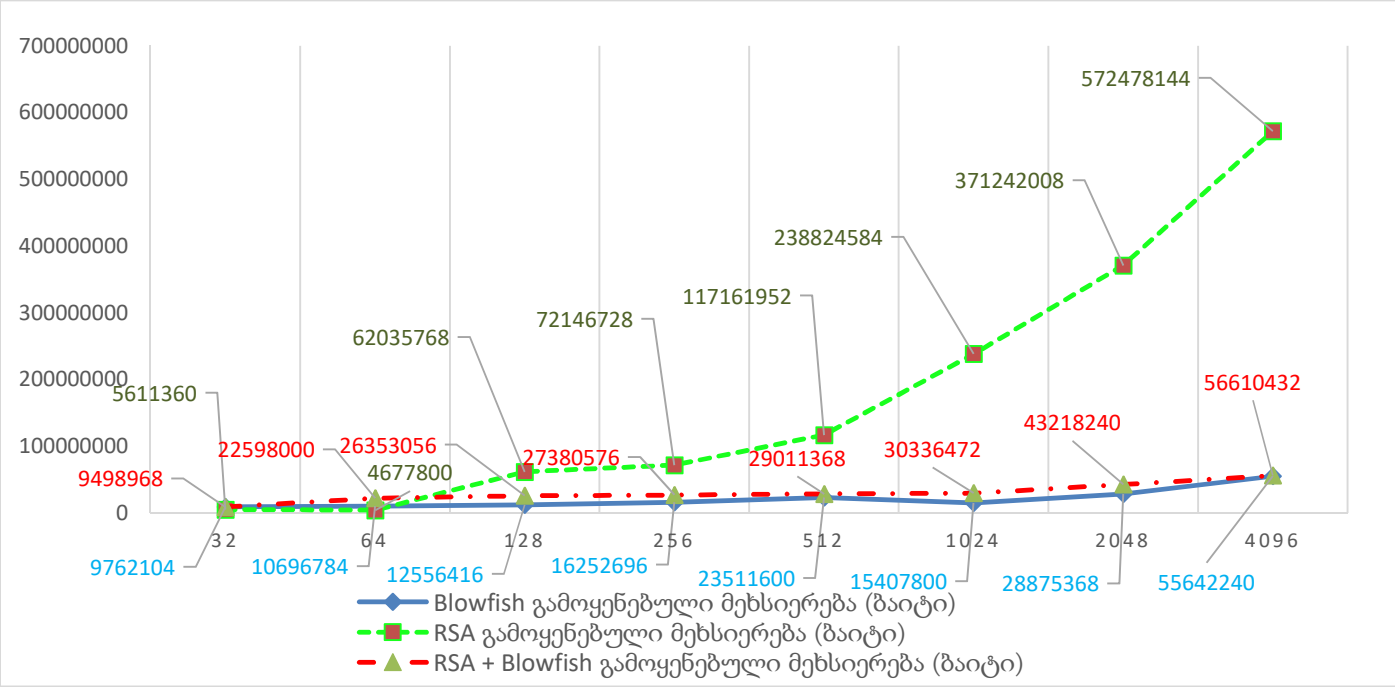
BLOWFISH, AES, IDEA ალგორითმების შედარებისას დგინდება, რომ BLOWFISH მოიხმარს უფრო ნაკლებ ტექნიკურ რესურსს. თუმცა IDEA მოიხმარს ნაკლებ რესურს ვიდრე AES, მაგრამ ჩამორჩება BLOWFISH ალგორითმს.



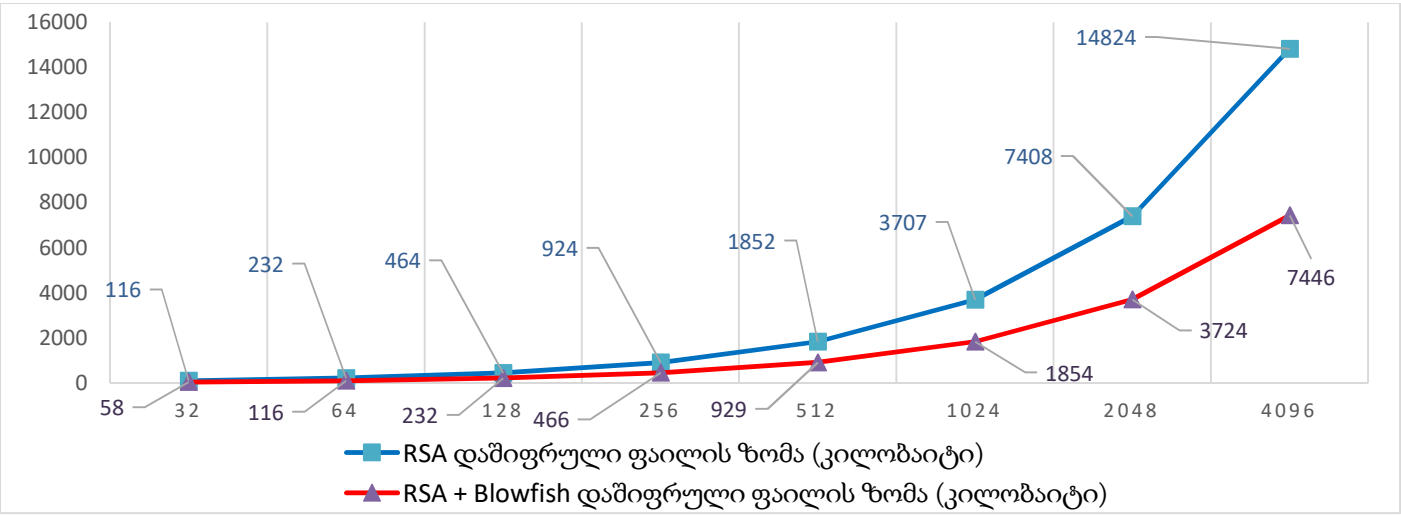
სურათი 4. Blowfish და RSA + Blowfish კრიპტოსისტემების შიფრაციის პროცესის დროის ვიზუალიზაცია



სურათი 5. *Blowfish და RSA + Blowfish კრიპტოსისტემების დეშიფრაციის პროცესის დროის ვიზუალიზაცია*



სურათი 6. *Blowfish, RSA და Blowfish+RSA სისტემებში მონაცემების (ბაიტი) შიფრაციისას გამოყენებული მეხსიერების გრაფიკი*



სურათი 7. *RSA და Blowfish+RSA სისტემებში შიფრაციის დროს დაშიფრული ფაილის ზომის ცვლილება*

დასკვნა

მოცემულ ნაშრომში განხილულია ორი სხვადასხვა სისტემის: სიმეტრიული Blowfish და ასიმეტრიული RSA ალგორითმის პროგრამული რეალიზაცია Java პროგრამირების ენაზე. წარმოდგენილია მოცემული ორი ალგორითმის კომბინაციით მიღებული ჰიბრიდული ალგორითმი და ასევე მისი პროგრამული რეალიზაცია.

მოცემულ ალგორითმებზე ჩატარდა ექსპერიმენტები, რაც ითვალისწინებდა სხვადასხვა ზომის საწყისი მონაცემის დეშიფრაცია/დეშიფრაციის პროცესების შესრულებას სამივე ალგორითმზე. შედეგად ძირითადი დაკვირვების ობიექტს წარმოადგენდა მათი შესრულების დრო და მოხმარებული მეხსიერების მაჩვენებელი. როგორც ჩატარებული ექსპერიმენტები უჩვენებს განხილული ჰიბრიდული ალგორითმი არის უფრო სწრაფი და ამავდროულად უსაფრთხო რადგან გათვალისწინებულია, როგორც სიმეტრიული ასევე ასიმეტრიული ალგორითმის ძლიერი მხარეები.

ჩატარებულმა ექსპერიმენტმა აჩვენა შემდეგი:

1) თუ Blowfish , RSA და Blowfish + RSA ჰიბრიდულ ალგორითმს შევადარებთ **გამოყენებული მეხსიერების მიხედვით** ყველაზე მაღალ ტექნიკურ რესურსს მოითხოვს RSA ალგრითმი, ხოლო Blowfish უმნიშვნელოდ ჩამორჩება Blowfish + RSA ჰიბრიდულ სქემას.
2) **შიფრაციის დროის** პარამეტრის გათვალისწინებით რა თქმა უნდა Blowfish რჩება თავის საწყის პირველ პოზიციაზე და ამ სისტემებში ყველაზე სწრაფია, თუმცა Blowfish + RSA ჰიბრიდული ალგორითმი არც თუ ისე დიდი მნიშვნელობით ჩამორჩება და მნიშვნელოვნად სწრაფია ვიდრე RSA, ხოლო RSA ყველაზე დიდ დროს ანდომებს შიფრაციას და ძალიან ნელია.
3) **დეშიფრაციის დროის** პარამეტრზე დაკვირვებამ აჩვენა, რომ Blowfish + RSA ჰიბრიდული ალგორითმი და Blowfish ალგორითმი თითქმის თანაბარი სისწრაფით ასრულებენ დეშიფრაციის პროცესს და არიან სწრაფი ვიდრე RSA ალგორითმი.
4) **დაშიფრული ფაილის ზომის პარამეტრზე** დაკვირვების შედეგად დადგინდა, რომ ყველაზე დაბალი მეხსიერება სჭირდება Blowfish სისტემას, შემდეგი არის Blowfish + RSA, ხოლო RSA ალგორითმი ყველაზე მაღალი მაცვენებლით ზრდის დაშიფრული ფაილის ზომას.

სამომავლოდ შესაძლებელია განხილული იქნას სხვა სიმეტრიული და ასიმეტრიული ალგორითმის ჰიბრიდული მოდელი, რომლებზეც განხორციელდება ენტროპიული კვლევა, რაც საშუალებას მოგვცემს დავადგინოთ თითოეული მათგანის მდგრადობა სხვადასხვა ტიპის თავდასხმის, მათ შორის დაშიფრული ტექსტის სიხშირული ანალიზის თავდასხმის მიმართ.

ლიტერატურა

[1] Johhanes A. Buhman, Introduction to Cryptography, Second Edition, 2000

[2] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanston, Handbook of Applied Cryptography, Massachusetts Institute of Technology, June 1996

[3] Ilya KIZHVATOV, Physical Security of Cryptographic Algorithm Implementations, , L'UNIVERSITÉ DU LUXEMBOURG, 2009

[4] Simson Garfinkel, Alan Schwartz, Gene Spafford, Practical UNIX and Internet Security, 3rd Edition Securing Solaris, Mac OS X, Linux & Free BSD

[5] The official Advanced Encryption Standard" (PDF). Computer Security Resource Center. National Institute of Standards and Technology. Retrieved 26 March 2015.

[6] Баричев С. В. Криптография без секретов. – М.: Наука, 1998.

[7] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С, 2-е изд . – М.: Вильямс, 2003.

[8] Мао В. Современная криптография: Теория и практика — М.: Вильямс, 2005

[9] Ященко В. В. Введение в криптографию. СПб.: Питер, 2001.

[10] Phillip Rogaway and Mihir Bellare, Introduction to Modern Cryptography, 2005

[11] "An Introduction to Modern Cryptosystems". Andrew Zwicke, 2003

[12] "Quantum cryptography: An emerging technology in network security". - Sharbaf, M.S. IEEE International Conference on Technologies for Homeland Security . 2011

[13] Adleman, Leonard M.; Rothemund, Paul W.K.; Roweis, Sam; Winfree, Erik (June 10–12, 1996). On Applying Molecular Computation To The Data Encryption Standard. Proceedings of the Second Annual Meeting on DNA Based Computers. Princeton University.

[14] Cramer, Ronald; Shoup, Victor (2004). "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack"

[15] Hofheinz, Dennis; Kiltz, Eike (2007). "Secure Hybrid Encryption from Weakened Key Encapsulation"

[16] Taher ElGamal (1985). «A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms

[17] https://www.techopedia.com/definition/1779/hybrid-encryption

[18] Криптология – наука о тайнописи //Компьютерное обозрение. –1999.

[19] Мао В. Современная криптография: Теория и практика — М.: Вильямс, 2005

[20] Ященко В. В. Введение в криптографию. СПб.: Питер, 2001.

[21] Hamdan O. Alanazi, B. B. Zaidan, A. A. Zaidan, Hamid A. Jalab, M. Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine factors", Journal of Computing, Volume, 2, Issue 3, March 2010, pp. 152-157.

[22] Dr. Prerna Mahajan and Abhishek Sachdeva, " A study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013, pp. 15-22.

[23] Deepak Kumar Dakate and Pawan Dubey, "Performance comparison of Symmetric Data Encryption Techniques", International Journal of Advanced Research in Computer Engineering and Technology, Volume 3, No. 8, August 2012, pp. 163-166.

[24] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms."

[25] Sumitra, "Comparative Analysis of AES and DES security Algorithms", International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013, pp. 1-5.

[26] Ayushi, 2010,A Symmetric Key Cryptographic Algorithm, International Journal of Computer Applications (0975 - 8887) Volume 1. No. 15, 2010

[27] "Quantum cryptography: An emerging technology in network security". - Sharbaf, M.S. IEEE International Conference on Technologies for Homeland Security . 2011

[28] The official Advanced Encryption Standard" (PDF). Computer Security Resource Center. National Institute of Standards and Technology. Retrieved 26 March 2015.

[29] "The Digital Millennium Copyright Act of 1998" (PDF). United States Copyright Office. Retrieved 26 March 2015.

[30] Cramer, Ronald; Shoup, Victor (2004). "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack"

[31] Hofheinz, Dennis; Kiltz, Eike (2007). "Secure Hybrid Encryption from Weakened Key Encapsulation". Advances in Cryptology -- CRYPTO 2007

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 51-63 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

AUTHENTICATION OF INFORMATION SYSTEMS USERS, BASED ON THE ANALYSIS OF THEIR HANDWRITING

Vysotska Olena[1], Davydenko Anatolii[2]
National Aviation University[1]
Pukhov Institute for modeling in energy engineering of NAS of Ukraine[2]

ABSTRACT. In this paper there was analyzed a relevance of the problem of an authentication of information systems users. There was also reasoned a choice of dynamic biometric authentication methods, namely the methods based on an analysis of a person's handwriting. Based on the results of the performed experiments, there were selected the handwriting characteristics, which were analyzed for recognition further. There were defined the requirements to training items and the stages of its selection and adjustment. On the basis of the created algorithm, there was written a program to perform the authentication of information systems users, with the help of which a number of experiments were carried out. According to the results of the experiments, it was concluded that it is advisable to use the handwriting recognition systems for the implementation of the authentication of information systems users.

Keywords: authentication, recognition, biometrics, handwriting, information systems.

With the increasing degree of computerization of most human activity areas, there is an increasing need of the authentication of information systems users. In different cases, it is advisable to use one or another authentication method. All the authentication methods can be divided into the following three types:

1. Password protection. The user presents a secret data (for example, password or PIN-code).

2. Key usage. The user presents his / her personal identifier, which is the physical carrier of a private key. For example, plastic cards with a magnetic stripe, key chains and other devices.

3. Biometric authentication, i.e. the usage of human biometric characteristics. The user presents a parameter that is a part of himself. With such authentication, the person's identity is exposed to recognition – his individual characteristics (fingerprints, face thermogram, retina, voice, handwriting, etc.).

In recent times, there increasingly began to use the biometric authentication [1]. The biometric authentication systems are very user-friendly. Passwords and storage media can be lost, stolen, copied. The biometric authentication systems are based on human parameters, that always remain with a person, and the problem of their safekeeping doesn't appear. It is almost impossible to lose them. It is also impossible to transfer the identifier to third parties.

Thus, we can say that the development of the biometric authentication systems is now one of the relevant problems.

The objective of this paper was to develop a biometric authentication system of information systems users, which could be used in various fields of human activity, not always associated with the computer.

To solve this problem, the following was done:

1. There were analyzed the existing methods of biometric authentication [2,3]. On the basis of the conducted analysis and taking into account the fact that biometric authentication, in this case, should be used for the user accessing the information system in cases which are not always associated with the user's work at the computer, as the analyzed characteristics of the person, it is proposed to use his handwriting in this work.
2. The varieties of handwriting authentication methods were analyzed and its characteristics are determined for their further use in the authentication process.
3. The analysis of the selected handwriting characteristics was conducted to determine their validation for further recognition [4,5].
4. The selection of training handwriting items of information systems users was made to increase the probability of correct recognition [6].
5. The adjustment of training handwriting items of information systems users was performed to increase the probability of correct recognition [6].
6. The program for handwriting authentication of information systems users was written. The neural network was used as a recognition mechanism [7].
7. On the basis of the conducted analysis, with the help of the written program, it was concluded that it is advisable to use handwriting recognition systems for the implementation of authentication of information systems users.

All methods of the biometric authentication are divided into two groups:

1. Statistical methods.
2. Dynamic methods.

Statistical methods are based on the measurement of physical (static) characteristics of a person, which must be unique for each person, or at least for most people. These characteristics aren't supposed to change significantly over a long period of time and be influenced by any external factors, such as cosmetics, weather events, etc. Statistical biometric authentication methods include methods that use the fingerprint, the shape of the palm, the location of the veins on the front side of the palm, the retina, the iris (each eye has its own picture), the shape of the face (full face, profile, volumetric geometry), the thermogram of the face, DNA, etc.

Dynamic methods of biometric authentication are based on the behavioral (dynamic) characteristics of a person, that is, which are built on the features, which are typical for the subconscious person's movements in the process of presentation of any action. Unlike physical distinctive characteristic, in this case, the biometric system doesn't necessarily have to measure the same phenomenon each time: a person may be asked to say, write, or walk in a certain way to reduce the risk of reproducing the characteristics by the violator. Dynamic biometric authentication methods are methods that use for recognition the handwriting, the keyboard pattern, the painting with a mouse, the voice (speech), the acoustic signal from the human body, the movement of the lips when reproduction a keyword, the gait, etc.

Let's consider in more detail the method of dynamic biometric authentication of information systems users, namely the method based on the analysis of handwriting. This method doesn't require an expensive equipment (only a graphics tablet or similar device is required), it can be used in cases unrelated to the work at computer of the authenticated one and, at the same time, it is a fairly reliable authentication method.

Handwriting recognition systems relate to dynamic person's identification systems based on the analysis of the dynamics of fast subconscious movements reproduction. Handwriting is an individual and quite stable characteristic of a person, when analyzing of which it is possible to identify the person who wrote the keyword. This fact is confirmed by the physiological maker of a person. Let's consider what determines the handwriting of a person more closely.

During the writing, the muscles of most fingers and forearm muscles are involved. In total, more than 50 muscles can be involved, but the most significant influence have about 10 muscles. That is, when writing some text, a person controls about ten muscles. This is quite a complex task and it can't be solved in real time. Therefore, during the writing the control of a person by muscles is based on standard solutions that are developed during a long enough writing training and are individual for

each person. These well-established standard solutions are kept throughout life and stay almost unchanged.

Dynamic characteristics of a person, including handwriting, can be used not only for recognition of people, but also for determining the character of the person, his mental and physical condition. For example, if a person is nervous or in a hurry, then the speed of writing increases and the handwriting becomes more boldly; the weak, sickly, and mentally ill persons have the letters that are non-uniform in size and with a variable inclination; the incompleteness of the words, simplified writing of the letters, bouncing up and down lines indicate the negligence of a person; etc. Analysis of these and other similar features is very useful when hiring (especially to the critical job) and while monitoring the work of computer users. For example, if the air traffic controller is tired or annoyed, he can make a mistake that will lead to serious consequences. A wide field of handwriting recognition algorithms usage determines the relevance of its analysis and improvement.

Let's consider the handwriting authentication more closely.

To perform this type of authentication, the user must depict (write) his password (signature or some keyword). As a password there can be used:

1. Some keyword, word or a letter combination.
2. Signature of a user.
3. Some figure.

In this paper, as a password there is proposed to use any common keyword or different words, but provided that all these words have the same fragment (letter combination).

In addition to that, in this paper it is proposed to divide the functioning of the authentication system into the following two stages:

1. The recognition of the written keyword. *At* this stage, it is checked whether the correct word was written by the authenticated one. If an incorrect word is entered, i.e. that it doesn't correspond to the pattern stored in the system for the given user, then the authenticated one is recognized as a violator, if the correct word is entered, then the second stage of recognition is performed [8].

2. Recognition of the keyword writing style. *At* this stage, the features of writing the analyzed word are checked for correspondence to the features stored in the system for this user. If the features correspond, then the authenticated one is recognized as a legal system user, otherwise he is recognized as a violator.

Mathematically the authentication (recognition) function $R=f(par_1,par_2,\ldots,par_g,\ldots,par_q)$ (where $1 \le g \le q$) can be expressed in the following way:

$$R = \begin{cases} 1, \text{ if } Usx \in Usl, \ Usx = Usl_d; \\ 0, \text{ if } Usx \in Usl, \ Usx \neq Usl_d; \\ 0, \text{ if } Usx \in Usb; \end{cases}$$

where $Usx \in Us$ is the authenticated person;

$Us=\{Us_1,Us_2,\ldots,Us_\infty\}$ is a set of people who can try to access the protected system;

$Usl=\{Usl_1,Usl_2,\ldots,Usl_t,\ldots,Usl_d,\ldots,Usl_l\}$; $1 \le t \le l$; Usl is a set of legal users of this system;

Usl_d is a legal user impersonated by an authenticated person ($Usl_d \in Us$ и $Usl_d \in Usl$);

Usb is the violator, i.e. the unregistered person in this authentication system ($Usb \in Us$, но $Usb \notin Usl$);

$par_1,par_2,\ldots,par_g,\ldots,par_q$ is the list of parameters on which the result of evaluation of the recognition function R depends.

One of the most important factors when constructing the recognition system is the optimal choice of the recognition mechanism that, accordingly, means the recognition algorithm constructing. There are various mechanisms for solving such problems. One of the most effective mechanisms for recognition is neural networks, and it is proposed to use it in this work.

For all types of biometric recognition technologies, an initial user template should be created first. To create it, it is necessary to collect (make a fixation of) a number of measurements from any device used (in this case, from a graphics tablet). Then, it is needed to pick out the specialties (characteristics) inherent to the user from the measurements, and use the extraction results for template creation. The creation of this initial template is called a registry. This initial template is then saved by the system and plays a part of a kind of password further. After registration, when the user attempts to pass the authentication procedure, the measurement data from the reader device is collected, processed into a usable form and checked for correspondence to the template that was previously registered. In case of confirmation, the user is recognized as the impersonated person. Thus, one can say that the handwriting authentication system should work in the following two modes:

1. The registration or accumulation of the training items database.

2. The user recognition (authentication).

Depending on the implementation of each specific biometric system, there may be some additional actions. For example, if necessary, it is possible to continue to

accumulate a database of training items, even at the recognition stage. Depending on the biometric authentication method used, the minimum size of such database will vary. For example, if the recognition method uses a fingerprint, there should be several items for each user (for several fingers and taking into account that the finger on the scanner can be placed at different angles) in the database. Conversely, if the method for recognition uses the handwriting, as in this work, then the database size is many times larger. This is explained by the fact that the fingerprint is a static parameter and does not change during a person's life, and the handwriting is a dynamic parameter and, depending on various factors, though not significantly, but can change. The need for a high volume of the training items database is also explained by the specifics of the functioning of the neural network, which is proposed to be used as a recognition mechanism in this work. Such a database usually reaches several hundred, and sometimes thousands of items for each user.

The key indicators of the efficiency of any authentication system are the error of the first kind (the denial of access to a legal user) and the error of the second kind (the omission of the violator). Therefore, when creating a handwriting authentication system, it is necessary to solve the problem of constructing the recognition function R, in which the error of the first kind (R=0, if $Usx \in Usl, Usx = Usl_d$) and the error of the second kind (R=1, if $Usx \in Usl, Usx \neq Usl_d$ or R=1, if $Usx \in Usb$) would be minimal, that is, to minimize the probability of false reject of a legal user (in case if he isn't impersonating another legitimate user) and the probability of omission the violator.

The result of evaluation the authentication function R depends on the list of parameters $par_1, par_2, \ldots, par_g, \ldots, par_q$. These parameters (features) selection is a primary target when constructing any recognition system. In this paper, there is used a set of features $At=\{At_1, At_2, \ldots, At_i, \ldots, At_n\}$; $1 \le i \le n$; as a set of features for recognition; where At is a set of features of person's handwriting; At_i is the i-th characteristic of handwriting.

Herewith, it should be noted that the At set depends on the level of computer technique development. The higher the level of technique, the larger the At set and the higher the maximum possible authentication quality. At earlier stages of the technique development it was possible to analyze only static characteristics of handwriting (the X and Y points coordinates), that's why the recognition quality wasn't high enough. And only with the advent of graphics tablets (and other similar devices) it became possible to determine and, therefore, to analyze the dynamic parameters of handwriting (the pen pressure on the tablet, the angle of the pen inclination, the speed and trajectory of

writing, etc.), which significantly increased the quality of recognition. Most of the features of the *At* set are the characteristics of the set of points presented for recognition of the keyword. These characteristics, as mentioned earlier, are such parameters as the X and Y points coordinates, the pressure (P) with which the user presses the pen on the tablet when drawing the next point, the writing speed, the angle of the pen the angle of the pen inclination, the angle of the characters inclination, the trajectory of writing, etc. (different systems can use a different set of characteristics). Thus, it may be said that the *At* set of features looks like this: $At=\{X, Y, P, ...\}$. However, to achieve the highest efficiency of the authentication system, f it is necessary to select the set of the most significant (control) points $Kt=\{Kt_1,Kt_2,...,Kt_{nkt},...,Kt_b\}$; $1 \le nkt \le b$; whose characteristics will be analyzed during recognition process, rom the set of these points $T=\{T_1, T_2,..., T_a,..., T_v\}$;. That is, from the set of data about the conveyed points $Pac=\{Pac_1, Pac_2, ..., Pac_a,..., Pac_v\}$ (where $1 \le a \le v$;), it's needed to create (to pick out) a set of data about control points $Pac\_kt=\{Pac\_kt_1, Pac\_kt_2, ..., Pac\_kt_{nkt},..., Pac\_kt_b\}$ (where $1 \le nkt \le b$;). This is quite an important stage of the authentication system operation, so we consider in detail.

When selecting control points, there appears the problem of the correctness of the automatic selection of control points. It is also important to determine the required number of control points. These two factors have a great impact on the efficiency of a particular recognition system, because if too few control points are selected or they are not correctly placed, the percentage of false recognition will be inadmissible large, and if there are set too many control points, then too much resources (time and memory) will be spent, and the recognition quality will increase slightly (or not increase) at the same time.

In this paper, there is proposed to emphasize control points of the following three types (Fig. 1):

1. The start and end points of each line. In figure 1, these points are shown in red color (points 1 and 15).

2. The angular points, that is, the points on the line bend. In figure 1, these points are shown in blue (points 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13).

3. The points of intercrossing of lines. In figure 1, these points are shown in green (points 8 and 14).

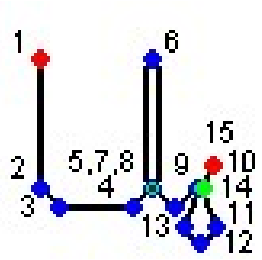


Fig.1. An example of control points placing

It is also rational to use the control point type as the point parameter to be analyzed.

In this work, it is recommended to divide the image of the whole keyword into images of individual letters and later work with images of each symbol separately. There are two reasons for this.

First, when checking the correctness of the written password (at the first stage of authentication), it is preferable to recognize the password not entirely, but symbolically. This is caused by the following reasons:

1. It is easier to collect items of writing N symbols (where N – is the number of characters in the used alphabet, taking into account the fact that not only lowercase letters can be used, but also uppercase letters and numbers, and various punctuation marks), than items of writing all possible passwords, which can be any combination of these N symbols, in the database. The number of possible passwords (the combinations of symbols), in this case is equal to $\sum_{Ks=1}^{Mks} Ks^N$ (where Ks is the password length, MKs is the maximum possible password length) or is equal to the Ks^N, if the Ks is known. The collecting of this amount of data is much more difficult than in the case of character-oriented recognition.

2. It is easier to check the classified object for belonging to one of the N classes than for belonging to one of the $\sum_{Ks=1}^{Mks} Ks^N$ classes. That is, the recognition process is easier in case of the character-oriented recognition analysis.

Secondly, data processing on all the password at once takes excessively large resources. When performing handwriting authentication with a help of the graphics tablet while writing a single symbol, the system receives the data on a one hundred points (sometimes on several hundred points) at an average. If the password, for example, has 6 characters, then it is necessary to process an average of 600 data points

to validate of the entered password. That is, at the first stage of authentication the neural network will need to process 1800 features (three parameters for each point: the X and Y coordinates and the type of control point), and it will take a very long time (and at the second stage there are more features and, therefore, there is needed even more time). Therefore, when performing each authentication step, it is recommended to analyze not all the password at once, but symbol by symbol, and if one of the symbols is incorrect, then the other symbols can be not analyzed (at least at the first authentication step). However, using such a strict condition, it is necessary to provide a very low probability of false failure when recognizing each character, so that false non-recognition of one character leads to false non-recognition of the entire password, and, consequently, the denial of accessing the protected system for the legal user.

Dynamic characteristics of a person are characterized by some instability. Neural networks cope with a small instability well enough (that is another reason for choosing this mechanism for solving the problem), but gross errors in the original data must be discarded, i.e. it is necessary to make the original data selection. For example, in the resulting training items there may be random deviations (errors), which characterize nothing and will only worsen the recognition quality, for this reason these deviations must be removed from the items, and if there are too many of such deviations in one item or they are too gross, then the item must be removed from the database (or simply not considered during recognizing). Most of these erroneous and atypical data are caused by the specifics of using a graphics tablet for the handwriting authentication of users. After analyzing the results of the performed experiments, the following five types of errors can be emphasized, which are caused by the specifics of the use of a graphics tablet for the handwriting authentication of users:

1. A sequence of points with zero pressure (except the first such point in each sequence).

2. Random points (in small amount).

3. Repeats, i.e. a sequence of consecutive points with unchanged coordinates along the X and Y axes (except for the case when one of the points has zero pressure).

4. Random small bends at the beginning of the lines.

5. Poor-quality item, discarded due to the inability to split the image of the password word for a given number of images of symbols (more often occurs as a result of lack of skills with the graphics tablet pen).

It should be noted that the algorithm for excluding erroneous data should be different at different stages of the authentication system. That is, some data that are erroneous at the stage of recognition of a written keyword can be distinctive

characteristics of the style of writing a keyword by a specific user and, accordingly, can be useful at the second stage of the authentication system operation.

In addition to that, to improve the efficiency of the performed recognition in this work, the original data is corrected, plus this correction should be different at different stages of recognition. The need for this adjustment is caused by the specifics of the graphics tablet usage for the handwriting authentication of users. The data adjustment should be performed after nominal splitting of the whole image of the password word into images of separate symbols, but before the control points placing. The necessity to adjust the data is explained by the following facts. The recognition is complicated by the fact that authentication can be performed using different graphics tablets. Herewith the characteristics of the tablet can vary (the size of the workspace, the press sensitivity, etc.), that affect the values of the analyzed parameters. For example, if the size of the tablet workspace is various, then the size of the analyzed image of the password word and its location may be various too. Therefore, to provide the correct recognition, it is necessary to recalculate the image parameters in accordance with some neutral (without reference to any particular tablet) workspace of the selected size. To do this, in any handwriting authentication system, with the usage of the graphics tablet, there are needed the image scaling and shifting (moving) functions on each axis. Therewith, even if the same graphics tablet is used, some writings may be written not horizontally, but at an angle (for example, if the tablet is rotated relative to the user), some may be written in large letters, some – in small, some labels may not be centered, but shifted in some direction. Such writing features interfere with the recognition of the password. Therefore, the recognition system should have the image scaling, shifting (moving) functions on each of the axes and the image rotation function. At the same time, it should be noted that we need not just the image shifting, scaling and rotation functions, but such its varieties as shifting the image to the center of the screen, rotating the image to a horizontal position and scaling (stretching) the image to the full screen. The presence of these functions is necessary to be able to recognize exactly the symbols of the word-password, not its location. Otherwise, the probability of correct recognition of the password word symbols will be very small.

All these functions are necessary as for the recognition of the whole password word and so for the character-oriented recognition, but in the second case, all these functions should be applied not to the image of the whole password word, but to the images of particular symbols. That is, the image of each symbol first should be rotated to a horizontal position, then placed in the center of the used workspace of the selected

size, and then proportionally stretch the image to the entire used workspace of the selected size. Otherwise, the location of the symbol will be recognized instead of itself.

Summing up, it can be said that this system requires the following three types of the character-oriented correction:

1. The character-oriented rotating of the symbols images for the normalization the angle of its axes inclination.

2. The character-oriented shift of the each symbol image to the center of workspace of selected size.

3. The character-oriented proportional scaling (stretching/compression) of each symbol image over the entire workspace of the selected size.

Summing up all the before-mentioned, it can be said that for the reliable recognition function *R* constructing it is necessary:

1. To make an optimal choice of individual biometric characteristics of a person to be used for authentication (the voice, the handwriting or the keyboard handwriting, the fingerprint, the retina, etc.).

2. To select the item recognition mechanism.

3. To determine the lists of *At* features that will be used for recognition (the number of consecutively performed recognition procedures can be one or more) during authentication, in accordance with the selected option.

4. To make a split of the entire password word image to the images of the particular letters.

5. To determine the criteria for the selection of analyzed samples.

6. To determine the necessary adjustments of the analyzed features.

7. To create an algorithm for placing control points.

8. To develop algorithms for solving the tasks of recognition to perform the authentication procedure.

To implement the above, there was written a program for performing the handwriting authentication of the information systems users, at the same time the neural network was used as a recognition mechanism. The results of experiments performed with the help of the written program showed the effectiveness of the proposed algorithm.

Conclusion

In this work, on the basis of the analysis, and taking into account that the developed biometric authentication system should be used for user accessing to the information

system in cases not always associated with his work at the computer, and as an analyzed characteristic of a person his handwriting was chosen. There were analyzed the varieties of handwriting authentication methods and its characteristics were determined for their further use in the authentication process. Then the analysis of the selected handwriting characteristics was performed, in order to determine their validity for further recognition. After that, the selection of training handwritings items of information systems users was made to increase the probability of correct recognition. The adjustment of training handwriting items of information systems users was performed to increase the probability of correct recognition, too. To implement the above, a program was written to perform the handwriting authentication of information systems users, while the neural network was used as a recognition mechanism. A number of experiments were carried out with the help of the written program. Based on the results of the performed experiments, there were given the recommendations (requirements) on the data pre-processing for recognition and on the configuration the most critical system parameters.

Thus, it can be concluded that the usage of handwriting recognition systems is advisable for the implementation of authentication of information systems users.

References:

1. Arthur Galeev.: Almost all companies in the U.S. and Europe will use biometrics in two years., 30.03.2018. http://safe.cnews.ru/news/top/2018-03-26_pochti_vse_kompanii_v_ssha_i_evrope_budut_ispolzovat

2. Vysotska O., Davydenko A., “Classification of biometric authentication systems”, Collection of scientific works of the Pukhov Institute for modeling in energy engineering of NAS of Ukraine, Vol. 27, pp. 108-114, 2004.

3. Vysotska O., Davydenko A., “Determination of critical parameters when choosing a biometric authentication system”, Modeling and information technologies. Collection of scientific works of the Pukhov Institute for modeling in energy engineering of NAS of Ukraine, Vol. 27., pp. 80-86, 2004.

4. Vysotska O., “Assessment of quality of biometric authentication methods and the ways of its improvement”, Modeling and information technologies. Collection of scientific works of the Pukhov Institute for modeling in energy engineering of NAS of Ukraine, Vol. 28, pp. 94-102, 2004.

5. Vysotska O., “Selection of analyzed characteristics when handwriting authenticating of computer systems users at different stages of computer technology development”, Modeling and information technologies. Collection of scientific works of

the Pukhov Institute for modeling in energy engineering of NAS of Ukraine, Vol.56. – pp. 31-39, 2010.

6. Vysotska O., Davydenko A., "Analysis of data pre-processing technology when authentication of computer systems users by the keystroke pattern and handwriting", Modeling and information technologies. Collection of scientific works of the Pukhov Institute for modeling in energy engineering of NAS of Ukraine, Vol.55. – pp. 34-41, 2010.

7. Kallan R.: Basic concepts of neural networks. Translate from English. Publishing house "Williams", 2001.

8. Vysotska O., "The problem of recognition of the written keyword as one of the problems solved when performing handwriting authentication of of computer systems users", Modeling and information technologies. Collection of scientific works of the Pukhov Institute for modeling in energy engineering of NAS of Ukraine, Vol.36. – pp. 67-76, 2006.

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 64-74 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

ANALYSIS OF THE CYBERSECURITY STATUS OF THE INFORMATION SPACE

Nikolay Brailovskyi [1], Valeri Kozura [2], Svetlana Kondakova [3], Volodymyr Khoroshko [2],

Taras Shevchenko National University of Kyiv [1]
National Aviation University [2]
Kyiv National Economic University named after Vadym Hetman [3]

ABSTRACT. The article analyzes the state of the current situation in the information and cyberspace. The differences between cyber influence and cyber threat are indicated and their classification is provided. Issues of cyberterrorism, cyber intelligence and cyberwarfare are considered.

KEYWORDS: information space, cyberspace, cyber influence, cyber threat, cyber terrorism, cyber intelligence, cyberwarfare.

Формирование и развитие современного информационного общества, факт образования которого официально было определенно представителями государств «Большой восьмерки» в ходе Окинавской встречи в июле 2000 года, базируется, как известно [1], на синтезе двух технологий: компьютерной и телекоммуникационной, а также определяется двумя простыми, но очень содержательными законами. Первый закон сформулирован одним из основателей Корпорации Intel Гордоном Муром: «… количество транзисторов в процессорах будет увеличиваться в два раза каждые полтора года…». Этот закон фактически объясняет формирование на рубеже тысячелетий так называемого информационного пространства [1], возникновение новых, специфических по форме и способам, субъектов и объектов информационной инфраструктуры, а также гарантированное возрастание скорости вычислений и объемом информации, которая при этом обрабатывается. Второй закон принадлежит Роберту Меткалфу (изобретателю технологии компьютерной сети Internet), который говорил, что: «…ценность сети находится в квадратичной зависимости от количества узлов, которые есть ее составляющими». Этими словами он констатирует, что основу современного информационного общества составляют сети разнообразного функционального назначения, совокупность и взаимосвязь которых информационное пространство собственно и образовывает [1], а также новейшие информационно-телекоммуникационные (IT) технологии, которые в последнее время:

— стали важной составляющей общественного развития мировой экономики в целом и вместе с тем в значительной степени изменили механизмы функционирования многих общественных институтов и институтов государственной власти;

— вошли в число наиболее существенных факторов, которые влияют на формирование современной высокоорганизованной информационной среды и дают возможность на качественно новом уровне информационного обслуживания в виртуальном и реальном пространствах вести повседневную оперативную работу, осуществлять анализ

состояния и перспективы деятельности информационно-аналитических подразделений, а также добывать исходные данные, необходимые для принятия рациональных научно обоснованных управленческих решений.

Постепенное и довольно условное объединение виртуальных информационно-телекоммуникационных систем (ИТС) и сетевых технологий различного функционального назначения, которые в процессах обработки, передачи и хранения информации используют электромагнитный спектр и действуют как единое целое, а также соответственного программного обеспечения (ПО) привело, как следствие, к формированию так называемого киберпространства - высокоразвитой модели объективной реальности, в которой сведения о личности, предметах, фактах, явлениях и процессах:

— представлены в некотором математическом, символьном или любом другом виде;

— размещаются в памяти любого физического устройства, специально предназначенного для её сохранения обработки и передачи;

— пребывают в постоянном движении в совокупности ИТ систем и сетей.

Под киберпространством разные специалисты в большинстве своём понимают коммуникационную среду, образованную системой связей между объектами инфраструктуры. Учитывая это, наиболее отличительными признаками киберпространства как субстанции является создание и внедрение электронно-цифровых форм обработки, хранения и передачи информации. Кроме этого специалисты считают, что киберпространство имеет непревзойдённые возможности по созданию многочисленных связей между отдельными индивидами и социальными группами с предоставлением разноплановых информационных услуг.

Про важность киберпространства свидетельствует появление концепции ведения борьбы в нём, создание в вооружённых силах ряда стран мира (Россия, США, Китай и другие) специальных структур, предназначенных для ведения такой борьбы – комплекса мер, направленных на осуществление управленческого и/ или деструктивного влияния собственных информационных ресурсов путём использования специальных аппаратно-программных средств.

Такое состояние дел, а также глубокие изменения по отношению большинства стран [2] к собственной информации и, как следствие, кибербезопасности (рис.1) – состояние защищенности киберпространства государства в целом или отдельных объектов инфраструктуры от постороннего влияния, а также своевременного выявления, предотвращение и нейтрализация реальных и потенциальных кибернетических вмешательств, и угроз личным, корпоративным и/или государственным интересам:

во-первых, дают возможность говорить о формировании принципиально новой геостратегической, геоинформационной и геополитической ситуации, когда возникают совсем новые угрозы безопасности для объектов критически важной инфраструктуры этих государств. Получив их, граждане и общество в целом выводят на безусловно более высокий уровень вес исследований, направленных на всестороннее анализ методов, средств, тактики и стратегии действий в информационном и киберпространствах, то есть ведение так называемых информационных и кибернетических воин;

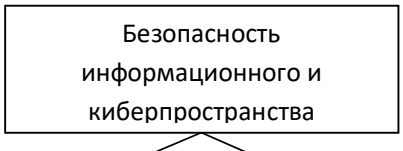


Рис. 1. *Объекты влияния в информационном и киберпространствах*

во-вторых, приводят к беспрецедентному разглашению персональных данных важных корпоративных ресурсов, конфиденциальной информации и информации, которая составляет государственную или другую предусмотренную законом тайну;

в-третьих, обуславливает насчёт кратко и долгосрочных приоритетов трансформации сектора безопасности этих государств по направлениям:

- - поиск и добыча информации путем совершенствования способов и методов организации и проведения атак на ИТ и защищенные криптосистемы противоборствующих сторон и автоматизации всех сопутствующих этому процессов;
- обмен информацией, путем разработки принципиально новых ИТС специального назначения;
- защита собственного информационного ресурса от внутренних и внешних кибервлияний и угроз.

С развитием информационно-коммуникационных технологий (ИКТ), ИТС и глобальные сети интернет мировое сообщество кроме полученных значительных возможностей по обмену информацией стало слишком уязвимым от постороннего кибернетического влияния [1,3], а именно от фактически не прикрытых попыток влияния противоборствующих сторон на информационное и киберпространства друг друга за счёт использования средств в современной вычислительной и/или специальной техники и соответствующего программного обеспечения и других проявлений их дестабилизирующего влияния на определенный объект, которые реализуется за счёт использования технологического и киберпространства, создавая при этом опасность как для их самих, так и для сознания человека в целом.

Инструктивные материалы интернета делят кибервлияние и киберугрозы на такие группы:

- собственно компьютерные инциденты, которые заключаются в вмешательстве в работу вычислительных систем, нарушении авторских прав на программное обеспечение, а также разворовывании данных и компьютерного времени и так далее;

- инциденты, «связанные с компьютерными», которые сопровождаются главным образом противоправными действиями по направлению финансового мошенничества;

- сетевые инциденты, которые способствует осуществлению незаконных договоров.

Существует и другая классификация [3] таких действий. Она определяет 7 основных групп, которые можно отнести к способам или методам, которые используют злоумышленники для совершения нападения, а именно:

- перехват паролей пользователей;
- «социальная инженерия»;
- использование ошибок программного обеспечения и программных закладок;
- использование ошибок механизмов идентификации пользователей;
- использование несовершенства протоколов передачи данных;
- получение информации про пользователей стандартными способами операционных систем;
- блокирование сервисных функций системы, которая атакуется.

Наибольший интерес позиций классификации кибернетических влияний и угроз становится схема, которая предложена конвенцией Совета Европы по борьбе с киберпреступностью. В ней говорится про четыре возможных группы таких действий [1]:

Первая группа — это инциденты, направленные против конфиденциальности, целостности и доступности компьютерных данных и систем, которые реализуются через:

— несанкционированный доступ в информационную среду (противоправный намеренный доступ к компьютерной системе или её части, а также к информационным ресурсам противоборствующей стороны, сделанные в обход системы защиты);

— вмешательство в данные (противоправные изменения, обезвреживание, удаление, перекручивание или блокирование компьютерных данных и управляющих команд, путём проведения кибератак на информационные системы, ресурсы и сети государственного и другого управления);

— вмешательство в работу системы (противоправное нарушение или создание преград функционирование компьютерной системы путем разработки и распространения вирусного программного обеспечения, использование аппаратных и программных закладок, радиоэлектронного и других видов влияния на технические средства и системы телекоммуникации, системы защиты информационных ресурсов, систем и сетей программно-математического обеспечения, протоколы передачи данных, алгоритмы адресации и маршрутизация и так далее);

— незаконный перехват (противоправное умышленное аудирование не предназначенных для общего доступа компьютерных данных, переданных СИТ специального назначения в обход средств защиты и безопасности);

— незаконное использование компьютерного телекоммуникационного оборудование (изготовление, покупка для использования, распространения или другие способы сделать доступными данные: устройства, включая программное обеспечение, разработанные или приспособленные для совершения каждого из преступлений 1 группы: компьютерные пароли, коды доступа, другие подобные данные, которые обеспечивают доступ к компьютерной системе или ее части) или её полное изъятие.

Вторая группа - это мошенничество и подделка, связанные с использованием компьютеров, которые состоят в:

— подделке документов с использованием компьютерных средств (противоправном умышленном внесении, хранении и удалении или блокировании компьютерных данных, которые приводят к снижению достоверности документов);

— мошенничестве с использованием компьютерных средств (вмешательство в функционирование компьютерной системы с целью умышленного противоправного получения экономической выгоды для себя или для других лиц).

Третья группа — инциденты, связанные с размещением в сетях противоправной информации.

Четвёртая группа — инциденты, относительно авторских и смежных прав.

Представленный список не является исчерпывающим, но он даёт возможность [2]:

во-первых, условно объединить приведённые типы действий в 2 укрупнённые категории — вмешательство и угроза, направленные непосредственно на нарушение нормального функционирования ИТС и подключённых к ним компьютеров [1] (тип 1 — по схеме,

предложенной конвенцией Совета Европы), а также традиционные противоправные действия (типы 2, 3, 4 — по той же схеме), которые или связанные с компьютером, или совершены с его помощью;

во-вторых, сделать вывод про то, что определенные таким образом подобные действия в киберпространстве вышли за границы отдельных государств и получили при этом существенную финансовую помощь и качественные коммуникации;

в-третьих, формализовать приведённые типы действий, представив их в виде модели, которая будет содержать 3 главных этапа:

— этап изучения определённого объекта;

— этап проведения нападение на него;

— этап скрытия следов нападения.

Кроме этого, как минимум, в каждом этапе должны быть по 2 стадии — стадия информационного обмена и собственно стадия нападения. Последние, в свою очередь будут состоять из: во-первых, операций по обмену данными, рекогносцировки, отмены и составления карты действий — характерные для информационного обмена и, во-вторых, с операцией получения доступа, расширение полномочий, кражи информации, бомбежки, уничтожение следов, создание «черных ходов» и отказом в обслуживании — характерные для стадии совершения нападения.

Последнее время именно такие действия совершаются противоборствующими сторонами с целью нарушения или блокирования работы информационных систем и сетей в стратегически важных отраслях (объектах) инфраструктуры друг друга, в том числе военного, транспортного, финансового, промышленного и энергетических секторов, а также несанкционированного получения информации из относительно открытых и закрытых баз данных (баз знаний) государственных, коммерческих и других учреждений, их модификации и/или полного уничтожения.

Согласно официальным данным интернета темпы их роста из года в год непременно увеличиваются [4,5]. Это в свою очередь привело к появлению принципиально нового распределения террористических действий в кибернетическом пространстве, который в конце концов получил в СМИ название — кибертероризм [2]. Директор центра защиты национальной инфраструктуры ФБР США Рональд Дик в докладе, который был опубликован на сайте Федерального бюро расследований, так характеризует ситуацию, которая сложилась на сегодня: "... в мире сформировалась новая форма терроризма — кибертерроризм, который использует компьютер и сети связи для разрушения частей национальной инфраструктуры и достижения собственных целей" [1].

Выступая по проблемам мировых угроз, директор ЦРУ Джордж Тенет заявил, что кибертерроризм, распространяясь по миру, может со временем приобрести значительно больших, чем ожидалось, масштабов и, как результат, стать реальной угрозой для национальной безопасности любого государства. По его утверждению, уже угрозы большинства террористических группировок для поддержки своей противоправной деятельности используют последние достижения информационных технологий и компьютерного прогресса — "... компьютерные файлы, электронная почта и криптография и стеганография". Подтверждением этому есть тот факт, что на сегодня в Internet представлены своими файлами абсолютно все известные террористические группы. Они выдают собственные

материалы, как минимум на 40 разных языках и в своей деятельности используют в большинстве такие приемы, как [5]:

— нанесение ущерба отдельным элементам информационного и киберпространства;

— разрушение аппаратных средств, сетей электроснабжения и элементов базы ИТС, а также наведение помех путем использования специальных программ, биологических и химических средств;

— кража или уничтожение информационных, программных и технических ресурсов информационного и киберпространства, которые имеют общественное значение, путем преодоления их системы защиты, внедрения вирусов и разного рода закладок;

— влияние на программное обеспечение и информацию с целью их перекручивания или модификации;

— раскрытие или угроза опубликования, или собственно само опубликование закрытой информации про функционирование информационной инфраструктуры государства, общественно значимые военные информационные системы, коды шифрования и принципы работы шифровальных систем;

— захват канала средств массовой информации с целью распространения дезинформации, слухов, демонстрация силы террористической организации и провозглашение своих требований;

— уничтожение или активное подавление линий связи, искусственные перегрузки узлов коммутации;

— проведение информационных и психологических операций и тому подобное.

Основным способом действия кибертеррористов является проведение атаки на компьютерную информацию, вычислительные системы, аппаратуру передачи данных и другие составляющие ИТ инфраструктуры противоположной стороны.

Это будет способствовать их распространению на систему, которая подвергается атаке, на перехват управления, подавление средств сетевого информационного обмена и совершение других деструктивных влияний.

Кроме отмеченного широко применяется и развивается кибербразведка. Её большинство специалистов по информационно-коммуникационным технологиям (ИКТ) понимает сейчас в основном как самостоятельный метод разведки средствами Internet. На наш взгляд сущность такого вида рода деятельности и основные функции и процедуры на современном этапе развития ИКТ и информационно-телекоммуникационных систем (ИТС) должны заключаться в:

1) систематическом и целенаправленном поиске и сборе информации об объекте разведки с помощью средств ЭВТ и ПО из ресурсов ИТС;

2) изучении, верификации и аналитической обработке накопленной информации, оценке на этой основе возможных угроз (рисков) собственно киберпространства, выявление их признаков и прогнозирование их возможного появления;

3) планирование и, в случае необходимости, осуществление воздействия на киберпространство путем применения активных и/или пассивных методов осуществления противодействия.

То есть, фактически кибербразведка (виртуальная разведка) сейчас представляет собой безусловное сочетание интеллекта, знаний и умений человека, а также внедрение в процесс её деятельности специальных ИТ, направленных на получение банков данных, обеспечение

контроля за сообщениями и информацией, циркулирующих в вычислительных сетях и Internet, получение персональных данных пользователей информационных сетей и другой ценной компьютерной информации.

Следует учитывать, что процесс информатизации всех сторон жизни наполняет качественно новым содержанием разведывательно-информационную работу. Она всё больше сосредотачивается в виртуальном информационном пространстве, заметно меняет роль и место человека в процессе добывания разведывательных сведений и их последующей обработки.

Эксперты спецслужб справедливо делают вывод о том, что складывается особая структура, объединяющая объекты разведки, их информационные образы, запечатлённые в открытом и закрытом информационных массивов, линиях телекоммуникации, выведенных для них, программные и аппаратно-технические средства поиска, преодоление рубежей защиты, обработки полученной информации, ее хранения и распределения [6].

Неотъемлемой частью такой структуры является человек. Эта структура ставит задачи на добычу, поиск, прорыв к защищенному информационному ресурсу, обработки полученных сведений и является потребителем конечной разведывательной продукции, выстраивая на ее основе свою виртуальную действительность, частью которой является сам.

Различные стороны разведывательной деятельности испытывает растущее влияние новых ИТ. Они формируют качественно новые потребности в разведывательно-информационном обеспечении государственной системы принятия политических, военных и экономических решений. Но с такими технологиями открываются и принципиально новые возможности удовлетворения этих потребностей.

Ведущие специалисты по проблемам теории и практики информационной борьбы отмечают, что решающую роль будут играть ИТ — взлом информационных сетей потенциального противника, посещение и уничтожение информации, внедрение дезинформации, внесение компьютерных вирусов и в конечном итоге — полное разрушение системы управления, контроля и выполнения стратегических и тактических планов противника.

Репетициями будущих информационных сражений служат сегодня преступления хакеров, которые вторгаются в информационные сети банков и похищают крупные суммы денег. Для победы в информационном пространстве нужно добиться решающего превосходства над противником в характеристиках и ассортименте суперкомпьютеров, в наборе и содержании программного обеспечения и их возможностях [6,7].

Поэтому, тенденция виртуализации разведывательного процесса отражает закономерный переход к псевдоиерархии узнаваемых природных и искусственных сред — от разведки естественной «первичной», а затем естественной биологической и искусственной среде, возникающей в результате деятельности человека и среды четвертого поколения — искусственного, которая появилась в результате деятельности искусственных интеллектов.

Как считает американский исследователь Майкл Кастанья, сейчас виртуальная (кибернетическая) разведка, которая возникла и совершенствуется — это прообраз разведки будущего. Под понятием "виртуальной (кибернетической) разведкой" — имеется в виду распределенная сетевая организация по производству синтезированной разведывательной информации тактического, оперативного и стратегического уровня с использованием новых ИТ [6].

Исследователи и эксперты обращают внимание на тенденцию, которая всё больше проявляется, виртуализацию деятельности по получению информации. В отличие от традиционной агентурно-оперативной деятельности с целью извлечения разведывательной информации, она ведется преимущественно с использованием новых ИТ в искусственной информационной среде с минимальным участием человека.

Следует отметить и такой важный фактор как кибервойна, которая уже идет. Тема кибервойны в последнее время довольно активно исследуется представителями большинства ведущих стран мира. Пристальное внимание этому вопросу придается также и определенными военными блоками. Так в руководящих документах Североатлантического Альянса кибервойна с недавнего времени рассматривается в одном ряду с противоракетной обороной и борьбой против международного терроризма. При этом в большинстве документов Альянса неоднократно подчеркивается, что из-за роста зависимости стран - членов НАТО от ИТ технологий и увеличения количества атак на их ИТ инфраструктуру, Альянс вполне серьезно подойти к вопросу классификации кибервойны как действия, подпадающего под статью 5 Вашингтонского договора.

Учитывая такое и, несмотря на то, что НАТО уже сегодня имеет три линии кибероборонь, а именно: службу NATO Computer Incidents Response Capabilities Center; Гаагский исследовательский центр проверки действующих систем и выработки новых стандартов защиты и Программу разработки защищенных систем связи, - руководство Альянса в последнее время с целью повышения эффективности ведения военных действий именно в киберпространстве дополнительно разрабатывает [6]:

- специальную структуру для защиты стран-членов от кибератак, которая будет заниматься сбором разведывательных данных и координировать действия членов НАТО в борьбе с киберпреступностью (создание отдельной структуры по предотвращению кибератакам одобрено участниками саммиту НАТО 2-4 апреля 2008 года в Бухаресте. Там же заложено отдельное направление работы альянса под названием "Политика кибернетической обороны");
- концепцию кибервойны будущего, в основу которой положен прежде всего военно-технические концепции C4I (Command, Control, Computer Communication and Intelligence for the Warrior), а также доктрину так называемого киберманевра, что предусматривает разделение всего театра военных действий на две составляющие - традиционную и в киберпространстве (идея предложена в 1996 году экспертом Пентагона Р. Банкер).

В данном случае концепция C4I предусматривает согласованное развитие систем управления, вычислительной техники, связи и разведки. Основным содержанием этой концепции является автоматизация различных процедур сбора, обработки, хранения и передачи информации. В ее рамках планируется достичь высокой степени автоматизации функций целеуказания и распределения информации различного вида, в том числе электронной почты, телеконференцсвязи и т.д. Значительная роль при этом возлагается на внедрение экспертных систем, средств моделирования боевых действий, комплексов технических средств автоматизации, использующих технологии высокопроизводительных ЭВМ и нейрокомпьютеров. Концепция C4IFTW предусматривает, прежде всего, сообщения и функциональную интеграцию систем управления, вычислительной техники, связи и разведки и, во-вторых, создание глобальной информационно-управляющей инфраструктуры, которая

должна обеспечить условия для начала боевых действий крупными военными формированиями без предварительного развертывания систем управления и связи сразу после переброски в места назначения, ее практическую реализацию планируется осуществить за счет: создания совокупности распределенных национальных баз данных, доступных командирам любых уровней; создание устройств сопряжения систем C4I; обеспечение многоуровневой безопасности; жесткой стандартизации требований к сообщениям, процесса испытаний и приобретения систем. Наличие в названии концепций C4I и C4IFTW термина Computer подчеркивает важность того, что применение вычислительной техники среди прочего высокотехнологичным оборудованием в значительной степени изменило способы ведения военных действий и стало жизненно необходимым элементом современных операций. При этом, как подчеркивают военные эксперты, основными объектами поражения на земле и на море, в воздухе и космосе новых войнах будут информационная инфраструктура и психика противника (в связи с этим термин "human network" получает в лексиконе американских военных аналитиков в последнее время все более широкое распространение) [6,7].

Одним из достаточно показательных примеров ведения кибервойны следует считать события 2010 года вокруг сайта Wikileaks на страницах которого была опубликована огромное количество грифованных документов, которые касались войн, которые ведут США в Афганистане и Ираке, а также более 250000 документов переписки американских дипломатов. Специалисты оказались не в состоянии предоставить однозначную оценку этому факту. Часть из них до сих пор считает Wikileaks проектом скрытой операции ЦРУ, что направлена на общую дестабилизацию обстановки в мире. Другие наоборот - характеризуют деятельность сайта как удар собственно по Европе и прямую угрозу западной демократии. Тем не менее, они сходятся в одном - атака, которая была проведена коллективом в несколько десятков сотрудников с годовым финансированием в 200 000 долларов: загрузила разведывательные службы многих стран мира анализом сотен тысяч непроверенных документов; доказала неготовность США - страны, которая имеет огромный арсенал ядерных и обычных вооружений и практически всех ведущих стран мира к ведению кибервойн, их уязвимость для такого рода атак, а также их неспособность обеспечить надлежащий уровень защиты собственных данных; послужила основой для отработки метода давления на некоторых неконтролируемых партнеров путем организованного сбора и обнародования против них ничем не подкрепленных обвинений.

Другим, не менее ярким примером возможности применения новейших ИТ технологий стала также, в последних несколько лет, действия России в киберпространстве.

До последнего времени было не очень понятно, что из себя представляет российская кибервойна. Сейчас картина прояснилась, это многофункциональный инструмент с высочайшим уровнем экспертизы, где задействованы не только тролли, работающие в России, Европе и США, но и огромные группы экспертов, обеспечивающие тончайший анализ актуальных ситуаций и очень быструю реакцию на них. Причём этот анализ и психологический, и политический, и военный.

Кроме того, оказывается воздействие на западные СМИ и институции. Фактически ведется подкуп журналистов и европейских политиков, который измеряется десятками миллионов долларов. И это без учета проектов, конвертированных в пропагандистские инструменты — телевидение, радио, газеты, Internet-издания, а также (что указано в резолюции

Европарламента) большое число институтов, работающих в Европе, США, Израиле и других местах. Плюс индивидуальные соглашения с лоббистами.

Пропагандистские кампании ранее рассматривались как идеологический инструмент для продвижения этих концепций. Первое время так рассматривали и пропагандистскую кампанию в современной России — как продвижение идеи "русского мира". Новое качество состоит в том, что это уже не только продвижение идеологии, но и инструмент ведения войны. Чего стоят только акты вмешательства российских представителей в процессы предвыборных кампаний США, Германии, Украины, Франции и т.д.

Кибератаки и огромные группы троллей только с одной стороны направленные на продвижение идей, а с другой — нацеленный на ведение военных действий, поддержание агентурной сети, деморализация противника, ослабление защитных механизмов и функции государства противника. Сейчас продолжают использовать словосочетание "пропагандистская кампания", хотя речь уже идет об инструментах ведения военных действий, которые наносят ущерб сознанию гражданского населения и вполне могут наносить материальный ущерб.

Таким образом, характерными признаками, которыми сейчас олицетворяют понятие кибербезопасности [2, 3, 4, 6] является совокупность активных защитных и разведывательных действий, которые в процессе информационного противоборства усилиями редких инсайдеров или организованных кибергруппировок разворачивается вокруг ИР, ИКТ, и ИТС [4,7] и которые направлены на достижение и удержание потенциальными противоборствующими сторонами победы в противодействии новым угрозам безопасности для собственных объектов критически важной информационной инфраструктуры.

В последнее время такие действия занимают четкое место в геополитической конкуренции преобладающего большинства стран мира, что в свою очередь обуславливает новые задачи их службам безопасности и вооруженным силам и выводит на первый план проблему информационного противостояния.

Библиография.

1. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки. – К.: Вид. НАУ. 2013 – 432 с.

2. Хорошко В. А. Кибертерроризм и информационная безопасность / Хорошко В. А., Шелест М. Е.// Правове, нормативне, та метрологічне забезпечення систем захисту інформації в Україні – Вип. 1 (27). 2014. – С.19-14.

3. Козюра В. Д. Методика оцінки рівня безпеки інформаційного простору/ Козюра В. Д., Піскун С. Ж., Хорошко В. О., Хохлачова Ю. Є.// Інформаційна безпека людини, суспільства, держави. №1 (11). 2013. – С. 121-126.

4. Хорошко В. О. Особливості застосування сучасної інформаційної зброї/ Хорошко В. О., Козел Т. І., Ярошенко О. О.// Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. Вип. 1 (29). 2015. – С.19-15.

5. Гриненко І. Структура кримінальних відносин у кіберпросторі/ Гриненко І., Прокоф’єва-Янчиленко Д., Гончаренко Д.// Правове, нормативне, та метрологічне забезпечення систем захисту інформації в Україні – Вип. 1 (25). 2013. – С.16-21.

6. Хорошко В.А., Шелест М. Е. Информационно-аналитическое обеспечение безопасности – К.: ВПВ «Задруга», 2016. – 183 с.

7. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки. – Житомир: ЖНАЕУ, 2016. – 636 с.

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 75-80 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

STEGANOGRAPHY AS A MEANS OF ATTACKING INFORMATION SYSTEMS

Anna Romanova [1], Sergiy Toliupa [2]
[1]Taras Shevchenko University of Kyiv, Faculty of Information Technology, [2] Taras Shevchenko University of Kyiv, Faculty of Information Technology

ABSTRACT. An analysis of steganography methods that are can be potentially used as instruments in attacks on information and communication systems is presented. The possible solutions to ensure resilience to such attacks are presented.

Keywords: steganography, TEMPEST, covert channel, information protection

Cryptography is widely used as one of the most efficient and approbated methods of critical information resources protection. Nevertheless, in particular cases it might be more effective to hide the communication channel itself instead of making the information within it unreadable. Such a practice, namely concealing data within unsuspicious, innocent-looking containers, is called steganography.

Any concept might have a double application. While being primarily considered a means of information protection, steganography can be used with ill intentions, as well. In fact, several high-tech attacks are based on the hidden data transmission, and contemporary methods of counteraction do not provide satisfactory level of resilience to those. These attacks are not always considered to be steganography-based, as they, for the most part, use a variety of features, characteristic for information and communication systems – physical effects, transmission protocols, communication infrastructure, specific features of software, cryptography etc. Nevertheless, the attack requires a classical statement of the task of steganography – how to transmit data so that a potential attacker could not acquire them due to not knowing about the presence of a transmission channel, even if he or she has a suspicion about one and the possible methods are known. In this case, though, an attacker and a legitimate user switch places, and the counteraction involves mainly the preservation of information resources.

In such attacks, the main advantage of steganography becomes the main source of threat – the channels of the attack, not to mention the information about the attacker left in the channels, cannot be identified due to the nature of the method. In other words, attacks become invisible, as does the transmission channel. The fact of trespassing itself cannot be easily detected or proven.

The purpose of this article is to conduct an analysis of attacks that are carried out with the use of steganography methods as their basis, and are directed against information and communication systems. Both existing and potential methods are presented.

1. Steganography as a means of hiding information

1.1. Basic terminology

Steganography is an art and science of storing and transferring secret messages within covert channels that are based on and created inside open channels in such a way that the cover data is perceived as if not having any embedded messages for its unplanned recipients.

The main concepts are:

- Container b (also: carrier) is open data used to conceal secret information;
- Message m (also: payload) is secret information to be concealed;

- Key k is secret information that is known only to a legitimate user and defines a specific concealment algorithm;
- Empty container c (also: unmodified container) is a container devoid of any secret data; it is a sequence of lc-long elements;
- Modified container s (also: package, steganogramme) is the one that contains a secret message;
- Steganographic algorithm means two transforms, a direct F: M x B x K → B and an inverse one F-1: B x K → M;
- Steganographic system (also: steganosystem) is a totality of messages, secret keys, containers and transforms that connect them [1, 3].

Most steganography methods are based on two key principles:

- Human senses cannot distinguish slight changes in colour, shape and sound perception;
- Consequently, there are files that do not demand absolute preciseness and therefore can be modified without losing their functional value.

As a result, said methods imply allocation of insignificant fragments of the container and replacement of the information within them with information that needs to be hidden.

Finally, the process of encoded steganogramme detection is called *steganoanalysis*.

Mostly, steganography uses the data concealment within digital images and audio files, less so video files and text. Electronic communications may also include hiding data inside of a transport layer (program or protocol) [4].

Starting with non-digital methods, physical steganography technics cannot be omitted. They have been developing for centuries and include, for example, blinking one's eyes in Morse code to spell a secret message [5].

Another example is adding tiny yellow dots to each page while printing a document. They are not detectable by the bare eye and contain the model, serial number and timestamps. This information cannot be obtained from a computer file and is embedded in a printout using dot-matrix code. The technology is used by many brand color laser printers, such as Xerox and Hewlett-Packard for traceability reasons [6].

The most popular methods of embedding data within an image container include Least Significant Bit method (LSB) (Sequential Insertion), LSB Psuedo Random Insertion, Palette permutation, Relative DCT (Discrete Cosine Transform) values change method, Fridrich method, Spread-Spectrum methods, and embedding pictures within video-files [2, 3, 5].

Audio steganography uses LSB-method for audio-files, Phase coding method, and echo-signal use [3, 7]:

Linguistic steganography [3]:

- Random interval methods. Changing the number of spaces in the end of the text string does not cause significant changes in the meaning of the sentence. What is more, an average reader is unlikely to detect insignificant space modifications:
  - Changing the interval between sentences. One or two additional spaces are added after the sentence.
  - Changing the number of spaces in the end of text lines. Spaces are added according to the secret bit to be hidden. Two spaces encode one bit a line, four spaces – two bits etcetera.
  - Changing the number of spaces between words in a flattened text. When the text is width aligned, spaces between words are not of the same length and some of them can be used to hide data.

- Making the text of the same colour as the background [5];
- Using similarly looking Unicode and ASCII characters [4, 8];
- Using non-printable Unicode characters [8];
- Creating a pattern of deliberate errors and/or marked corrections [4].

Some other methods:

- Converting a file so that it has the statistical characteristics of another one [4];
- Format steganography;
- Blog-steganography. Secret data is added as commentary pin boards on social networks [5].

Surely, the list above is not at all exhaustive. New methods and applications are being continuously developed, effectively putting steganography at top positions within the field of security.

2. Steganography methods used as instruments for attacks

To identify the methods of steganography that can be used as tools for attacks, it is necessary to first determine channels of information transmission that can be used in a covert way. Those are numerous, and file formatting, as well as different emanations from electronic devices are among them.

2.1. Format steganography

Perhaps, the easiest and the most well-known way, which is actually a steganography method, is using legitimate features of file formats to carry hidden malicious software within their structure. A file of every format contains specific fields, which ensure that the former will be processed correctly on the target computer. Some of these fields are optional, or more strictly – information that they contain is not vital for the file. Thus, changing data bits in these fields most probably will not lead to errors while operating with the file. Such characteristics make these formats perfect containers [10].

A vivid example is a virus Win95.CIH – specific malware which is embedded in *.exe files by using Portable Executable format features. This format includes a lot of additional data which are grouped according to their functions. Every group gets its own section in the file structure, and the size of the sections is predefined. If they are not entirely filled with data, it means the file contains a lot of spare space. For example, the first section is only for the PE header, so a big part of the virus uses it as a covert container [11].

This method is no commonly seen as a steganography method, though the analysis of scientific works has shown that such a question has not been even risen. A covert channel is being used, and data are being secretly embedded into the containers, which makes this a classical steganographic system. The next step in this research is to provide a mathematical model for a steganosystem used in a potential attack with file formats as carriers of malicious software and other instruments of intrusion and destruction.

2.2. Soft Tempest

In fact, there are a lot of ways to covertly transmit necessary information to the target system. Not only harmless files but also network protocols can be used as efficient containers within the attacker’s steganography system. Nevertheless, necessary means depend on the final objective of the attack. If the goal is to steal data, there is need for both an inward and an outward information flow. Getting information into a system is important. A more interesting question, though, is how to get the stolen data out without raising suspicion of a legitimate user.

While operating, every electronic device (including those inside a computer) gives off compromising emanations – electromagnetic emanations, which can be demodulated and accordingly processed to illegitimately get the critical information from them. These are called TEMPEST emanations after an American standard on the matter.

Contemporary TEMPEST-based attacks tend to become more and more sophisticated as the countermeasures are being continuously enhanced, as well. Systems are contaminated with the malicious software which then conducts the search of necessary information (key data, passwords, specific files etc) and induces the leak through TEMPEST emanation. For example, if reception of the signal is the one from the monitor, then the information will be, say, amplitude modulated and sent as a visual picture to the monitor. The obvious disadvantage is that such an activity cannot be missed by an operator and will be deemed highly suspicious, which, on its part, will lead to finding and neutralizing the virus.

M. Kuhn and R. Anderson conducted a series of experiment in which they shown a possible solution [12]. The human eye is more sensitive to low-frequency than to high-frequency vibrations, while TEMPEST receivers work vice versa. What is more, any devices primarily perceive luminosity in a linear way, while humans are more sensitive for the dark colours. This difference in sensitivity perception can be used to embed a message in the emanation and make it invisible to an unsuspecting user. The suggested method is to control and modify monitor dithering patterns. Pixels of two colours put in a check pattern are seen as a uniform colour, on the one side; on the other side, they create a high-frequency signal, which is best received by TEMPEST equipment with the following use of gamma-correction. Basically, the target computer is programmed so that it acts as a radio transmitter and emits a compound TEMPEST signal: a legitimate user observes one picture, and the attacker receives another – embedded – one on the monitor of his/her TEMPEST receiver.

The only suggested method of counteraction, which is specific enough for this very type of attack, is still based on using the difference in perception sensitivity between humans and devices. TEMPEST fonts are designed with top 30% of the Fourier transform of the signal removed, which is most probably not noticed by a human eye, but makes it impossible to receive a strong TEMPEST signal [12]. Nevertheless, special equipment with necessary parameters (enhanced sensitivity to low-frequency emanations) might be designed, which will make the use of such fonts ineffective.

2.3. Acoustic emanations as containers

Electromagnetic fields are not the only by-product of the computer systems operation. A. Shamir and E. Tromer published the results of their research, in which they showed that computer emit high-pitched noise while operation, due to vibration in some of their electronic components [13].

A series of experiments conducted by the scientist revealed that acoustic emanations can provide a potential attacker with information about what kind of software is currently running on the target system, as well as leak data on security-related parameters and computations. For example, loops of CPU instructions were highly distinguishable, and different RSA keys appeared to induce different sound patterns. To extract individual keys, the technic of acoustic cryptoanalysis was presented (applicable to GnuPG's implementation of RSA). According to the results, it takes about an hour to extract full keys from a target computer, irrespectively to their models and manufacturers. The key piece of equipment used for the attack is a microphone, and that of a mobile phone was demonstrated to be enough. Apart form acoustics, the scientists demonstrated a low-bandwidth attack, based on the same principles. The

main difference was that the attacker had to get the leakage from ends of VGA, Ethernet, USB or other cables [13].

If electromagnetic emanations can be used as containers in steganography systems, acoustic waves can be, too. The first case could be based on the nature of sound perception itself – the classical steganography technic. Human hearing systems cannot distinguish slight variations in an acoustic flow. Here, any known method, mentioned above (Least Significant Bit, Echo-signal use etc) can be used to embed stolen information in parasitic sounds, emitted by the target computer. The second possible scenario is similar to the use of emanations in Soft Tempest. Sound dithering is a widely used method in music digital processing. The principle is the following: any piece of musical record might contain extensive frequency transitions that are too slow and smooth. This is where so called quantization noise can appear. If the level of frequency fluctuation is insignificant, the processing software simplifies the sound by removing the frequencies that exceed some medium limit. To cope with such a situation, special noises are generated and gradually added to the record. In music processing, this technic allows to achieve a natural sound lost during quantization.

It is possible to suggest, that the same technic can be used in attacking steganography systems. The noise emitted by a computer is quite stable. It is not foiled by fan system noise, as critical acoustic signals appear to be mostly above 10 KHz, while a typical fan noise along with other noises lie in a much lower frequency band [13]. Task-switching is not a problem either, as it is the tasks that carry distinguishable acoustic spectral signatures. The same can be said about several computers working simultaneously in a closed space: they can be told apart using different sound patterns, as their depend on specific hardware, temperatures inside and outside the system, humidity, and other conditions. Thus, it acoustic emanations seem to be a sufficient container, while dithering can be accordingly modified and applied as an embedment method.

The only suitable countermeasure seems to be the use of sound dampening equipment that can diminish the level of high-frequency leakage. As for means of active protection, strong wide-band noise source can serve for masking the critical data signals. Rough-scale behaving algorithms are another solution: despite somewhat diminishing the level of performance, they can thwart side-channel attacks by shuffling the signal and making it thus useless for the attacker [13]. In addition, electronic components of the system should be those of the highest quality, designed to reduce the level of acoustic and any other leakage.

Nevertheless, at this point, efficiency of such protection methods is rather relevant, as sound-proving degrades other performance features along with being quite expensive. At the same time, due to the need of ventilation, there are still open parts in the cases, so their structure has to be constructed to shuffle outcoming noises very efficiently.

3. Conclusion

Stenganography is a powerful means of information protection. Nevertheless, it has to be also regarded as an instrument for a potential attacker, with all of the advantages turned threats.

Compromising emanations of different physical nature are invisible and can only be noticed with the use of special equipment. Using steganography technics for the attacks ensures that the fact of using those emanations is efficiently hidden, and the system operations remains unsuspicious. This is exactly why there is need to consider technics described above a real threat for information and communication

systems, and to join academic and technical potential to develop cost-effective and technically efficient counteracting means.

REFERENCES

[1] Зорин Е.Е., Чичварин Н.В.: Стеганография в САПР. Учебное пособие. МГТУ им. Н.Э. Баумана, Москва (pdf).

[2] Alexandre Miguel Ferreira: An Overview on Hiding and Detecting Stego-data in Video Streams. University of Amsterdam, System & Network Engineering – Research Project II, March 23 2015.

[3] Konakhovich G. F., Puzyrenko A. Yu.: Computer steganography. Theory and practice with Mathcad (Rus). MK-Press Kyiv, Ukraine 2006.

[4] Fridrich, jessica, M. Goljan, D. Soukal: Searching for the Stego Key. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI 2004 (pdf): http://www.ws.binghamton.edu/fridrich/Research/Keysearch_SPIE.pdf.

[5] Christopher League: An overview of digital steganography, particularly within images, for the computationally curious. Long Island University 2015: https://www.youtube.com/watch?v=-7FBPgQDX5o.

[6] Secret Code in Color Printers Lets Government Track You; Tiny Dots Show Where and When You Made Your Print. Electronic Frontier Foundation October 2005: https://www.eff.org/press/archives/2005/10/16.

[7] Echo Data Hiding (html): http://www.slidefinder.net/a/audio_steganography_echo_data_hiding/24367218.

[8] Akbas E. Ali: A New Text Steganography Method by Using Non-Printing Unicode Characters. Eng& Tech. Journal, 28 (1) 2010 (pdf): http://www.uotechnology.edu.iq/tec_magaz/volume282010/No.1.2010/researches/Text%287%29.pdf.

[9] Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А.: Стеганография, цифровые водяные знаки и стеганоанализ. Москва: Вузовская книга 2009.

[10] Anna Romanova, Sergiy Toliupa: Perspective steganographic solutions and their application. Proceedings of the VII Inter University Conference „Engineer of XXI Century" at the University of Bielsko-Biala (ATH), December 08, 2017, Bielsko-Biala, Poland. Volume 2 – p 269-278.

[11] С. Чеховский: Современные методы скрытой передачи информации путем программного управления излучением компьютеры. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, випуск 7, 2003.

[12] M.G. Kuhn, R. Anderson: Soft Tempest: Hidden data transmission using electromagnetic emanations. University of Cambridge, Computer Laboratory, New Museum Site, 1998 (pdf): https://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf.

[13] D. Genkin, A. Shamir, E. Tromer: RSA key extraction via low-bandwidth acoustic cryptoanalysis.Tel Aviv University, December 18, 2013 (pdf): http://www.cs.tau.ac.il/~tromer/papers/acoustic-20131218.pdf.

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 81-86 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ К ОЦЕНИВАНИЮ ЗАЩИЩЕНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА

Sergiy Gnatyuk, National Aviation University, Doctor of Science (Cybersecurity), Associate Professor, Kyiv, Ukraine
Viktoriia Sydorenko, National Aviation University, PhD in Information Security, Kyiv, Ukraine
Yuliia Polishchuk, National Aviation University, PhD Student, Kyiv, Ukraine
Vitaliy Kotelianets, National Aviation University, PhD Student, Kyiv, Ukraine

ABSTRACT. Currently, due to the large number of cyber incidents which occur daily, critical information infrastructure protection and assessing its security level is an important technical and scientific task. In this scientific paper, a qualitative analysis of well-known approaches and methods for assessment the security of information resources in critical information infrastructure objects is carried out. It will be useful for improving the level of critical information infrastructure protection of the state.

KEYWORDS: critical information infrastructure, security assessment method, cybersecurity, security of information resources.

Современное понятия критической информационной инфраструктуры (КИИ) выходит за рамки изучения лишь одной дисциплины. На сегодня, это сложная система, которая характеризуется совокупностью автоматизированных систем управления процессами критически важных объектов и систем, обеспечивающих их взаимодействие необходимых для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка. Именно поэтому, проблема обеспечения защищенности такой инфраструктуры является одним из наиболее актуальных вопросов, изучение которого требует системного подхода (Рис. 1). Исходя из того, что обеспечения безопасности объектов КИИ должно происходить на государственном уровне, государству необходимо обеспечить нормативно-правовую базу для регулирования вышеупомянутого вопроса. Для примера, рассматривая законодательную базу Украины, как и в большинстве пост-советских государств, на сегодня отсутствует методика оценивания защищенности информационных ресурсов (ИР) объектов КИИ, разработка которой безусловно есть актуальной научной задачей.

Рис. 1. Сектора КИИ согласно IPREM

В связи с этим, **целью настоящей работы** является проведения анализа современных подходов и методов для оценивания защищённости ИР объектов КИИ.

Основная часть. Проведя обзор подходов к оцениванию защищенности объектов КИИ, можно выделить следующие:

Украинский опыт

Приказом Администрации Государственной службы специальной связи и защиты информации Украины №112 от 2008 г. был утвержден Порядок оценки состояния защищенности государственных ИР в информационных, телекоммуникационных и информационно-телекоммуникационных системах (Порядок) [1]. Под процессом оценивания защищенности государственных ИР (процесс оценки) в информационных, телекоммуникационных и информационно-телекоммуникационных системах (ИТКС), согласно [1], следует понимать совокупность мероприятий, направленных на выявление угроз государственным ИР от осуществления несанкционированных действий в ИТКС. Согласно [1], объектом оценивания защищенности является состояние защищенности государственных ИР, которые обрабатываются в ИТКС, независимо от наличия комплексной системы защиты информации (КСЗИ), которая осуществляется с целью выявления существующих угроз государственным ИР в ИТКС и является составной частью мер по защите информации. Ответственность за проведение оценивания защищенности возлагается на Государственную службу специальной связи и защиты информации Украины (Госспецсвязь). Одной из задач Госспецсвязи, в соответствии с [1], является разработка общей программы и методики оценивания защищенности в органах государственной власти, органах местного самоуправления, воинских формированиях, предприятиях, учреждениях и организациях независимо от форм собственности, а также отдельные программы и методики оценивания защищенности зависимо от вида ИТКС и режима доступа к информации, которая в них обрабатывается. Кроме этого, в Концепции создания государственной системы защиты критической инфраструктуры Украины от 2017 г. [2] указано отсутствие единой методологии проведения оценивания угроз критической инфраструктуре.

Опыт Грузии

Рассматривая законодательную базу Грузии, важно отметить, что в 2010 г. было создано Агентство по обмену данными (DEA) при Министерстве юстиции Грузии [3]. В компетенцию DEA входит обеспечение кибербезопасности всей правительственной сети (за исключением ее военной части). DEA устанавливает минимальные требования по информационной безопасности для критических информационных систем. Под руководством DEA функционирует Компьютерная группа реагирования на чрезвычайные ситуации (CERT) – она отвечает за реагирование на киберинциденты и наблюдение за работоспособностью правительственной сети Грузии. CERT уполномочена требовать доступ к критическим информационным системам или активам. На международном уровне Грузия в 2012 г. ратифицировала Конвенцию о киберпреступности, разработанную Советом Европы. В 2015 г. был принят Закон Грузии «О порядке планирования и координации политики национальной безопасности», где сфера информационной безопасности (статья 11) включает действия по обеспечение защиты критических информационных систем [4]. Кроме того, в январе 2017 г. была принята национальная Стратегия по кибербезопасности и план действий на 2017-2018 гг., где одной из задач является исследование критериев идентификации и стандартов для КИИ [5]. Анализируя ситуацию в Грузии, можно сделать вывод, что страна поддерживает политику

Европейского Союза (ЕС) в области кибербезопасности, но, так же как и Украина, будучи ассоциированным членом ЕС, на данный момент не сформировано список объектов КИИ и, соответственно, методов и методик по их защите.

Опыт США

В январе 2014 г. в США был создан National Critical Information Infrastructure Protection Centre (NCIIPC), главной целью которого является оценивания уровня кибербезопасности в КИИ. Позже был разработан специальный документ – NCIIPC Framework for Evaluating Cyber Security in Critical Information Infrastructure [6] в котором предложен алгоритм оценивания кибербезопасности в КИИ (Рис. 2). Этот Framework демонстрирует 5 этапов проведения оценивания уровня кибербезопасности КИИ и показывает роль NCIIP в этом процессе. Однако, эта структура является вспомогательным механизмом, направленным на то, чтобы дать представление о процессе оценивания уровня кибербезопасности в рамках определенной организации, а не отрасли.

Опыт РФ

Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий разработало «Методические рекомендации по оценке защищенности критически важных объектов» (Рекомендации РФ) [7]. В Рекомендациях РФ оценивается состояние защиты критически важных объектов по уровню реализации мероприятий повышения их защищенности. В Рекомендациях РФ под защищённостью объекта понимается состояние (способность), при котором предотвращаются, преодолеваются или предельно снижаются негативные последствия возникновения потенциальных опасностей от угроз техногенного, природного характера и террористических проявлений. Однако, в Рекомендациях РФ под защитой критически важных объектов понимают только физическое или инженерно-техническая защита. Это обусловлено тем, что ИР и информационная система не считается критически важным объектом.

Рис. 2. Схема оценивания кибербезопасности в КИИ [4]

Результаты научных исследований в области защиты КИИ

Невойт Я.В. в диссертационной работе [8] разработала метод оценивания защищенности ИР на основе исследования источников угроз информационной безопасности. В работе были решены следующие задачи: по совокупности наиболее опасных угроз, на которые должны быть направлены первоочередные меры защиты, – сформировано совокупности пар «угроза-уязвимость»; по совокупности сложившихся пар «угроза-уязвимость» – определяется индекс защищенности ИР и вычисляется комплексный показатель их защищенности. Однако, в данном методе используется не полный перечень угроз и уязвимостей, что не позволяет эффективно повысить уровень обеспечения информационной безопасности.

Янчук В.А. разработал методику оценивания защиты информационных локальных объектов системы электронного управления [9]. Исследователь определяет эффективность защищенности информации локальных объектов системы электронного управления через эффективность комплекса мер по защите информации локальных объектов системы электронного управления и оценивает степень защищенности информации локальных объектов системы электронного управления. Однако, автор не адаптировал указанную методику для оценки эффективности защиты информации в информационной системе в обобщенном случае, например, для оценки эффективности состояния защиты информации объекта -сфера-отрасль общественной деятельности государства, а также для оценивания состояния защиты информации в государстве.

Бурькова Е.В. исследовала задачи оценивания защищенности информационных систем персональных данных [10]. Автором была разработана схема этапов оценки защищенности персональных данных в информационных системах, однако в этой работе

большее внимание уделяется защите самой информационной системы, а не ИР; а также не исследуются основные характеристики информации.

В работе Евсеева С.П. предложена методология оценивания безопасности информационно-коммуникационных технологий на примере автоматизированных банковских систем, которая базируется на концепции стратегического управления безопасностью указанных систем [11]. Предлагаемая концепция предполагает синергетический подход к выбору наиболее эффективных направлений достижения поставленных целей кибербезопасности с учетом величины риска на каждом уровне модели стратегического управления. Подобный выбор позволяет комплексно проводить отбор альтернативных вариантов возможных стратегических решений по вопросам кибербезопасности. Однако, предложенная концепция ориентирована исключительно на банковский сектор, не является универсальной и не может применяться для других отраслей КИИ.

Голобородько М.Ю., Курченко А.А. и Кирис А.С разработали метод числовой оценки уровня защищенности информации в сегменте корпоративной информационной системы [12]. В исследовании использован вероятностно-статический подход, при котором не учитывается динамика изменения значений вероятность угроз и уязвимости информации во времени. Оцениваются также априорные ожидаемые значения вероятности нарушения защищенности информации. Однако, для получения информации, необходимой для расчета приведенных показателей метода, обязательным условием является наличие системы мониторинга деятельности информационной службы предприятия.

Сидоренко В.Н. разработала метод оценки уровня кибербезопасности [13], который дает возможность рассчитать количественные параметры, характеризующие защищенность определенной области или КИИ государства в целом. Однако, в данной работе, при разработке методики не принимались во внимания характеристики информации и влияния человеческого фактора на ситуацию.

Исследователями Soon-Tai Park, Jong-Whoi Shin, Bog-Ki Min, Ik-Sub Lee, Gang-Shin Lee и Jae-Il Lee была предложена методика оценивания уровня информационной безопасности объектов КИИ [14], которая включает процедуры для измерения уровня безопасности организации и получение уровня зрелости путем анализа данных. Авторами были созданы контрольные списки для 12 категорий управления, которые будут оцениваться на пяти уровнях. На основе модели измерения зрелости SSE-CMM и SP800-26, предлагаемые пять уровней были разработаны в качестве контрольных. Далее сертифицированными аудиторами проводится заполнения контрольных листов и выставления оценки по 12 категориям. Как только результаты оценки будут подтверждены, оценки для каждого элемента управления рассчитываются для оценки уровня информационной безопасности организации. Однако, данная методика не учитывает специфику отраслей КИИ и есть базовым аудитом уровня информационной безопасности предприятия.

В табл. 1 отображены результаты анализа подходов и методов оценивания защищённости ИР в объектах КИИ по таким критериям: SS – учет способов и средств кибербезопасности; ICT – учет имплементации ИКТ; QP – вывод количественных показателей; CIIP – оценивание отраслей КИИ; UN – универсальность; HF – учет человеческого фактора при оценке; IP – учет характеристик безопасности информации (основных и дополнительных).

Подходы и методы оценивания
защищённости ИР в объектах КИИ

Таблица 1

Критерии / Название метода	SS	ICT	QP	CIIP	UN	HF	IP
NCIIPC Framework	+	+	-	-	+	+	-
Рекомендации РФ	+	+	+	+	-	+	-
Невойт Я.В.	-	-	+	-	+	+	-
Янчук В.А.	-	+	+	+	-	-	-
Бурькова Е.В.	-	+	-	-	+	-	-
Евсеев С.П.	+	+	+	-	-		
Голобородько М.Ю., Курченко А.А., Кирис А.С	+	+	+	-	+	+	-
Сидоренко В.Н.	+	+	+	+	+	-	-
Soon-Tai Park, Jong-Whoi Shin et al	-	+	+	-	+	+	-

Выводы

Таким образом, в данной работе проведен многокритериальный анализ подходов и методов оценивания защищённости ИР в объектах КИИ. Установлено, что на сегодня не разработан универсальный метод оценивания, который учитывает все критерии для качественного оценивания защищённости ИР объектов КИИ. В дальнейших исследованиях, с учетом результатов этой работы, планируется разработать метод оценивания, который будет учитывать особенности информационной составляющей и позволит оценить защищённости ИР объектов КИИ.

БИБЛИОГРАФИЯ

1. Наказ 04.07.2008 N 112 Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. URL: http://za kon. rada.gov.ua/laws/show/z0690-08.

2. Розпорядження від 6 грудня 2017 р. № 1009-р Про схвалення Концепції створення державної системи захисту критичної інфраструктури. URL: http://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80.

3. Закон Грузии Об информационной безопасности от 5 июня 2012 года №6391-Ic. URL: https://matsne.gov.ge/en/document/download/1679424/3/ru/pdf.

4. Закон Грузии О порядке планирования и координации политики национальной безопасности. URL: https://matsne.gov.ge/en/document/download/2764463/2/ru/pdf.

5. Cybersecurity Strategy of Georgia 2017 -2018. URL: http://csbd. gov.ge/doc /Cybersecurity%20Strategy_eng.pdf.

6. NCIIPC Framework for Evaluating Cyber Security in Critical Information Infrastructure, version 1. URL: http://nciipc.gov.in/documents/Evaluating_ Cyber_ Security_Framework.pdf.

7. Методические рекомендации по разработке планов повышения защищенности критически важных объектов, территорий субъектов Российской Федерации и муниципальных образований (утв. МЧС России 28 декабря 2011 г. N 2-4-60-21-14). URL: http://base.garant.ru/71408274/.

8. Невойт Я.В. «Метод оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеці»: дис. канд. техн. наук. ДУТ, Київ, 2016. URL: http://www.dut.edu.ua/uloads/ p_1539_26349739.pdf.

9. Янчук В.О «Методика оцінювання стану захисту інформації локальних об'єктів системи електронного врядування». URL: http://academy. gov.ua/ej/ej11/txts/10ivoseu.pdf.

10. Бурькова Е.В. «Задача оценки защищенности информационных систем персональных данных». *Вестник Чувашского университета*. 2016. № 1. С. 112–118.

11. Евсеев С. П. «Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины». *Безпека інформації*. 2016. Т. 22, № 3. С. 297-309.

12. Голобородько М.Ю, Курченко О.А., Кирись О.С. «Методи числової оцінки рівня захищеності інформації у сегменті корпоративної інформаційної системи». *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*, №2(51), 2014р. С. 137-139.

13. В. Сидоренко, А. Положенцев, С. Гнатюк, «Метод оцінювання рівня кібербезпеки галузі критичної інформаційної інфраструктури держави», *Вісник інженерної академії України*, вип. 4, с. 142-148, 2017.

14. Soon-Tai Park, Jong-Whoi Shin, Bog-Ki Min, Ik-Sub Lee, Gang-Shin Lee and Jae-Il Lee, « Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection)», *World Academy of Science, Engineering and Technology International Journal of Information and Communication Engineering,* Vol:2, No:2, 2008, p.446-449.

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 87-94 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

OVERALL REVIEW OF THE AUTHENTICATION PROBLEM IN THE CLOUD SERVICES

Oksiiuk O[1]., Vialkova V[2]. Chaikovska V[3]., Shestak Y.[4]
1-4 Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ABSTRACT. This article presents the secure authentication in cloud technologies and determining vulnerabilities in the algorithms. The research performs the development direction of the authentication protocols and their analysis. It is needed to identify the legislation and standards in the research field. After that, the threats investigation is the most crucial part, as we need to protect all vulnerable elements in the authentication process. The importance of such research is the rapid growth of the cloud technology industry. The result is offering new methods in the authentication algorithms.

Keywords: authentication, protocols, confidential information, secure connection, information security, cloud services, cybersecurity, threats, data storage, legislation, authentication algorithms, data protection.

1. Introduction

The term cloud services is a full category that encompasses the myriad IT cloud-based resources provided over the internet. Cloud-based means giving different services over the internet and all you need for accessing them is a connection to the internet and device that can do it.

The usage of cloud services has become associated with everyday cloud products, such as software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Examples of cloud services include online data storage (like google drive) and backup solutions, Web-based e-mail services (like Outlook Mail on the Web), database processing (like some tools in SPSS), managed technical support services and more.

As you can see, there are a lot of tools that cloud services can offer. That is why more companies and people at all decide to use them. The most challenging question here is protection the authentication process. The pieces of evidence of this are the papers written by different scientists around the globe like Deepanshu Goyal, M. Bala Krishna “Secure framework for data access using Location-based service in Mobile Cloud Computing”, J. Angela Jennifa Sujana, T. Revathi “Ensuring Privacy in Data Storage as a Service for Educational Institution in Cloud Computing”; Mr. Santosh P. Jadhav, Prof. B. R. Nandwalkar “Efficient Cloud Computing with Secure Data Storage using AES”; Dimitrios Zissis, Dimitrios Lekkas “Addressing cloud computing security issues”; H A Dinesha, V K Agrawal “Multi-level authentication technique for accessing cloud services”; Slawomir Grzonkowski, Peter M. Corcoran, Thomas Coughlin “Security analysis of authentication protocols for next-generation mobile and CE cloud services Sign In or Purchase” and more.

The authentication into the cloud services has the following features:

- Every company will have its identity management system to control access to information and cloud services. Cloud providers either integrate the customer’s identity management system into their infrastructure, using federation or SSO technology or a biometric-based identification system or provide an identity management system of their own.
- CloudID provides privacy maintaining cloud-based biometric validation. It leads the users' confidential information to their biometrics and stores it in an encrypted appearance. Making use of a searchable encryption technique, biometric identification is performed in the encrypted domain to ensure that the cloud provider or attackers do not get access to any sensitive data.

- Data confidentiality is the attribute that data contents are not accessible or disclosed to unauthorized users. Outsourced information is stored in a cloud and out of the owners' direct control. Only authorized users can access the sensitive data while others, including CSPs, should not gain any information about the data. Meanwhile, data owners expect to utilize cloud data services fully.
- Access controllability means that a data owner can perform the selective restriction of access to his data outsourced to the cloud. Authorized users can be authorized by the owner to access the data and others cannot reach it without permission. Only the owner in untrusted cloud environments must control the access authorization.
- Data integrity demands to maintain and assure the accuracy and fullness of data. A data owner expects that their data stored in the clouds has to be stored correctly and reliably. It means that the data must not illegally interfere, somehow modified, consciously deleted, or maliciously faked. If any undesirable operations damage or remove the data, the user should be able to identify if something went wrong.

The resulting methods allow minimizing the risks in the authentication process. It shows that topic of research devoted to the vulnerabilities in the authentication algorithms to the cloud services is urgent.

The results reveal the importance of the law background in the information security at the national level. It has demonstrated the need for secure connection to add more methods of the authentication. In addition, users have to use the most convenient tool for the accessing on their devices.

2. Formulation of the problem

This paper presents the secure authentication in cloud technologies and determining the vulnerabilities in the algorithms. The research performs the development direction of the authentication protocols and their analysis.

The object of the study is the threats of the authentication in cloud technologies. The subject of research is vulnerabilities in the authentication algorithm. The analysis based on the comparison of the protocol, synthesis of the main features and reviewing the results.

It was determined the following tasks for achieving the goal:

- Analysis of the legislation in cloud services security.
- Identifying the threats of the authentication process to the clouds.
- Study of the vulnerabilities in the current authentication protocols.

3. Data protection law in the cloud services

It is essential to find a way to settle all aspects of the dispute that can be everywhere. We cannot avoid this regulation in the cloud technologies, as a lot of people decide to use this storage method instead of hard drives.

We can find in Ukrainian law only general thesis that international society requires. Here it is the law about information (02.10.1992), about the State Service for Special Communications and Information Protection of Ukraine (23.02.2006), about information protection in the information and telecommunication systems, about government secrets, etc. If we analyze all these documents, we can find only general terms that can protect nobody. Such tendency creates an excellent place for cybercrimes.

However, such situation has a place not only in Ukraine, but it also has a place in more countries that it should be.

Much can be learned from countries that have been able to reduce threats in clouds. Such states are the UK, US, Germany, and Japan.

The legislation creates a legal a basic structure underlying a concept to resolve the progressively frequent severe disagreements between the United States and foreign countries over access to outside data stored. The fundamental legitimate question is that of external jurisdiction which the legal system of one country can extend to another country. Examples of such areas include terrorism and piracy.

Policy in this area tends to focus on moving government agencies to cloud services. One example is the Cloud First Initiative, launched by former US government CIO Vivek Kundra, which aimed to cut waste and increase efficiencies within the US federal government's technology services by reducing government IT expenditures by US$4 billion dollars over the next two years. As one result of this initiative, the General Services Administration, the federal government's procurement agency, has developed some resources to assist government agencies in procuring cloud services. More recently, President Trump recently signed an Executive Order on cybersecurity mandating that federal systems move to the cloud.

The act amended US law to make clear that law enforcement warrants can apply to data that the United States based technology corporations have stored anywhere in the world. It also gives those enterprises the right to challenge these licenses based on the privacy laws where the data are stored.

British data protection laws make the UK one of the best places in the world to adopt cloud computing services, according to new research. The yearly ranking is designed to help countries find an equivalent for their current policies and identify the following levels for increasing adoption of cloud computing. Researchers referenced Ministers' decision to incorporate the EU's General Data Protection Regulation into UK law as a critical reason for the UK rising the rankings.

Researchers referenced Ministers' decision to incorporate the EU's General Data Protection Regulation into UK law as a critical reason for the UK rising the rankings.

The German authorities have recently developed specific regulations on IT security requirements. According to them [Directive 2015/2366/EU] the basis of the technical standards on authentication and communication developed by European Banking Association (EBA) under section 98 of Directive 2015/2366/EU:

"The personalised security credentials used for secure customer authentication by the payment service user or by the payment initiation service provider are usually those issued by the account servicing payment service providers. Payment initiation service providers do not necessarily enter into a contractual relationship with the account servicing payment service providers and, regardless of the business model used by the payment initiation service providers, the account servicing payment service providers should make it possible for payment initiation service providers to rely on the authentication procedures provided by the account servicing payments service providers to initiate a specific payment on behalf of the payer."

This statement concerns only banking, but it can be implemented for cloud services.

To sum up, we can see the tendency of regulation the authentication process in the banking, but not the cloud services. That is why it is needed to implement the best solutions to protect user's theft while the authentication process into the clouds.

4. Authentication process threats in the cloud technologies

The authentication process becomes not useful in case of users' lost, forgeting or damaging their authentication key, which depends on the authentication method. It has a significant impact on the safety of the authentication system in the clouds.

CSA asked experts to compile professional opinions on the most significant security issues within cloud services [CSA]. The experts think that the primary reason for the lousy tendency for cracking the cloud services is higher strategic decisions by executives in cloud adoption.

According to the report, the main threats are data cracking, lack of access management, insiders, misusing the cloud services, vulnerabilities in the shared technologies. A data violation might be the primary objective of a targeted attack or just the result of human error, application vulnerabilities, or poor security practices that are used in the system. The enterprises' cloud-based data may have the material or monetary worth to different parties for different reasons as well.

A data violation is an incident where confidential information is broken, viewed, stolen or used by an unauthorized user.

Cloud service providers reveal a set of application programming interfaces (APIs) that customers use to maintain control over the cloud technologies and interact with them. The security of these underlying APIs determines the safety and accessibility of main cloud services. If providers are not careful, an attacker with access to the key can cause a denial-of-service or rack up fees on behalf of the victim [Insecure API]. They need to be done or planned with a protecting purpose against the accidental and malicious make an effort to achieve the circumvent policy.

System vulnerabilities mean dupable bugs in programs that attackers can use to gain access to the computer system in motivation to steal the data, taking control over the network or interrupting service operations. Weaknesses over the components of the operating system like Kernel, system libraries and application tools that put the security at high risk.

Everybody who connected to the cloud service management system can read, modify, and delete data; issue control level and management operations; monitoring the data in transit or release ransomware that is convinced to go from a reliable source. In the end, insufficient identity, credential, or critical controlling can enable unauthorized access to data and possible extremely unfortunate damages to all parties.

Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still are used and successfully here. Cloud solutions are no exception. These types of stealing are widely used here as well. If an attacker gains access to the user's credentials, they can monitor the activities and transactions in the account, change data, misuse confidential information and redirect the customer to unlawful web-pages.

All types of attack can be successful because of the weak authentication algorithm. Authentication protocols differ from the protection methods they provide against assaults [Hickey K. Dark cloud].

The insider threat is a real potential risk, as it can be anyone who works for the company. An insider, such as an auditor, can access potentially sensitive information. An everyday basis is attacking the employer's cloud applications and functions. Revenge might motivate these people. Overall, the 'inside job' is responsible for most cloud computing security woes. Enterprises have to become proactive in finding solutions to their security threats to protect their sensitive information [INSIDER THREATS].

Data stored in the clouds can be lost for reasons other than cyber attacks. The data can be physically removed from the storage server or building, where this server is located, can be destroyed by earthquake, fire, etc. However, these type of catastrophes can be prevented, and protection methods have to be implemented.

Enterprises often struggle with identity management as they try to set aside permissions appropriate to the employees' job. The crucial mistake is that they forget to remove user access when a job position changes or a user leaves the organization at all. Such behavior can lead to different bad consequences.

One more critical threat is lack of diligence. It is about the confirmation of the information that has been submitted to the service providers and the validation of the given back information by the services providers. It creates with all benefits a lot of risks [CLOUD SERVICE VENDOR].

As well as ransomware attacks are successful, so are Denial-of-service (DoS) attacks. More cloud services come into usage, the more DDoS attacks on them will become more ordinary and daily [As cloud use grows].

In conclusion, we can see that many threats caused a lot of risks. Some of them are data losing, damaging the buildings, appearing the insiders, misusing the confidential data, the personal discredit, cracking the network, unauthorized transactions. And based on these risks, it is possible to find the best method to protect the authentication process in the cloud services.

5. Methods of protection and authentication protocols

According to the identified risks, it is crucial to determine the methods of protection.

Considering that cloud service is using over the Internet, the most proper method is having the user turning extra to the traditional username and password pair. From this point, it is recommended to use one or more of the techniques as:

- Physical token;
- Digital certificate;
- Biometry;
- SMS password confirmation.

Encryption is a well-known technology that can keep under control the access, and its use has been demonstrated its ability to provide data useless to those who do not have the key. It is exemplified by the uselessness of encrypted information and hashed passwords to cybercriminals. The cryptography is an excellent power in protection data, and it is standardized [The Impact of a Data Breach].

Multifactor authentication systems – smartcard, one-time password (OTP), and phone authentication. This form of authentication helps address password theft, where stolen passwords enable access to resources without user permission. Password theft can manifest in common network attacks, such as “pass the hash.”

The Cloud Security Alliance has developed the most effective ways of the cloud protections. Here are some methods [DEVELOPMENT OF AUTHENTICATION PROTOCOLS]:

1. Data storage. Encryption

Encryption is one of the most effective ways to protect data. The provider gives access to the data must encrypt the customer information stored in the data center, as well as, if not necessary, irrevocably deleted.

2. Data protection during transmission

Encrypted data during transmission should be available only after authentication. Data cannot be read or modified, even if accessed through unreliable nodes. Such technologies are quite known, providers have long used algorithms and reliable protocols AES, TLS, IPsec.

3. Authentication

Authentication - password protection. For higher reliability, tokens and certificates are often used.

4. Isolation of users

Using an individual virtual machine and a virtual network. Virtual networks must be deployed using technologies such as VPN, VLAN, and VPLS.

Credentials and cryptographic keys must not be implanted in the source code or are given a share in public facing repositories such as GitHub because there is a significant chance of the misuse. Keys need to be appropriately hidden and secured; that is why a well-secured public key infrastructure (PKI) is required in order to ensure key-management activities are accomplished.

As the lack of diligence is a significant threat to the cloud solutions, there are some points to fix the situation [CLOUD SERVICE VENDOR]:

- Asked to prove the cloud service provide their reliability using the free trial version and ceasing from storing essential data.
- Reading the feedback from customers of the chosen service provider.
- Visit service provider site
- Regular providing the audits (compliance and security)

As for Denial-of-Service attacks, the only solution is to use automated tools to spot and defend the core cloud technology from this type of attacks. Further, the tools will become better, that will help to prevent such threats.

Now, modified versions of old protocols are used around the world, which makes it possible to improve the algorithms already developed and make them more cryptoresistant.

In recent years, enterprises want to get convenient and flexible information infrastructure through the cloud computing. However, information security issue of cloud computing has been one of the thresholds for the enterprise to adopt cloud computing. The enterprises began to deploy a private cloud to solve the cloud security issues. SSL virtual private network (VPN) gateway is a solution for the enterprise to access private cloud services securely. There are two main types of SSL VPN gateway, i.e., SSL Portal VPN and SSL Tunnel VPN.

IT administrators may integrate existing account of active directory or lightweight directory access protocol (LDAP) to SSL VPN gateway. Therefore, IT administrators can easily configure SSL VPN gateway to control the different groups of users which can use what kind of resources and applications. Besides, SSL VPN gateway provides a mobile one-time password (MOTP) to enhance security authentication.

Here are some methods of protection the cloud attacks while implementation of the protocols:

- request-response, timestamps, random numbers, identifiers, digital signatures have to be used;
- the administrator must establish the result of the authentication, e.g., exchange secret session key will be used for the connection with the user;
- the new authentication must be initiated during the reconnection.

As we are passing our data through the internet, we need to check that our data is secure not only in storage but also when it is transmitted through different channels. The network security parameters should be considered to achieve the goal. Firewall and gateways should be set up appropriately to avoid hackers entering and stealing valid data. We also need to make use of secure communicating layers and protocols to prevent data loss by violator. The expert can use the secure socket layer for communicating. Other options include HTTP over SSL which is called HTTPS. Another alternative to HTTPS is secure HTTP (SHTTP). Depending on what kind of security mechanism we need to deploy for our application, we should decide on the communication protocols considering its pros and cons.

Here are some methods of protection the cloud attacks while implementation of the protocols:

- request-response, timestamps, random numbers, identifiers, digital signatures have to be used;
- the administrator must establish the result of the authentication, e.g., exchange secret session key will be used for the connection with the user;
- the new authentication must be initiated during the reconnection.

There are other methods of authentication:

1. Server SSH/RDP proxy.
2. Two-factor authentication.
3. Kerberos.
4. LDAP and SAML.
5. Single Sign-On.

Finally, it has demonstrated the need for secure connection to add more methods of the authentication. Besides, users have to use the most convenient tool for the accessing on their devices.

6. Approbation of research results

The results can be used for creating new authentication algorithms. That consider all strong sides in the current authentication solutions and strengthen the weak parties.

The research shows a massive number of vulnerabilities, and with the development of the cloud, it is clear that weaknesses will increase.

7. Conclusions

We can see the tendency of regulation the authentication process in the banking, but not the cloud services. That is why it is needed to implement the best solutions to protect user's theft while the authentication process into the clouds.

The research has demonstrated the need for secure connection to add more methods of the authentication. Besides, users have to use the most convenient tool for the accessing on their devices.

Frist, it is easily perceived that simple password authentication should be supplemented in other ways. Second, with the advent of a large number of devices, users need to use a reliable way to authenticate these devices. Finally, each user, developer, and provider have to care about the security of the data they are using.

In this article, the method of protection must contain not only practical usage but consider all weaknesses of the platform – the cloud solutions. The research shows that there are o lot of vulnerabilities that have to be fixed. Since the hackers for unauthorized access to the stored data can use them.

REFERENCES

1. Cloud Standards Customer Council. Security for Cloud Computing Ten Steps to Ensure Success Version 2.0. – 2015. – 35p.
2. Filimoshin V. Yu. Davletkireyeva l.z.: Secure authentication without using https. - International Journal of Open Information Technologies (2017) 7, 17-23.
3. Hickey K. Dark cloud: Study finds security risks in virtualization / Kathleen Hickey // Technology, Tools and Tactics for Public Sector IT. - 2010 - № 3 — p. 3-5
4. Khazhieva A. S.: Principles of information protection in the cloud. - Achievements of science and education (2017) 6(19), 14-16.
5. Lozhnikov P., Sulavko A., Buraya E., Pisarenko V.: Authentication of Computer Users in Real-Time by Generating Bit Sequences Based on Keyboard Handwriting and Face Features. - questions of cyber security (2017) 3(21), 24-34.
6. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing / National Institute of Standards and Technology / Rebecca M. Blank. – Gaithersburg: NIST, 2011. – 286 p.
7. Vishniakou U.A., Ghondagh Saz M.M.: Authentification models in cloud computing for mobile applications with intellectual support of choice. – Doklady BGUIR. - Electronic resource: https://www.bsuir.by/m/12_104571_1_112204.pdf#page=82, 2017.
8. Winkler J.R. Securing the Cloud. 1st Edition / Vic (J.R.) Winkler. - US : Syngress, 2011. - 314p.
9. Cloud Standards Customer Council. Security for Cloud Computing Ten Steps to En-sure Success Version 2.0. – 2015. – 35p.
10. Filimoshin V. Yu. Davletkireyeva l.z.: Secure authentication without using https. - In-ternational Journal of Open Information Technologies (2017) 7, 17-23.
11. Hickey K. Dark cloud: Study finds security risks in virtualization / Kathleen Hickey // Technology, Tools and Tactics for Public Sector IT. - 2010 - № 3 — p. 3-5.

12. Khazhieva A. S.: Principles of information protection in the cloud. - Achievements of science and education (2017) 6(19), 14-16.
13. Lozhnikov P., Sulavko A., Buraya E., Pisarenko V.: Authentication of Computer Users in Real-Time by Generating Bit Sequences Based on Keyboard Handwriting and Face Features. - questions of cyber security (2017) 3(21), 24-34.
14. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing / National In-stitute of Standards and Technology / Rebecca M. Blank. – Gaithersburg: NIST, 2011. – 286 p.
15. Vishniakou U.A., Ghondagh Saz M.M.: Authentification models in cloud computing for mobile applications with intellectual support of choice. – Doklady BGUIR. - Elec-tronic resource: https://www.bsuir.by/m/12_104571_1_112204.pdf#page=82, 2017.
16. Winkler J.R. Securing the Cloud. 1st Edition / Vic (J.R.) Winkler. - US : Syngress, 2011. - 314p.
17. Douglas Paris-White. Five features of information security every cloud platform should provide. - IBM Cloud Blog, February 6, 2018 – [access: https://www.ibm.com/blogs/bluemix/2018/02/five-fundamentals-cloud-security/]
18. Eric O'Neill. Why the future of cybersecurity is in the cloud? - Eric O'Neill. - 27 April 2018 – [access: https://www.cloudcomputing-news.net/news/2018/apr/27/why-future-cybersecurity-cloud/]
19. ICT. Online Authentication Threats and Attacks. - ICT.govt.nz. Authentication standards - 21/09/2016
20. Krutz, Ronald L. and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. - Indianapolis, IN: Wiley, 2010. - 179p.
21. Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview. – IBM Security, June 2017 – 34 p.

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 95-103 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

MODEL-BASED ANALYSIS OF THE ESTIMATION OF INTEGRAL LEVEL OF SECURITY OF THE INFORMATION SYSTEM

Hnatiienko Hryhorii[1], Vialkova V[2].
1-2 Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ABSTRACT. Providing the functionality of the security system of any modern information system is relevant in every conceivable environment and in all areas of human life. Solving the problems, which encountered in relation to protection of the information, is a complex process, which is based on the system method that is used to create an integrated system of protection information. For developing a model of information security, we will assume that the intended purpose of the system consists of the sequential or parallel execution of tasks that provides the reliable functioning of all elements of the system. It suggested raising of task and different models of evaluation of informative strength of the system security. For the decision of task application of methods of theory of decision-making and artificial intelligence is envisaged

Keywords: information system, security level, integral security level

The problem of providing information security is important and currently central due to the intensive development of technologies and increased competition in market environment and international relations. Providing the functionality of the security system of any modern information system is relevant in every conceivable environment and in all areas of human life [1]. Solving the problems, which encountered in relation to protection of the information, is a complex process, which is based on the system method that is used to create an integrated system of protection information [1]. The quality of the functioning of the information security system depends on the quality of the functioning of the system elements. Therefore, model-based analysis of the integral level of the security of the information system is an actual strand of research and also an assessment of the quality of the functioning of the system elements, which is a reliable mechanism for determining the level of security of the information system generally .

For research investigation of the functioning of systems such models as theoretically-gaming, probabilistic, graph and matrix models are traditionally used [2]. For the assessment of the quality of the functioning of a complex information system, we will apply the tasks of collective ordering of objects, which is a wide class variety of tasks for modeling of practical situations in various subject areas [3]. Among the tasks of the adoption of decisions , the problem of organizing objects is distinguished by a large number of specific applications and is relevant as ever .

It should be reminded that a complex information system consists of hundreds of elements that complete thousands of tasks and can have different nature: for example,

providing information security of the system, maintaining the survivability of the information system, timely diagnosis of economic security, determining the level of physical security, a map of business processes organization, algorithms of interaction of some hierarchical system, etc.

Problem definition

For developing a model of information security, we will assume that the intended purpose of the system consists of the sequential or parallel execution of tasks that provides the reliable functioning of all elements of the system. Let us suppose that there is the resultant (aggregated, collective) seriation n of tasks $R^* = (a_{i_1},...,a_{i_n})$, $i_j \in I = \{1,...,n\}$, $j \in I$, which is based on some logic conclusions that characterizes the processes of functioning of some information system. This seriation R^* is based on the individual ordering of tasks that are accomplished k by the elements of the system $R^i = (a_{1_i},...,a_{n_i})$, $i \in J = \{1,...,k\}$, where $n_i, i \in J, -$ are the numbers of tasks in the individual ordering that are accomplished by the $i-$ elements of the system. Let us denote that $A^i, i \in J$, -subset of tasks that are accomplished by the $j-$ element of the system.

Considering that R^* represents the logic of solving a collective problem, tasks in the individual segregation could have indices , which are out of phase with the positive integers .For example, tasks $a_2 \succ a_5 \approx a_1 \succ a_6$ have conditional segregation R^1, at the same time tasks $a_4 \succ a_3 \approx a_7$ have conditional segregation R^2.The enumeration of tasks of the comlex of the information security emphasizes on the sequence of tasks in the functioning of the system.In the event if it is indicated that ratio in tasks is when $a_i \succ a_j$, $i, j \in J$, this means that in order for the system to function properly, these tasks must be realized consistently. In the event if $a_i \approx a_j$, $i, j \in J$, the tasks of ensuring the qualitative functioning of the system could be realized in a parallel way.

For this purpose ,tasks which are realized by various elements of the system and are not duplicated, i.e $n = \sum_{i \in J} n_i$ –i.e each task in the system is unique and each task in the segregation R^* appears only one time : $A^{i_1} \cap A^{i_2} = \varnothing, i_1, i_2 \in J$, where $\varnothing -$ the empty set.

Each task of providing qualitative and secure functioning of the information system from the set of tasks $A = \{a_1,...a_n\}$ is characterized by two parameters:

c_i^0 – the face value of fulfilment or nominal demand for resource , $i \in I$;

t_i^0 – the nominal time of fulfilment , $i \in I$.

The nominal resource requirements, particularly , price and time of completing the task, are the same values that are acquired during completing information security task routinely- - when it is realized by a system element that completes the task according to the a priori approved staffing schedule and none of the elements of the system is capable of completing this task better,besides it. For specific applications, the maintenance of a reliable operation of the information system could have additional options, but we will take in account this region under consideration according this work .

During the realization of $i-$ task $j-$ component of the information system ,it is known:

c_i^j – the real price of this task, $i \in I,\ j \in J$;

t_i^j – the real time of completing the task, $i \in I,\ j \in J$.

Each component of system routinely complete the tasks ,which are estimated for it and has limited capabilities for completing all of its subset of tasks:

$$\sum_{a_i^j \in A^j} c_i^j = C^j, \quad j \in J, \tag{1}$$

$$\sum_{a_i^j \in A^j} t_i^j = T, \quad \text{for } \forall j, j \in J. \tag{2}$$

The remarkable thing is that for some tasks it could be some restrictions,

$$\sum_{a_i^j \in A^j} t_i^j = T^j, \quad j \in J,$$

when for each element of the system or group of elements are applied limits on resources for the time of completing the task. When approaching these limits, the quality of providing information security of any element of the system is significantly reduced and appear threats to the information security of the entire system.

Restrictions (1) are the appraisement of completing the tasks as an element of the information system - an employee's analogue in the simulation of business processes, and restrictions (2) are limited by time-an analogue of the monthly norms of the number of working time in the functioning of organizations.

During the fulfilment of normative tasks, determined by the nominal tactical and technical characteristics of the information security system, the needs of the system and its elements in resources (1) - (2) are constant, and the quality of the tasks performed by all subsystems and the system as a whole is 100%. In practice, the

providing of such situation requires the usage of substantial resources and in some cases, is unattainable.

Nominal tactical and technical characteristics of the information security system are characterized due to the requirement of a variety of resources, in many organizations the most important of which are:

$\sum_{i=1}^{n} c_i^{0i} = C^0$ – the budget operation of system ,

$\sum_{i=1}^{n} t_i^{0i} = T^0$ – the general demand of time for completing system functions

Due to the fact that tasks are not duplicated, there is no need for direct redundancy.

Redundancy of the ability to complete tasks with different elements of the information system is potential, hidden: the functional moves to another element of the system, when the element, which according to the norm should perform the task, can not do this. But this is due to ancillary charges despite of a limited resource that uses the information security system.

It is necessary to develop a model that will reflect the system's reaction on various types of environmental influences and changes in the status of system elements. In this case, the quality of the functioning of the information security system and its elements should be evaluated, depending on the state of the system elements.

According to [1, 4], the most common methods in the field of information system security are three main methods of protection of the system: formal, static and classification. The assessment of system security is needed to create a mechanism and conditions for prompt response to threats to information security and manifestations of negative trends in the functioning of the system.For this, should be used a set of measures and countermeasures. The increasing of the objectivity and complexity of appraisal facilities of information protection based on the formalization of expert data has a promising future.

Developing a model of decision-making situations for information system security

During the process of functioning in real conditions, the situation described in the statement of the problem, could significantly differ from the normative. For example, in the case of a big organization, there are always employees involved in the information security system, which currently

- are at the hospital;
- are on vacation;
- sent on business trips;
- absent for unknown reasons;
- officially issued rejections;

- dismissed from work for various reasons;
- violate labor discipline and do not observe the order of the day;
- not due to force majeure circumstances;
- undergo adaptation and therefore do not perform qualitatively enough tasks;
- reduce the quality of functioning due to conflict situations;
- insufficiently high-quality work is carried out due to the influence of various factors of demotivation, etc.

For all the reasons stated above we could estimate, heuristic determine the current level of performance of each task and evaluate the quality of each task at the 100 percent scale.

If it happens a temporary or long-term failure of the system element, all functions that must be fulfilled by this element are not fulfilled by the system. For their implementation, it is necessary to make decisions about redistribution of functions or their replacement. For example, in the absence of an element of the system in time, its tasks can be:

- distributed to perform among other elements of the system;
- passed to execute one element of the system;
- ignored as such, without which the information system will not significantly lose its level of functionality.

Model 1. Distribution of tasks between the elements of the system.

Distribution tasks can be carried out only between those elements that can execute the tasks of providing of informative safety, in accordance with their qualification, present certificates and others like that. In this case necessarily it follows to take into account a few features.

At the decision of tasks that are not for the element of the system normative, undoubtedly quality of implementation of these tasks goes down by new elements that intended for temporal implementation of tasks. The level of quality of performance of objective is set individually for every case and can fold, for example, 80%. At a necessity the decision of the system of additional tasks an element, there is a situation of overload of element and that is why quality diminishes:

a) implementation of own normative tasks, for example, to the level of 90-95%;

b) implementation of additional tasks taking into account Heuristic 1.

Cost of resource of kind (1) in case of redistribution of tasks in connection with absence of one of elements of the system, can increase in an interval from 101% to 115% - for the increase of motivation of new elements to execute additional tasks. After taking into account of the features marked higher there is a count of resources that is needed for implementation of tasks of providing of informative safety in new circumstances. Clear that new values will substantially differ from normative. Thus quality of implementation of tasks, and consequently, and quality of functioning of the system will largely differ from ideal 100%.

Model 2. Transmission of tasks of absent element for their implementation by other element of the system.

At the considerable additional loading at the element of the system, that the tasks of absent element passed for implementation, largely go down not only quality of implementation of new tasks but also tasks that he executed normatively to it. In such model it follows to take into account additional features.

At the considerable additional loading on the element of the system, quality of implementation to them of additional tasks falls substantially, for example, after a linear function the parameters of that can be appointed separately for every situation of decision-making.

Loading on the elements of the system can not exceed some set size, for example, 2*T, where T is limitation at times, set by a formula (2).

It follows to weigh such on that a function can not be executed by the new element of the system on a greater percent, than percent of her payment is for every element.

At application of the described features determination of new levels of quality of implementation of tasks and quality of functioning of the system of informative safety comes true on the whole. In addition, there are changes in requirements in resources, that is needed for implementation of tasks that stand before the system, in new terms - at the transmission of all tasks of absent element of the system to other element.

Model 3. Ignoring of tasks, that was executed by the absent element of the system

If it is known that a system element is temporarily absent, and an experienced person understands that there is no urgent need for the task of this element, a temporary moratorium may be made to perform the relevant tasks.

If there is not an element accountable for the performance of autonomous objective, quality of performance of objective falls gradually, during some time. Conformity to law of falling of quality of implementation of tasks can be set separately for every individual case.

If a task for that a performer is not certain is not autonomous, id est, other tasks depend on her implementation, the function of change of quality of implementation of dependent tasks is set separately for every certain situation of decision-making.

A decision-making about ignoring of tasks, that temporally remained without a performer, is very responsible and needs the permanent monitoring from the side of person that makes decision or the inspector appointed by him. At each monitoring iteration, an assessment is made of the change in the quality of the functioning of the information system in accordance with the above-mentioned features.

Calculation of results of evaluation of strength of the informative system security.

After making decision about the redistribution of functions between the elements of the system or their substitution, the new values of resources for the tasks of the system and even qualities of their functioning settle accounts. On the basis of the got values, the function of belonging of levels of quality of functioning of the system to the fuzzy set (0,1) is determined. Going near determination of functions of belonging and algorithms of construction of functions of belonging on the basis of analysis of

frequency of values is driven to works [3, 5]. Id est quality of functioning of the system as a result of application of the described procedure will be characterized the function of belonging to the fuzzy set. In-process [4] it is suggested for realization of estimation of the system of informative safety to apply procedures of unclear expert evaluation of elements of the system that also can be used in future for perfection of model of estimation of informative strength of the system security.

It is thus possible to compare the level of providing of informative safety depending on application of decision about personalization of performance of objective. It maybe also to build functions for the linguistic variables entered a priori with such by an orientation names: "critically possible informative strength security", "risk functioning of the system", "sufficient informative strength security", "high informative strength security" and others like that.

Table of contents of base of knowledge of evaluation of quality of functioning

Practical meaningfulness of offer models will rise considerably, if to give to the person that makes decision, instruments for the evaluation of different variants of decision-making in relation to providing implementations of tasks, that had to be executed by the absent elements of the system. For the use of the described models of evaluation of quality of functioning of the informative system it is necessary to create the base of knowledge with such reference filling:

- interchangeable elements of the system and degrees of their interchangeability at a decision-making about substituting for elements;
- a limit on possibility of implementation or delegation of implementation of tasks, related to the hierarchical copulas in the system;
- a decouplig of tasks in the elements of the system and potential distribution of tasks for critical elements;
- functions of change of capacity of elements of the system at non-normative overloads;
- information about possibilities of duplication of some tasks by the separate elements of the system;
- priority of duplication of tasks by a few elements - in case of possibility and necessity;
- possibilities of temporal moratorium on implementation of some tasks;
- formulas of count of loading for the elements of the system;
- plugged of tasks in processes, criticism of implementation of some tasks, estimation of loss of level of quality of functioning of the system;
- an estimation of decline of quality of functioning of elements in default of co-ordination from the side of elements that carry out a management in the hierarchical system;
- taking into account of factors of falling of quality of functioning of the system: insufficient competence of element, that temporally executes a task, or overload of element by additional tasks.

Possibilities of application of different classes of models to the evaluation of informative strength of the system security

On the first stage of design the elements of the system can answer a non-orientable count - the fact of presence of tasks is specified only, without the gone into detail description of entrances-exits.

For the systems, that execute tasks among that there is a substantial order of implementation, it is necessary to apply the models of strict segregation of tasks, described in this work.

If the parallel processes of implementation of tasks are designed, then there can be the applied models of unstrict segregation - for the deeper working out in detail.

When there are cycles in intertask communication, it is necessary to apply the individual matrices of sequence of implementation of tasks - in such cases a resulting matrix of pair arrangement of tasks will be block-diagonal and substantially rarefied.

The metrical matrix of pair arrangement of tasks is used in the cases when substantial is pointing of terms between the offensive of events or beginning of implementation of tasks - for example at description of diagram of Gant with the help of matrices.

If these terms of implementation of tasks are unclear, then for the design of such systems there can be the applied matrices of pair arrangement of tasks with elements as functions of belonging.

The prospects of increase of adequacy of design of informative strength of the system security

For more complete taking into account of features of the real systems must be complicated the described mathematical model. In particular, it can take place by taking into account of such factors:

- an appropriation to the elements of the system of grades, determination of subordination between elements;
- establishing hierarchical connections between the elements of the system and determination of levels of influence of one element on other or absence of such influence;
- determination of a priori priority of tasks regardless of their ponderability from the point of view of cost or term of implementation:
- taking into account of coefficients of competence of elements of the system;
- an increase of working out in detail and level of model adequacy by description of sub-tasks; it is description of processes that set intercommunication between tasks and sub-tasks.

Directions of further researches

On the basis of the described approach the new raising of tasks and certain new going can be worked out near the increase of design adequacy:

- a priori evaluation of reliability of functioning of the system in the safe mode;
- determination of borders of decline of margin of safety of the system, estimation of threats of her to informative safety;

- an estimation of possible level of decline of informative safety of functioning of elements of the system and level of implementation of tasks;
- taking into account of presence or absence of connections between tasks: to influence of task on quality of functioning of other tasks;
- a decision of optimization tasks of prognostication of quality of functioning of the system, cost of providing of this quality and calculation of possible charges of time;
- proceeding in AQL of functioning of the system on leaving from the line-up of a few her elements: determination of necessary operating conditions.

Conclusions

It suggested raising of task and different models of evaluation of informative strength of the system security. For the decision of task application of methods of theory of decision-making and artificial intelligence is envisaged. The prospects of design the brought class over of tasks and application of new methods are certain for the increase of adequacy of models to the real informative systems.

References:

1.Oksiyuk OH, Shestak Y. V. Analysis of modern methodologies and methods for assessing the security of information systems //Scientific Proceeding of Ukrainian Research Institute of Communication. – 2015. - № 4. – P. 17 – 23.

2. A.G. Dodonov, D.V. Lande. Vitality information systems. - K .: Science Dumka, 2011. - 256 p.

3. G.M. Gnatyenko, V. . Snituk. Expert tehnologies of making decisions – K .: Maklaut, 2008. - 444 p.

4. Oksiyuk A.G., Shestak Y.V., Ogbu O.D. Building a Safe Infrastructure as a Need for Survival // Bulletin of the National Technical University "KhPI". Collection of scientific works. Series: Mechanic-technological systems and complexes. - 2016 - №50. - P.112-117.

5. Gnatyenko G.M. Algorithms for determining the membership function by analyzing the frequency of values // Proceedings of the III-th international school-seminar "Theory of decision-making", Uzhhorod, 2006. - P. 32-34.

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 104-110 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

CRYPTOCURRENCY USE IN MEDICAL TOURISM

Mikhael Barkan, Natan Tapliashvili

Medical Tourism Centre

ABSTRACT: Currently a cryptocurrency comes to replace traditional money that the state issues. This means of payment is already gaining momentum in use in the developed countries of the world. Since the healthcare sector is one of the most important for humanity, and medical tourism is at the peak of development under the influence of globalization processes, it becomes very important to improve and introduce new technologies not only at the stage of diagnosis and treatment, but also payment for services. Therefore, it is important to analyze and predict the development of a new currency in order to recognize it as a global means of payment.

Today, the global medical services market has emerged with its specific structure - medical management, accrediting bodies, medical tourism agencies, tour operators, lawyers specializing in this field, etc. Medical tourism forced not only the patients, but also the doctors to treat the organization of the medical care system in a new way. The motto of modern medicine "Patients Without Borders!" is truly justified. After not being able to solve a health problem, the patient chooses a country, a medical or health institution, and even a specific specialist who can offer the necessary examination, treatment or rehabilitation at his own discretion.

The main factors affecting the rapid growth of a relatively new industry are the process of globalization, the development of the health system of individual countries, technological progress, and the development of information technology. Bitcoin and modern medicine have much more in common than it might seem at first glance. Since most countries have a patient's statutory confidentiality right, the medical record must contain a minimum of patient data and access to it must be limited.

However, the use of a credit card as the most popular means of payment, especially in a foreign country, leads to the fact that the bank receives information about the provision of medical services to its client. Moreover, the bank is allowed to find out the details of the services provided in the case of checking the validity of the transaction. This entails consequences, as the patient's personal information becomes available to third parties. In the case of using Bitcoin, no medical information can be transferred to third parties, respectively, medical secrecy will indeed remain confidential.

Today the market of so-called "virtual" or "electronic" money is overflowing with various cryptocurrencies. It functions successfully and makes it possible to analyze the dynamics of cost, supply and demand of about 90-100 different cryptocurrencies.

The main advantage of virtual currency is decentralization, as well as the fact that all involving operations are anonymous. An important aspect that affects the rapid development of cryptocurrency is the lack of a center that regulate the cryptocurrency and the way it is emitted. The cryptocurrency emission is called "mining" and meaning that the computers of users, who are located in different parts of the planet, are installed with special software that generates a unique character set that forms the cryptocurrency. For example, a Bitcoin address looks like

1DSrfJdB2AnWaFNgSbv3MZC2m74996JafV. It consists of a string of letters and numbers, starting with "1". The Bitcoin network is based on the block chain technology, which is a public register that stores data on all transactions of the system. These transactions are protected by digital signatures of users who participate in the network, who produce bitcoins or carry out any operations with them. In this case, the branching of the process of creating and distributing bitcoins ensures their security.

Trading transactions with cryptocurrencies are conducted only in digital format, and sales transactions can be made through online exchanges (for example, BTC-E). Cryptocurrency can be exchanged for the main currencies of the world, using special exchange points in online networks (WebMoney) or by means a broker in Forex (FXOpen). Cryptocurrency can be obtained by means of accepting payment for the goods or provided , or the purchase directly from another owner. The latter option is the most profitable, since it does not have commission inherent in the exchange office. Bitcoins are similar to electronic money, but it applies the principles of complete anonymity, lack of control and limited release that distinguishes it from the operation of electronic payment systems.

Cryptocurrency is an alternative expression of the usual currency and has several advantages:

1) Operations with cryptocurrency are anonymous and confidential. All information about transaction is encrypted in the set of character; personal data is not attached to the cryptocurrency wallet;

2) Each cryptocurrency unit has a unique code protected from forgery;

3) The cryptocurrency is decentralized, it does not have a control center that is why the founder of digital money or any financial institution cannot influence its existence. Rate and operations are fully regulated by e-wallet users;

4) The cryptocurrency is not integrated to any of the banks, which significantly reduces the size of the commission for carrying out operations. The cost of commission is usually the cost spent for energy resources on the transaction;

5) The absence of binding to banks contributes to a significant reduction in the time spent on performing cryptocurrency operations;

6) Operations are carried out directly between the owners of electronic wallets, which contributes to increasing the speed of operations and reducing the commission;

7) The emission of most types of cryptocurrency has a maximum threshold. This is due to the restriction of all possible combinations of symbols that form each new unit of cryptocurrency. This fact contributes to the reduction of unjustified money supply in circulation and lower inflation. “

Bitcoin is the first and most expensive cryptocurrency. The merger of the words “bit” (computer memory unit) and “coin” (piece of money) forms the term “bitcoin”. Despite the fact that at the beginning of its development, Bitcoin was a local cryptocurrency, which was used only by a limited number of people (its founders and persons associated with them), in a few years it turned into a world-class system. Today, in addition to exchanges, exchangers and Internet resources, some shops and service centers carry out bitcoin operations. It accepted in many restaurants and hotels in different countries around the world. There are even cases of salary payments to US civil servants in bitcoins. In some Asian countries, bitcoins are used as an

alternative to bank accounts and plastic cards, since banking services in these countries are quite expensive.

The development path of Bitcoin was not smooth. Bitcoin rate is very volatile, look at its dynamics in Fig. 1.

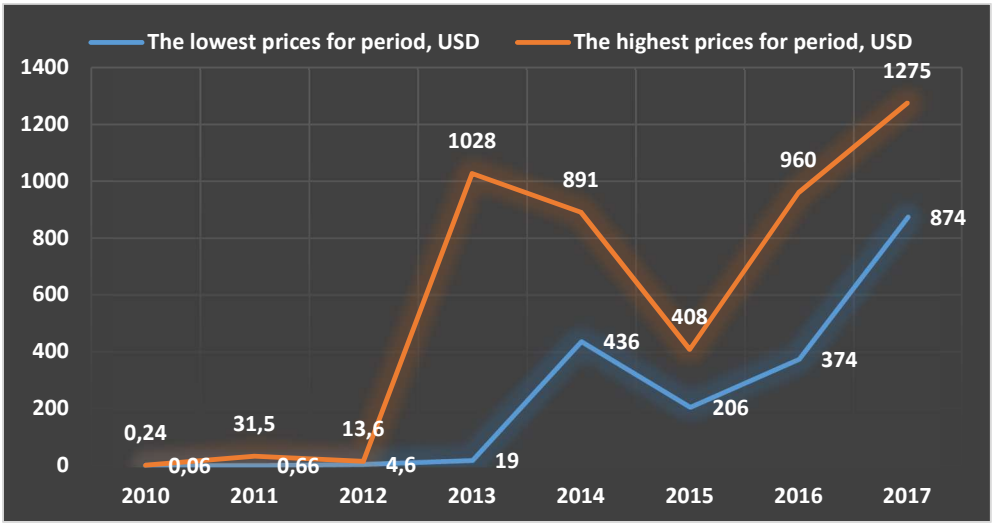


Fig. 1. Dynamics of the dollar to bitcoin 2010-2017

In fig. 1, we can see the best price for buying and selling bitcoin for a certain period (curve 1 - the lowest prices, curve 2 - the highest prices). After analyzing this chart, we can understand that the rate fluctuations occur very sharply, for example, if in June 2013 the purchase of one bitcoin cost $ 19, then in November of this year, the rate was 1028 USD for one bitcoin. That is, for 1 year the bitcoin rate has grown more than 54 times. Similarly, recessions occur, for example, in 2014, the rate went down: June - 891 USD, November - 436 USD for one bitcoin. In 2015, the downward trend continued and, in June 2015, bitcoin was already bought for 206 USD. In 2016-2017, the rate began to grow rapidly, and already in December 2017, the cost of one bitcoin was 1275 USD.

Separately, we singled out the 2018 year, since due to a significant jump in January (the rate rose from 1275 USD to 17542 USD for one bitcoin), it is difficult to clearly demonstrate the general trend of Bitcoin development over the entire period (Fig. 2).

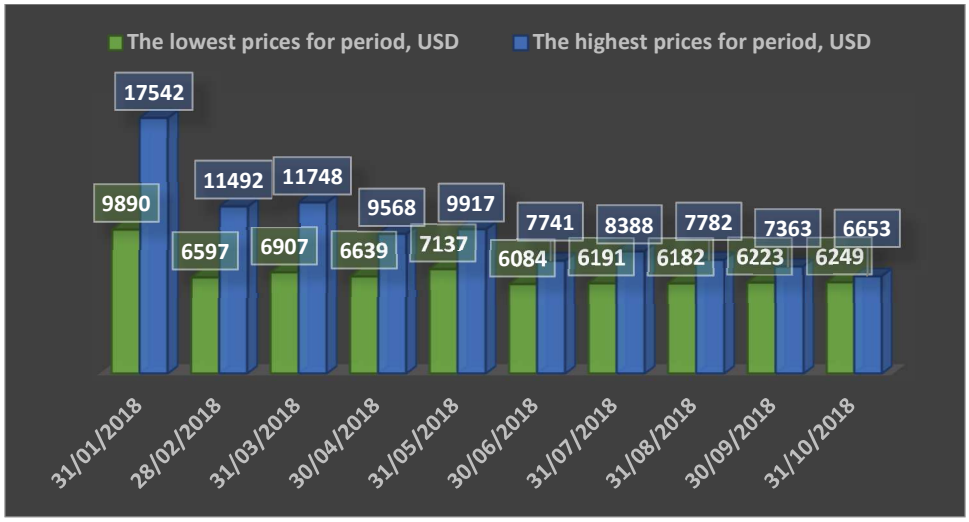


Fig. 2. Dynamics of Bitcoin exchange rate in 2018 in the monthly section

According to the logarithmic graphs, it is much easier to evaluate results in the long term than linear ones. In a line chart, a rise from $ 1 to $ 20 looks almost invisible, than, for example, from 100 to $ 200, although in the first case we are talking about the growth of 20 times, and the second - just 2. When we use the logarithmic graph of such problems does not arise. That is why we consider that it is appropriate to analyze this indicator using a logarithmic function (shown in Fig. 3).

Fig. 3. Dynamics of Bitcoin 2010-2018

According to the graph, which shows the dynamics of Bitcoin price change since 2010, we can see, that it is in the stable growth phase, but it is the subject to strong fluctuations. The price change chart became parabolic, that is, the line went up almost vertically three times in the entire history of Bitcoin. This is difficult to achieve, because the rate must be changed very much for that. There are three such precedents so far: in 2011 and twice in 2013. In all three cases, the price of Bitcoin increased by 100 and more times. As you can see, the rise in 2017 did not leave a

parabolic section on the chart. In order for this to happen, the cost must take off more than $ 100,000.

Cryptocurrency of its kind is "information in the network", but since it is not freely available, it therefore has some value. Bitcoins do not have gold reinforcement in the state fund and do not depend on the country's GDP. Bitcoin quotation depends solely on the interaction of his supply and demand, which in turn confirms the fact that nobody regulates the price. Thus, neither a huge increase nor a huge drop is limited, which is typical and often occurs on stock exchanges by stopping trading.

Based on the theory of the value of money over time, cryptocurrency also tends to increase its value due to various factors over time.

Now, one of such driving factors is the great interest of the public in the new form of cashless payment. In addition, we should not forget that the value of any money and their value changes over time. Inflation is evidenced about it. One of the main advantages of this currency is that it protected from inflation, since the issue procedure programmed to reduce the amount of virtual money in circulation. It planned to “get” 21 million units of this cryptocurrency. The fact that the rate of bitcoins is not affected by political conditions or the activities of the Central banks is attractive for investors.

In the global economy, the cryptocurrency appeared just in time. Due to the global economic crisis, the image of traditional investment methods has suffered; in the result, investors lose billions of dollars and confidence in leading national currencies. All of this together contributes to an increase investor interest in cryptocurrency, which every year strengthens its position in the global financial system.

As analysts from Gartner define that, the most of new technologies that appear in the world go through a certain development cycle (Fig. 4). The technology trigger, the peak of inflated expectations, trough of disillusionment, slope of enlightenment and a plateau of productivity are the main stages that the technology goes through. Cryptocurrency and related technologies demonstrate very well the existing relationship with this curve [5].

Fig. 4. Main stages of the Gartner Hype Cycle

After having compiled a statistical forecast for the next 3-4 years (Fig. 5) and having compared it with the Gartner Hype Curve, it becomes clear that, most likely, in 2015-2017, Bitcoin was in the "Peak of Inflated Expectations" phase. During this period, everyone actively began to get acquainted with technology and try to get business benefits from it. Bitcoin moves to the "trough of Disillusionment" stage, because users are disappointed after a significant drop in the course, and this trend may drag on. But since the technology has many strengths, it is likely that the "Slope of Enlightenment" stage will follow in parallel. Starting from the end of 2019, we can say that bitcoin can go into the "Plateau of Productivity" stage.

One of the most popular methods for predicting the dynamics of market indicators is the compilation of a trend model that shows "What will happen if there is something that has already been". To build a statistical forecast, we used the average values of the Bitcoin exchange rate for 2010-2017. (Fig. 5).

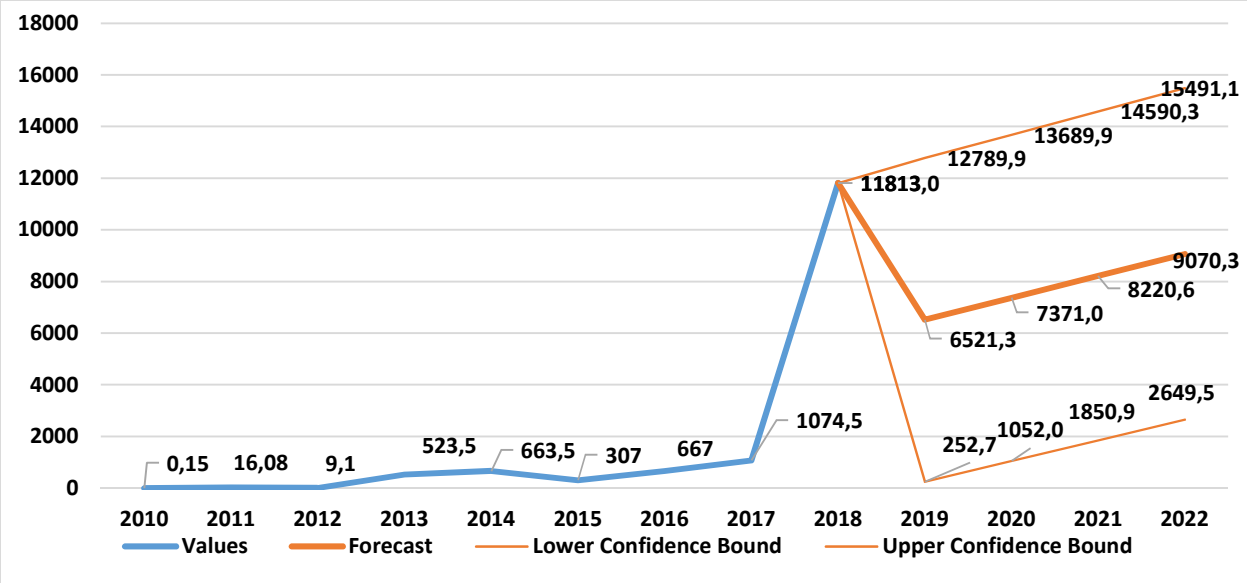


Fig. 5. Prediction of the Bitcoin exchange rate to USD for 2019-2022

From the study, we can conclude that, despite the fact that Bitcoin has recently demonstrated impressive growth dynamics, it is a consequence of the rapidly growing interest in cryptocurrencies, which provokes market demand, while limiting supply. It is important to note that most likely the peak of rush demand has already been reached. Until the end of 2019, a certain fall will continue, but the predicted values for the next 3-4 years show that the course of Bitcoin will stability grow. According to the forecast, in 2019 the average price for 1 Bitcoin will be 6521.3 USD. According to the optimistic forecast, the Bitcoin rate in 2019 is 12789.9 USD, at the same time, the pessimistic allows even 252.7 USD for 1 Bitcoin.

Cryptocurrency has already become a significant player in the modern financial market, and the object of investment of many market players that have leverage to support it. Therefore, even after the inevitable drop in rate, the development of cryptocurrency will continue, but the volatility is likely to subside.

Virtual currency involves a huge amount of computing power and digital assets. At this stage of technological development of mankind, cryptocurrency is gaining a stable position in the international market. The rapid development causes a further increase in capacity and interest of the masses, but on the other hand, it can lead to collapse. Health care is one of the areas that has not use properly the virtual currency yet. But some companies are starting to integrate Bitcoin with online health care, and medical tourism is a big step forward in the development of this area.

When price stability of cryptocurrency is achieved, it will be possible to talk about using it in international transactions, and not just for speculative gain. However, this issue will already be directly related to the legalization of the new currency and its recognition by central banks as a means of exchange, or storage of the value of money.

REFERENCES:

1. Bitcoin for all time. URL: https://probtc.info
2. Bitcoin history: a brief excursion into the past and the future of cryptocurrency. URL: https://habr.com
3. Athey S., Parashkevov I., Sarukkai V., Xia J. Bitcoin Pricing, Adoption, and Usage: Theory and Evidence. Stanford University Graduate School of Business Research Paper, 2016, No. 16-42, p.70
4. Andreas M. Antonopoulos "Mastering Bitcoin" URL: https://github.com/bitcoinbook/bitcoinbook/blob/develop/preface.asciidoc
5. Gartner Hype Cycle. URL: https://www.gartner.com/technology/research/methodologies/hype-cycle.jsp
6. Gandal N., Hamrick J.T, Moore T., Oberman T. Price Manipulation in the Bitcoin Ecosystem, Journal of Monetary Economics, 2017, p. 26

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 111-114 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

INSTALLATION FOR STUDY OF DATA PROTECTION TECHNIQUES IN COMMUNICATION CHANNELS

Nataliia Tmienova 1, Bohdan Sus 2.
Faculty of Information Technology, Taras Shevchenko National University of Kyiv 1
Institute of High Technologies, Taras Shevchenko National University of Kyiv 2

ABSTRACT. The growing threat of computer crime puts forward new urgent tasks. The relevance of information security depends on the growing threat of cybercrime in modern hardware and software intellectual and telecommunications systems. Modern electronic devices allow you to control most of the channels for data collecting, processing and transmitting. The need for practical training of specialists in protection of information using laboratory workshops becomes evident. Laboratory work on the study of data protection capabilities based on the achievements of modern microelectronics such as programmable microcontrollers, receivers, transmitters, repeaters and communication channels can be very effective means of training specialists. The article describes a demonstration installation that can be used in such lab activity.

Keywords: cryptography, hardware encryption systems, programmable microcontrollers, security, privacy, forensics analysis, embedded systems.

1 Актуальность разработки

В настоящее время наблюдается растущая тенденция нарушения безопасности данных. Утечки информации часто происходят вследствие неэффективного управления кибербезопасностью или в результате применения устаревших или неправильно реализованных процедур безопасности. Шифрование данных с применением соответствующих схем управления ключами может уменьшить утечку данных. Однако при использовании методологии с ключами шифрования возникают такие проблемы как генерирование и безопасная передача ключей участникам взаимодействия; установка безопасного канала передачи информации между участниками взаимодействия; аутентификация. Существуют симметричная и асимметричная технологии шифрования. Каждая методология использует свои собственные процедуры и способы распределения ключей, типы ключей, а также алгоритмы шифрования и расшифровки ключей [1].

Хотя криптография с использованием известных стандартов, современных алгоритмов и библиотек является достаточно эффективной, разработка аппаратных комплексов шифрования остается актуальной задачей [2, 3]. Программные средства обеспечения информационной безопасности являются потенциально уязвимыми, поскольку весь процесс кодирования данных выполняется во внутренней памяти вычислительных устройств, к которой может получить доступ любое запущенное на компьютере приложение. Это означает, что существует возможность проводить разноуровневые атаки на любое программное обеспечение, в том числе и на предназначенное для обеспечения безопасности обрабатываемой информации. Таким образом, построить высокоуровневую защиту исключительно программными средствами практически невозможно [4]. Для ограничения доступа к средствам, выполняющим криптографические преобразования, необходимо перенести их из ЭВМ на закрытую аппаратную подсистему. В результате чего злоумышленник не сможет получить непосредственный доступ к процессам кодирования данных. Прежде всего аппаратная реализация алгоритма шифрования гарантирует неизменность самого алгоритма, тогда как программной алгоритм может быть намеренно модифицирован. Кроме того, аппаратный шифратор исключает вмешательство в процесс кодирования. Другое преимущество - использование аппаратного датчика случайных чисел, который гарантирует абсолютную

случайность генерации ключей шифрования и повышает качество реализации различных криптографических алгоритмов. Кроме того, аппаратный шифратор позволяет напрямую загружать ключи шифрования в устройство кодирования, минуя оперативную память, тогда как в программном шифраторе ключи находятся в памяти даже во время его работы. Также важен и тот факт, что на базе аппаратного шифратора возможно создавать различные системы разграничения и ограничения доступа к вычислительным системам. Также применение аппаратных систем затрудняет возможность сокрытия доказательств вмешательства в каналы связи.

В данной работе для исследования аппаратных возможностей уменьшения вероятности несанкционированного доступа к информации предлагается аппаратное устройство для демонстрации шифрования данных на базе программируемых микроконтроллеров. Комплекс позволяет совместное использование различных каналов связи. Оптико-волоконные линии связи позволяют обеспечить передачу информации с минимальными искажениями, что позволяет улучшить технологии защиты передачи информации.

Дополнительный интерес вызывает использование в комплексе поляризационной модуляции света. Работа таких устройств основана на применении электронно-управляемых анизотропных сред.

Данный комплекс может использоваться для успешного изучения студентами технологий, алгоритмов и физических методов шифрования и безопасной передачи сигналов в каналах связи.

2 Описание комплекса

Для оценки эффективности алгоритмов шифрования данных был разработан ряд практических решений, включающих в себя программные коды и аппаратную реализацию на базе встроенных систем. В настоящее время по оптическому каналу связи передается большое количество информации, и есть риск того, что она может попасть к злоумышленникам, которые имеют необходимые ресурсы и оборудование. Поэтому предлагается сочетание стандартных оптических каналов с радиоканалами, которые переключаются по специальному алгоритму. Возможность использования аппаратного датчика случайных чисел гарантирует случайность генерации ключей шифрования и повышает качество реализации различных криптографических алгоритмов. Предложенное шифрования не устраняет возможности перехвата данных через оптический канал, но делает похищенную информацию малополезной для злоумышленников.

Комплекс создан на базе высокопроизводительного микроконтроллера. У комплекса шифрования информации доступны такие основные функции:

- передача и прием сигналов по отдельным оптическим каналам;
- передача и прием сигналов по общему оптическому каналу с использованием спектрального мультиплексирования;
- передача сигналов или ключа шифрования по радиоканалу;
- возможность синхронной коммутации каналов связи.

Для кодирования сигналов используется библиотека x-cube-cryptolib, в которой поддерживаются алгоритмы шифрования данных AES-128, AES-192, AES-256, ECB (Electronic Codebook Mode), CBC (Cipher-Block Chaining).

Программа посылает сообщение, которое в свою очередь может быть дополнительно зашифровано программным образом. При использовании программного шифрования информация всех типов сначала разбивается на пакеты малой фиксированной длины, содержащие заголовки (так называемые ячейки). Дальше происходит их мультиплексирование

в цифровом канале.

Сообщение вводится в окно программы терминала модуля передатчика. Для наглядности при передаче информации оптическим каналом использованы излучатели излучения красного, зеленого и синего цветов.

Для передачи данных также используется радиоканал на доступных модулях MX-F01 и MX-RM-5V. Связь между радиомодулями и микроконтроллером организована через периферийный интерфейс USART. Количество излучателей можно изменять в соответствии с количеством каналов.

При передаче закодированного сообщения осуществляется коммутация каналов (переключение передатчиков и приемников в соответствии с определенным алгоритмом шифрования). Эффективность приёма изменяется в зависимости от скорости передачи и задержки между пакетами данных.

В демонстрации может использоваться также комбинация оптических каналов со спектральным уплотнением сигналов и алгоритм динамического плавающего кода.

Дешифрованное сообщение выводится в окно программы терминала последовательного порта, который получает данные из микроконтроллера, который выступает в качестве приемника.

Такое кодирование особенно эффективно для передачи коротких пакетов данных. В таком режиме возможно дополнительное кодирование информации в оптическом канале с помощью изменения поляризации излучения. Использование поляризационных ячеек на жидких кристаллах и анализаторов меняется в соответствии с алгоритмом шифрования. Небольшая скорость передачи информации в таком режиме связана с использованием недорогих микромеханических электронных систем для поворота поляризаторов.

3 Выводы

Растущая опасность компьютерной преступности выдвигает набор новых актуальных проблем. При этом разработка аппаратных комплексов шифрования может быть эффективной на пути преодоления некоторых из них.

Описанный демонстрационный комплекс позволяет оценить эффективность шифрования потоков данных в каналах, сравнивать пакеты, принятые от передатчика, с числом отправленных, анализировать спектр зашифрованного сигнала и шумы радиоканала.

Данный комплекс может удачно использоваться в следующих областях: банковской сфере, военной и медицинской отраслях, телекоммуникациях.

К основным достоинствам можно отнести надежность передачи, простоту реализации, гибкость функционала и возможностей применения.

Также, демонстрационный комплекс возможно использовать для проведения лабораторных занятий по созданию протоколов передачи информации и фильтров обработки сигналов.

Комплекс дает возможность проводить физические эксперименты по мониторингу сигналов в оптическом волокне и радиоканале связи для выбора оптимального алгоритма устойчивости шифрования.

Предложенные подходы можно использовать для модификации оборудования передачи данных и оценки надежности шифрования.

Библиография:

1. Введение в криптографию (авторизованный перевод статьи Дж. Чандлер "Cryptography 101") [Электронный ресурс]. Режим доступа: http://citforum.ck.ua/security/cryptography/crypto_1.shtml
2. Безопасность информационных систем [Электронный ресурс]. Режим доступа: http://intuit.valrkl.ru/course-1312/index.html.
3. Security with STM32 & Secure Elements [Electronic Resource]. Mode of access: http://www.emcu.it/SILICA-STDay2016/X/Presentazioni/2_STM32&SecureElements.pdf
4. Stallings W. Cryptography and network security: principles and practice. – New York: Prentice Hall, – 2006. – 680 p.

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 115-176 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

MIND MAPPING TECHNIQUE FOR NOTE TAKING

A Senior Scholars Thesis

by

AUGUSTINE EJEH

Submitted to the Office of Undergraduate Research

Department of Computer Science

American University of Nigeria

In partial fulfillment of the requirements for the award of the degree of

BACHELOR OF SCIENCE IN COMPUTER SCIENCE

December 2011

Major: Computer Science

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 115-176 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

MIND MAPPING TECHNIQUE FOR NOTE TAKING

A Senior Scholars Proposal

by

AUGUSTINE EJEH

Submitted to the Office of Undergraduate Research

Department of Computer Science

American University of Nigeria

In partial fulfillment of the requirements for the award of the degree of

UNDERGRADUATE RESEARCH SCHOLAR

Approved by:

Research Advisor:

Coordinator for Undergraduate Research:

December 2011

Major: Computer Science

Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 115-176 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

Mind Mapping Technique for Note Taking.

ABSTRACT

Note taking is the process of taking note in a place where an event is happening like class or meeting or any important occasion when necessary. It is important to take note because the information presented in class or meeting often contains the central concepts of the course and the material most likely to be included on exams if a students or being asked by the boss if a secretary (Academic Skill Center, 2011).

The main aim of my project which is "mind mapping technique for note taking" is to develop a system with the aid of information communication technology tools that enables user who learn best by using words (NovaMind, 2011) to regularly review key concept, repeating or reciting key concepts from class, reflecting or connecting your ideas or speaker owns to other notes and reading, event (class, meeting, etc) (Academic Skill Center, 2011). That is, developing a system that enable you to quickly create notes using a Mind Map as you listen to lecture (Garret, C., 2007).

A mind map is a graphical figure used to represent and focus on an idea or central key word that other ideas, words, tasks, or other items are arranged around it and then linked to. It is actually a graphical method of taking notes. Mind Maps are a visual diagram with bubbles and lines representing relationships and ideas between them. The core idea usually sits in the middle with related topics branching out from it. Ideas are further broken down as well as extended until your page looks like an impressionist painting of a spider colony (Garret, C., 2007). Mind map with ideas branching into their subsections generally take tree branching or hierarchical format. Mind map allows when recording ideas and information, a greater creativity by allowing the association of words with visual representation hence helping with memory and organization (Farrand, P., Hussain, F and Hennessy, E., 2002).

Keywords: Note taking, Mind map, Information communication technology.

DEDICATION

This project is dedicated to my parents Mr. and Mrs. Ejeh.

ACKNOWLEDGEMENTS

Thanks to my supervisor Dr. Mathias Fonkam and my project coordinator Dr. Denis Smoline for his assistance in the course of this project. I appreciate the help and support of my colleagues in the developmental process. I want to thank my parents for their dedication and support in my study in AUN.

CHAPTER ONE

INTRODUCTION

About note taking using mind mapping technique

The mind mapping technique is published by the noted psychologist, Tony Buzan in his book title, “Use Your Head”. The technique mimics the way the human mind works by connecting related ideas to a central one in a kind of 2-dimensional space rather than linearly as on the written paper such as this project that must be read from top to bottom (Hunt, A., 2009).

Problem statement:

Tens of thousands of students around the world are taking lecture notes in a completely inefficient way that is, either writing them down in some languages column by column or line by line (Dryden, G., Ves, J., 1999). .

The brain does not work by storing information in neat lines or columns. It stores information on branches called dendrites tree like branches. It also stores information by associations and patterns. And as a result of trying to store information the way the brain does, British psychologist Tony Buzan invented Mind Mapping (Dryden, G. & Ves, J., 1999).

Justification from the implementation of mind mapping for note taking:

- The software will provide a GUI screen applicable on laptops or I-pads from which users can create and link ideas in a 2-dimensional space.
- The use of the software works more in-line with how the brain operates.
- The software provides more focus on understanding rather than words or syntax.
- Users can keep pace with lecture or presentations by focusing on ideas instead of words.
- The tasks performed on the software provide transition to report. That is, tasks performed on the software can be reported or aid in reporting.

- The software is an electronic document (e-doc) of paper which reduces cost, time and wastage.
- Works on the software are safer to paper.
- Categorization and hierarchy are clearly and visually defined (Garret, C., 2007).
- A mind map can be read back at a glance; jumping right to the part you need (Garret, C., 2007).

CHAPTER TWO

ORGANIZATION

Stakeholders

The stakeholders intended in this project are:

The stakeholders are learned persons, secretaries and students who prefer expressing ideas as text.

CHAPTER THREE

METHODOLOGY

Proposed Methodology

The note taking application for use in meeting is created using the iterative development that is implemented through the following processes: analyze the requirements, design the solution, validates the design, implement the design, test the solution and document the solution. The mind mapping technique would be implemented using the Java programming language guideline I described below

1. Write the central idea in the center idea holder.

2. Write each of the agenda item in the idea holder linked to the outside of the main idea.

3. Draw lines that point to sub-thoughts, facts, and idea as well as figures, as the meeting progresses then label automatically indicating it hierarchical order.

4. Without or with arrows, draw pictures and interlink (Mind Map, 2009).

Advantages of using mind mapping.

1. The way the brain works which is not in nice neat lines is how minds maps are created.

2. Memory is naturally not linear but associative. Any idea probably has thousands of links in your mind. Mind maps allow links and associations to be reinforced and recorded.

3. The mind does not remember sentences but images and key words -- try recalling just one sentence from memory! Mind maps use just key images and key words, allowing a lot more information to be put on a page.

4. Because mind maps show associations between key words and are more visual, they are much easier to remember than linear notes.

5. Starting your mind mapping from the center of the page rather than from the top-left corner allows you to work out in all directions.

6. The way your own brain organizes ideas is reflected in the organization of a mind map.

7. Mind maps are easy to review. Memory is reinforces by regular review. Trying to review in your imagination first is best, then go back and check on those areas that were blurred.

8. Key points stand out easily due to visual quality of mind maps (Russel, P., 1996).

9. Ideas stick out in mind mapping (Pash, A., 2009).

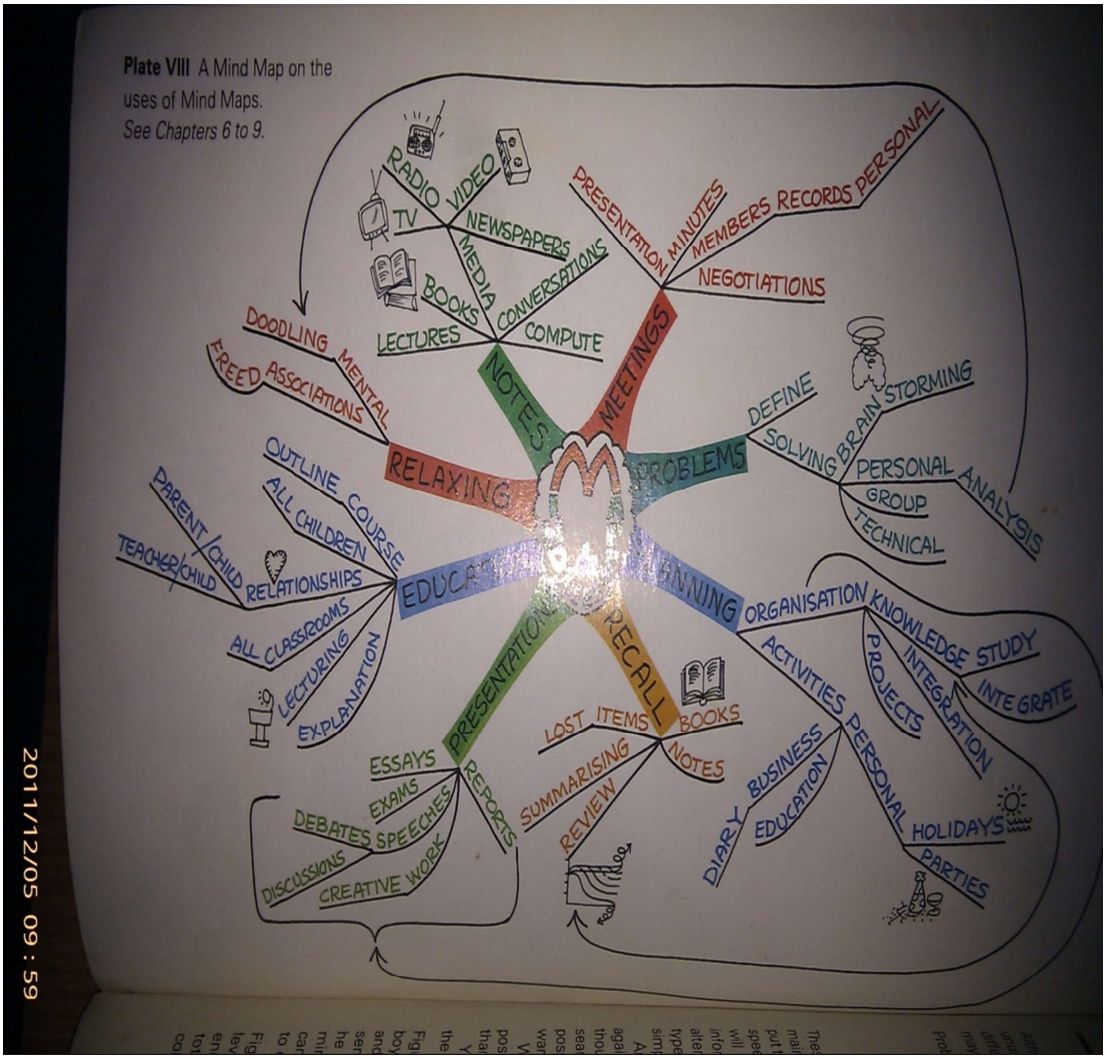
10 By attracting to both the logical and creative side of the brain, it stimulates the brain (Mohidin, F., 2010).

Disadvantages of traditional linear notes.

1. Time and energy are wasted writing down words that are unnecessary.
2. While an idea is being noted down, some information may be missed.
3. Take longer time to review and read.
4. The connections and associations between ideas and key words are not readily clear.
5. The attention of readers wanders easily.
6. The lack of color and other visual qualities hamper memory.
7. Traditional notes aid forgetting not memory (Russel, P., 1996).

8. Many sub ideas can be lost or forgotten due to been hidden under larger concepts in traditional note taking (Pash, A., 2009).

The Mind Mapping Technique by Example



(Buzan, T., 1995).

CHAPTER FOUR

PROGRAM SCOPE

Limitations.

My note taker software aids in numbering ellipses automatically and smartly compared to other mind map note taking software. It labels based on the hierarchy of how ideas are linked. It also used short cut key combination to make work on the note taker faster.

Duration.

The time period for completion of each milestone is as follows in the table below:

Milestone	Description	Proposed Finish Date	Finished Date
1	Analyze the Requirements	6/10/2011	6/10/2011
2	Design the Solution	13/10/2011	15/10/2011
3	Validate the Design	20/10/2011	20/10/2011
4	Implement the Design	24/11/2011	29/11/2011

5	Test the Solution	1/12/2011	2./12/2011
6	Document the Solution	8/12/2011	12/12/2011

Duration table

Future prospects.

1. A web-based version of my software in other languages apart from Java applet.
2. A version of the software that listen to speaker and mind map taken note automatically.
3. Adding more shapes to the note taker note page.
4. Improving the user interface.
5. User manuals.

CHAPTER FIVE

PROGRAM DEVELOPMENT

Analysis and Design

Purpose:

My program is not free software and should not be modified without my permission. My program is easy to use software that enable user to take note using the mind mapping technique which is a graphical figure used to represent and focus on an idea or central key word that other ideas, words, tasks, or other items are arranged around it and then linked to.

Application Title:

Note Taker

Algorithms:

The note taker is used to take note after execution as follows:

If user select a new note, output a page with mind mapping tools

If user select an idea holder as ellipse or an idea explanation holder as a folded rectangle from the tool bar and click anywhere on screen

Output it at that location with a number

If user's double click on an ellipse or folded rectangle on the screen

Output a dialog box to enable user describe idea as text or explain idea in details as text

If user select an ellipse or folded rectangle on the screen and drag to another location

Output it at that location

If user has put more than one ellipse or folded rectangle on the screen as well as selected a sub-idea connector or idea explanation connector from the tool bar and dragged it within any two ellipses on screen

Output a connected ellipse with a directed line between them or output a connected

folded rectangle or an ellipse connected to a folded rectangle with an undirected line between the notes.

Number the ellipse automatically.

If user clicks on exit Close the program.

To number drawn ellipses automatically.

Drawn first ellipse and it name to “1.0”

Draw another new ellipse

i=1;

While line is drawn from first ellipse to a new ellipse{

Label new ellipse: “1.”+i;

Increment i;}

j=1;

While line is drawn from newly labeled ellipse apart from first ellipse to another new ellipse{

Label the new ellipse: newlyLabeledEllipseName+” ”+j;

increment j;}

Notes:

User can open save files, view recent files.

User can save files, save files as other format like violet files or all files.

User can export image as image file as well as print them.

User can delete drawn object.

User can change the theme of the software as well as change different drag type.

Problem Analysis

The problem that the Note taker is to solve is to support the mind-mapping technique of note-taking that can be used by secretaries in meetings or even students in a lecture class with the aim of providing a GUI screen applicable on laptops or I-pads from which users can create and link ideas in a 2-dimensional space working more in-line with how the brain operates as well as mimicking the way the human mind works by connecting related ideas to a central one rather than linearly as on the written paper. The software is to provide more focus on understanding rather than words or syntax. It should also enable users keep pace with lecture or presentations by focusing on ideas instead of words. And, it should enable the tasks performed on the software being safer to paper, aid in reporting as well as reduce cost, time and wastage.

To achieve the mind mapping technique for note taking on the software, the user would drag an ellipse on the screen after clicking on an idea holder button to fill it with the focus idea description by either clicking or double clicking on the ellipse. The user

would then try to links the drawn ellipse to another ellipse by clicking on a sub-idea connector to enable them drag from one ellipse to another ellipse with the head of the directed connector pointing to the radiating ellipse. The focus idea on the drawn ellipse can also be explained more by connecting with an idea explanation connector from it to an explanation holder.

Designing the Solution

In designing the interface of the system, critical analysis of the possible scenarios were taken into consideration. The program is made available for now as a standalone program which can be installed on any computer.

Standalone:

The look and feel of the user interface is initially set to the default java look and feel but can be change to others look and feel by selecting from the theme menu. It has three basic panels. The Note Taker panel is the first that is seen by the user which contains menus with functionalities. Some of the menus are File, Edit, View, Theme, Drag, Window and Help menu. The second panel is the Note Diagram panel which contains all the buttons required to take note using mind mapping technique. The third panel is a scroll-pane to enable user to describe their idea as text as well as display them for text editing when a drawn ellipse or line is right or doubled clicked.

User Interface: The user interface contain the following functions

- Toolbar is on top
- For selecting nodes/edges, grabber button are used.
- Buttons for current node/edge type
- Menu
- Drawing area (Horstmann, C., July, 2009).

Mouse Operations

- Empty space is clicked on: current node inserted
- Node or edge is clicked on: select it
- When current tool an edge, drag node: connect nodes
- When current tool not an edge, drag node: move node (Horstmann, C., July, 2009).

PROTOTYPE Pattern

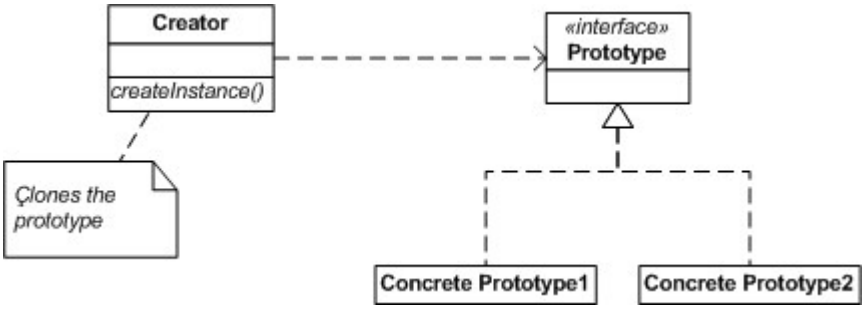
Context

1. Objects of classes that are not known when the system is built is being instantiated by a system.
2. For each kind of object, you do not want to require a separate class.
3. You want to avoid a separate hierarchy of classes whose responsibility it is to create the objects (Horstmann, C., July, 2009).

Solution

1. Define a prototype interface type that is common to all created objects.
2. For each kind of object that the system creates, a prototype is being supply.
3. Whenever a new object of the given kind is required, the prototype is clone (Horstmann, C., July, 2009).

PROTOTYPE Pattern



(Horstmann, C., July, 2009).

PROTOTYPE Pattern

NAME IN DESIGN PATTERN	ACTUAL NAME (graph editor)
Prototype	**Node**
ConcretePrototype1	**EllipseNode**
Creator	**The GraphPanel that handle the mouse operation for adding new nodes**

(Horstmann, C., July, 2009).

Framework UI Classes

- GraphFrame: the toolbar, the menu bar, and the graph panel are being managed by this frame.
- ToolBar: toggle buttons for the node and edge icons are held by this panel.
- GraphPanel: graph is shown and the mouse clicks are handled and drags for the editing commands by this panel.
- Application programmers need not subclass these classes (Horstmann, C., July, 2009).

A Framework Instance

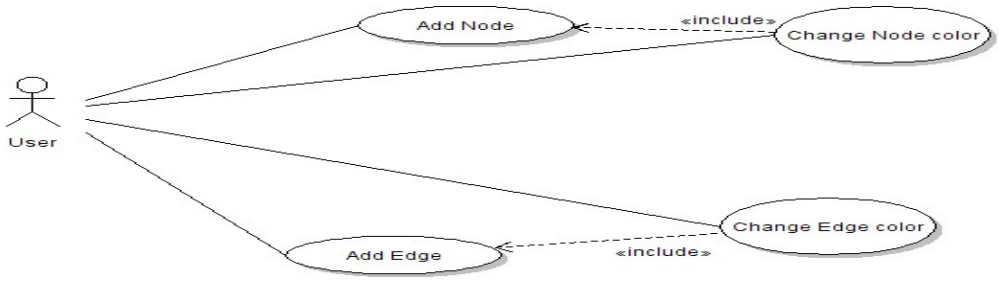
- Simple application
- Draw colored nodes
- Join nodes with straight lines (Horstmann, C., July, 2009).

Responsibilities of programmer

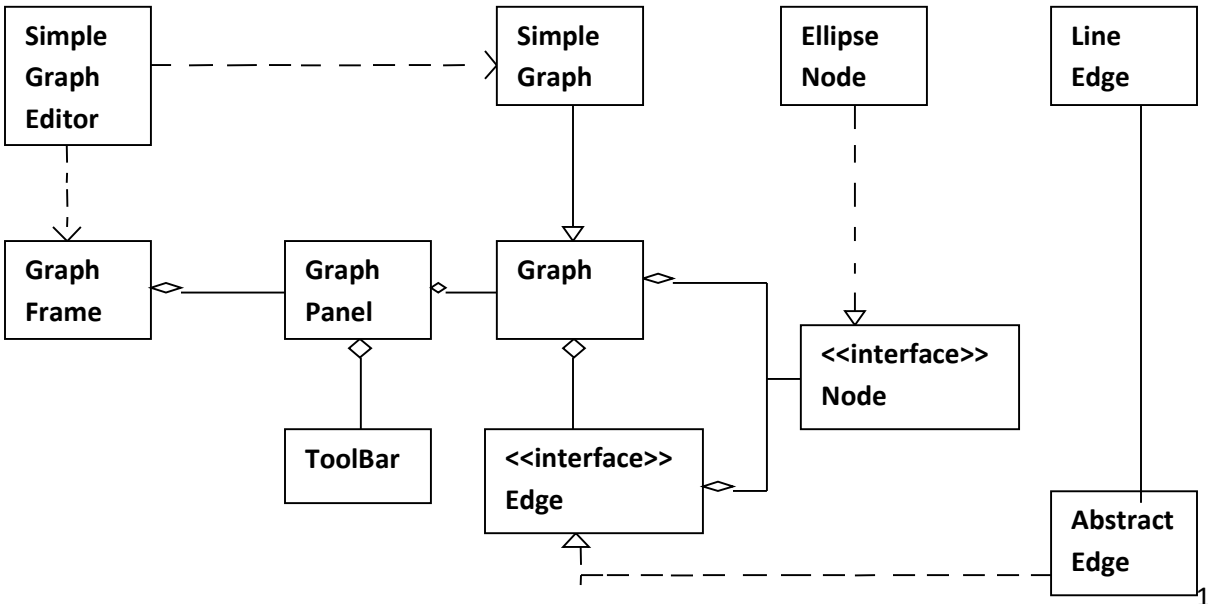
- A class that implements the Node or Edge interface type is being defined for each node and edge type is to be defined.
- All required methods are to be supplied, such as drawing and testing of containment.

- A subclass of the Graph class has been define and getNodePrototypes, getEdgePrototypes are being supplied (Horstmann, C., July, 2009).

Use case diagram for the Note taking System

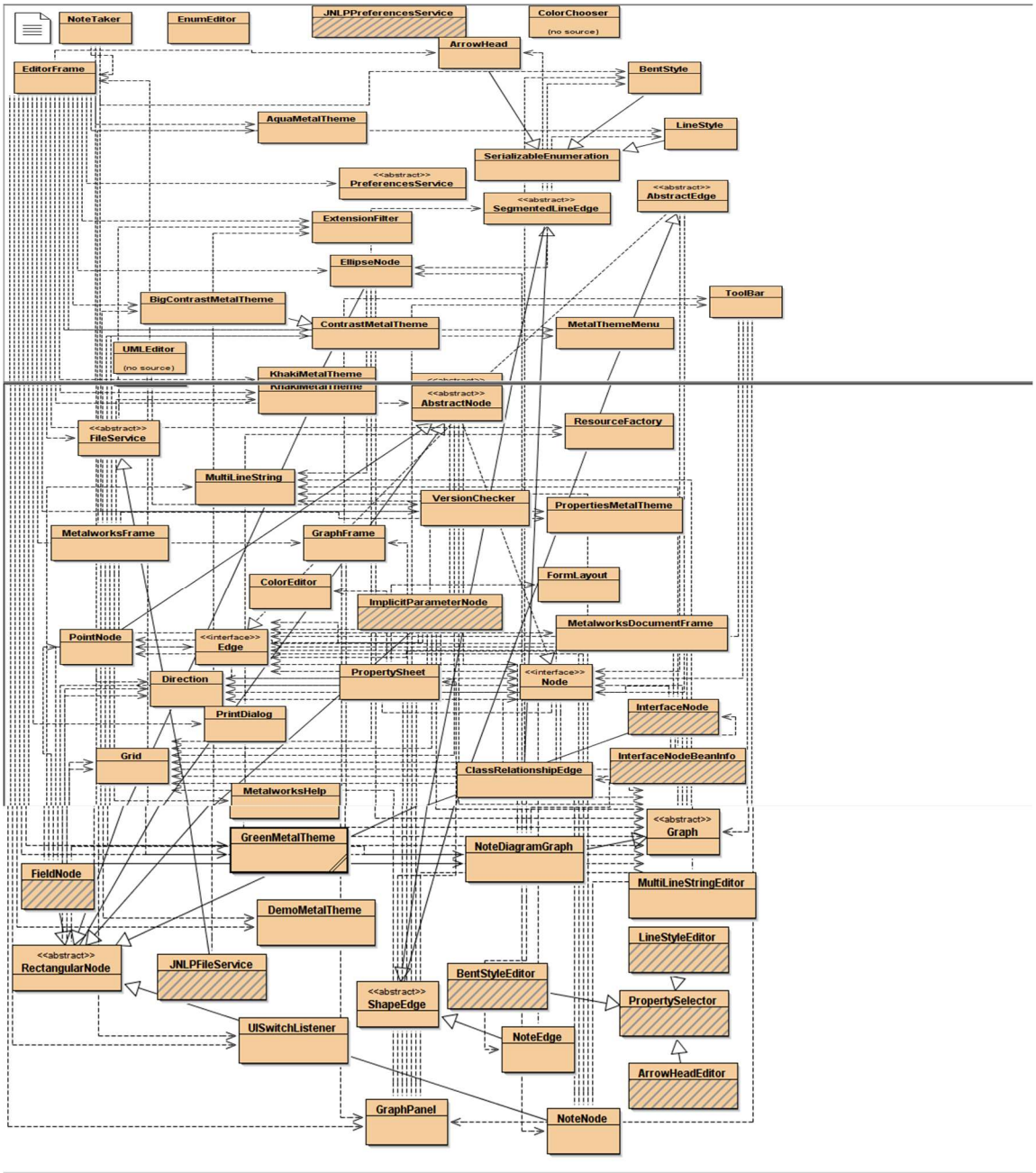


A Framework Instance



(Horstmann, C., July, 2009).

Class Diagram for the whole Note taker system

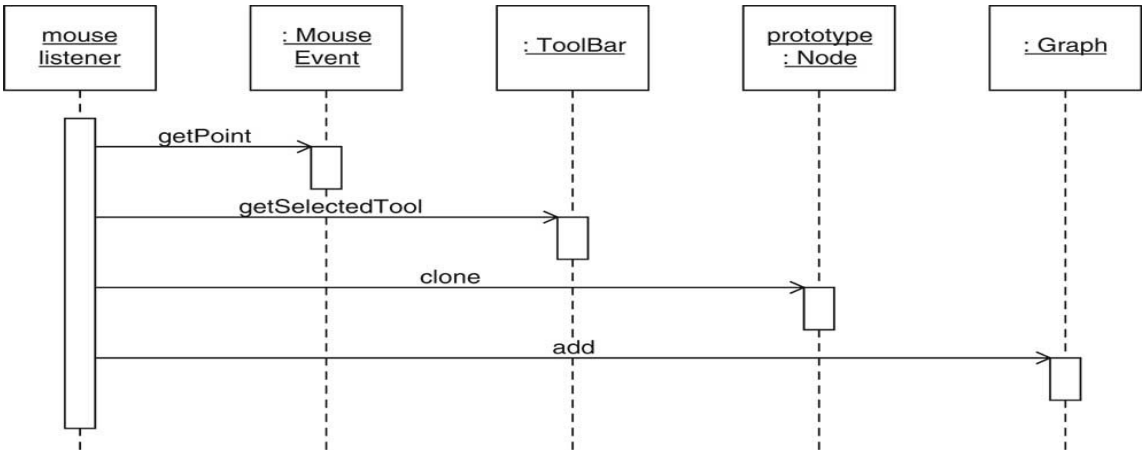


Add New Node

```
public void mousePressed(MouseEvent event)
{
        Point2D mousePoint = event.getPoint();
         Object tool = toolBar.getSelectedTool();
        ...
        if (tool instanceof Node)
        {
                Node prototype = (Node) tool;
                Node newNode = (Node)prototype.clone();
                graph.add(newNode, mousePoint);
        }
        ...
        repaint();
}
```
(Horstmann, C., July, 2009).

Implicit running time for adding new node: O(1)

Sequence Diagram for Add New Node



(Horstmann, C., July, 2009).

Add New Edge

- Check if mouse was pressed inside existing node, first

```
public Node findNode(Point2D p)
{
      for (int i = 0; i < nodes.size(); i++)
      {
            Node n = (Node) nodes.get(i);
            if (n.contains(p)) return n;
      }
```

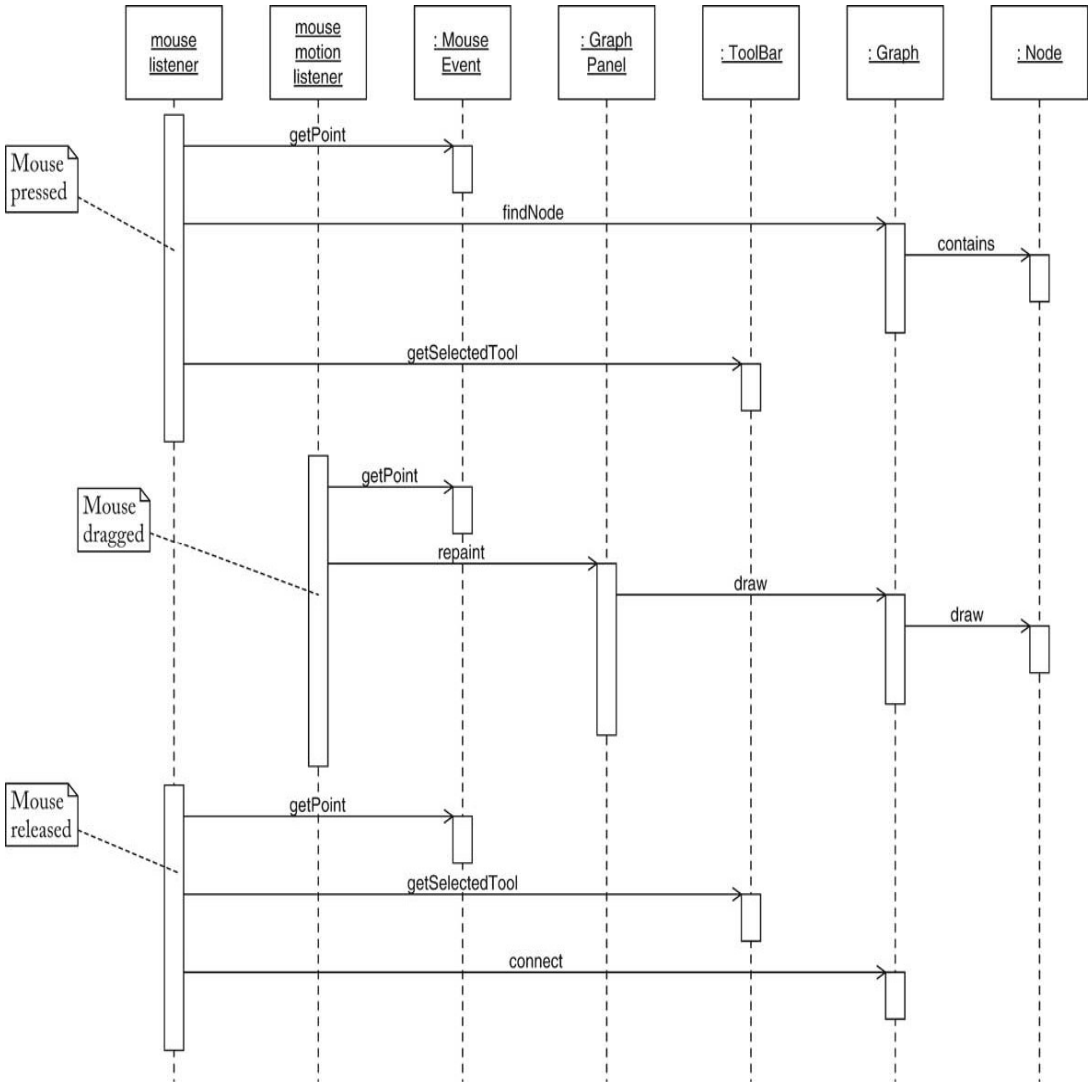
```
        return null;
}
```
(Horstmann, C., July, 2009).

Implicit running time for adding new edge: O(n)

Add New Edge

- `mousePressed:`
    - Check if mouse point inside node
    - Check if current tool is an edge
    - Mouse point is start of rubber band
- mouseDragged:
    - Mouse point is end of rubber band; repaint
- mouseReleased:
    - Edge is added to graph (Horstmann, C., July, 2009).

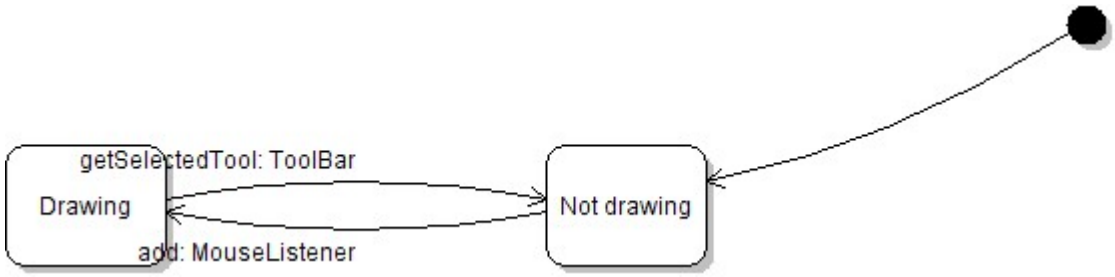
Sequence Diagram for Add New Edge



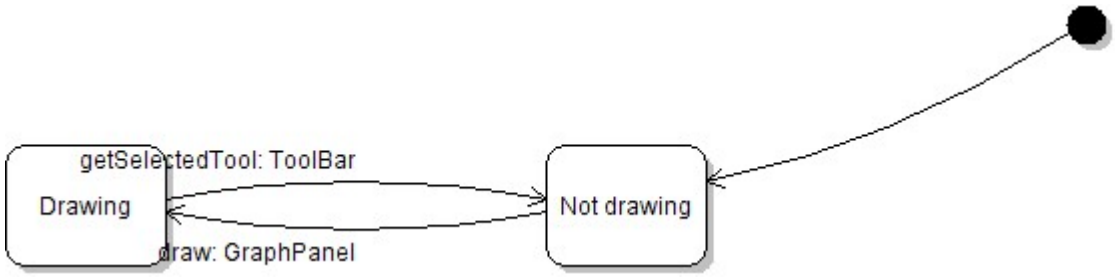
(Horstmann, C., July, 2009).

State diagram for each object

Adding new node state



Adding new edge state



Validating the Design

To validate the design set for the program, survey was carried out and questions asked as to get information to better improve on the design if necessary. It appeared that the design for the standalone was accepted by the public but would like it if a web-based version is also created.

Implementing the Design

The design was implemented into a system that is working by using

Java language: Used in coding the standalone version. Both the user interface and the program logic were implemented using this.

Html language and cascading style sheet: To code the web-based version. Part of the interface was implemented using this.

Testing the Solution

Installing the System

Stand-alone Version

Before the Program can be run, the client computer must have installed Java runtime used to run the program.

If the above are present on the computer,

then the program proceeds to installation

else the above programs must be installed.

Web-based Version

The web-based version is a java applet which requires to be hosted in companies that support it hosting. Before the Program can be run, the client computer must have installed Java runtime and a web-browser used to access the program.

Running the program

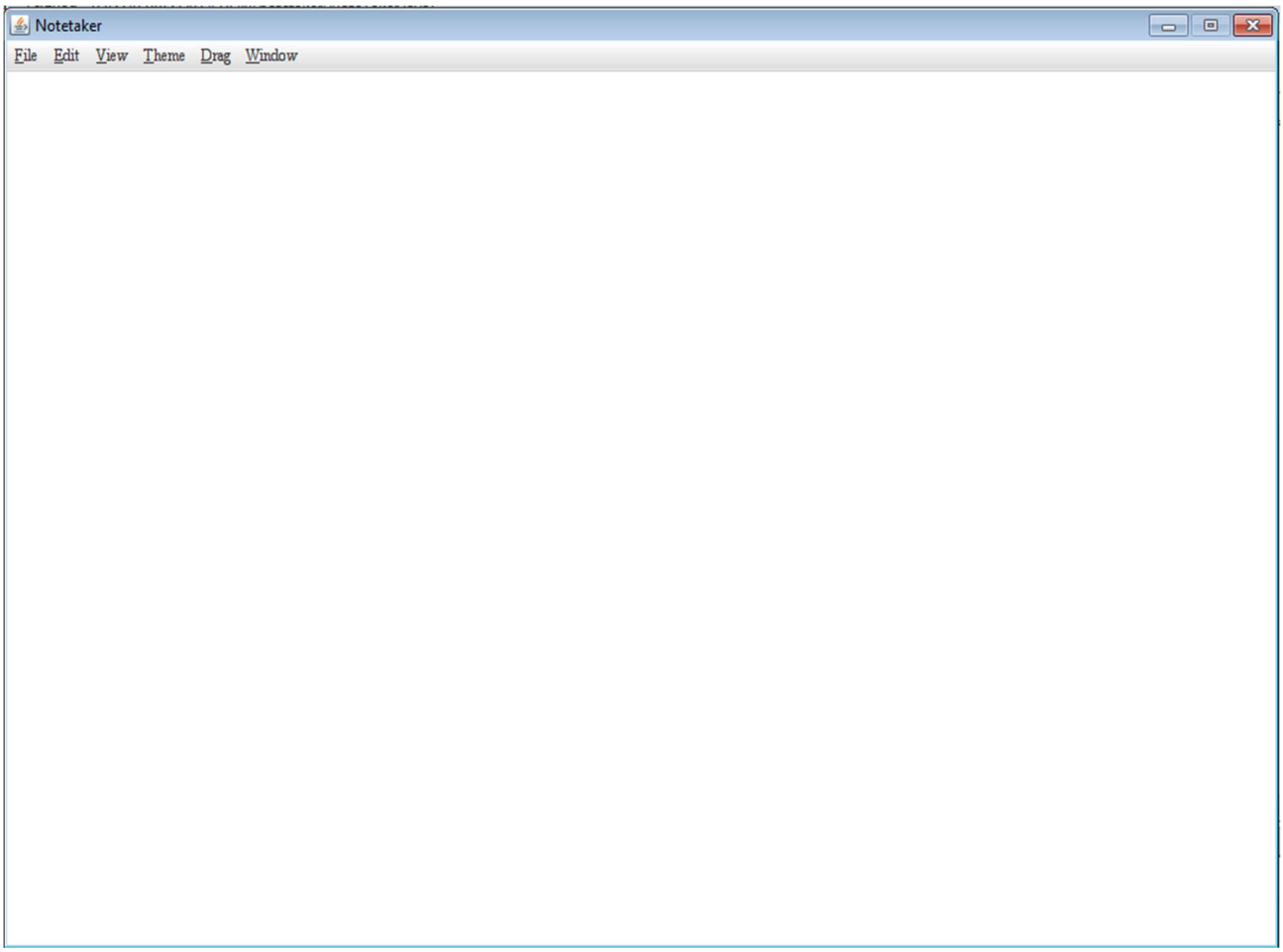
Stand-alone Version

When the program is opened after installation, the user is presented with a Note Taker view. This view contains Note Taker menu such as the File, Edit, View, Theme, Drag, Window and Help menu that are most common and crucial.

Web-based Version

Entering the address of where the applet is hosted by the user presents him/her with the Note Taker view with same interface and functionality as the stand-alone version.

Note: Snipping tool was used to get a snap shot of my implemented software. But could not be used to get areas where menu was selected since it menu close as you try to click on the snipping tool.

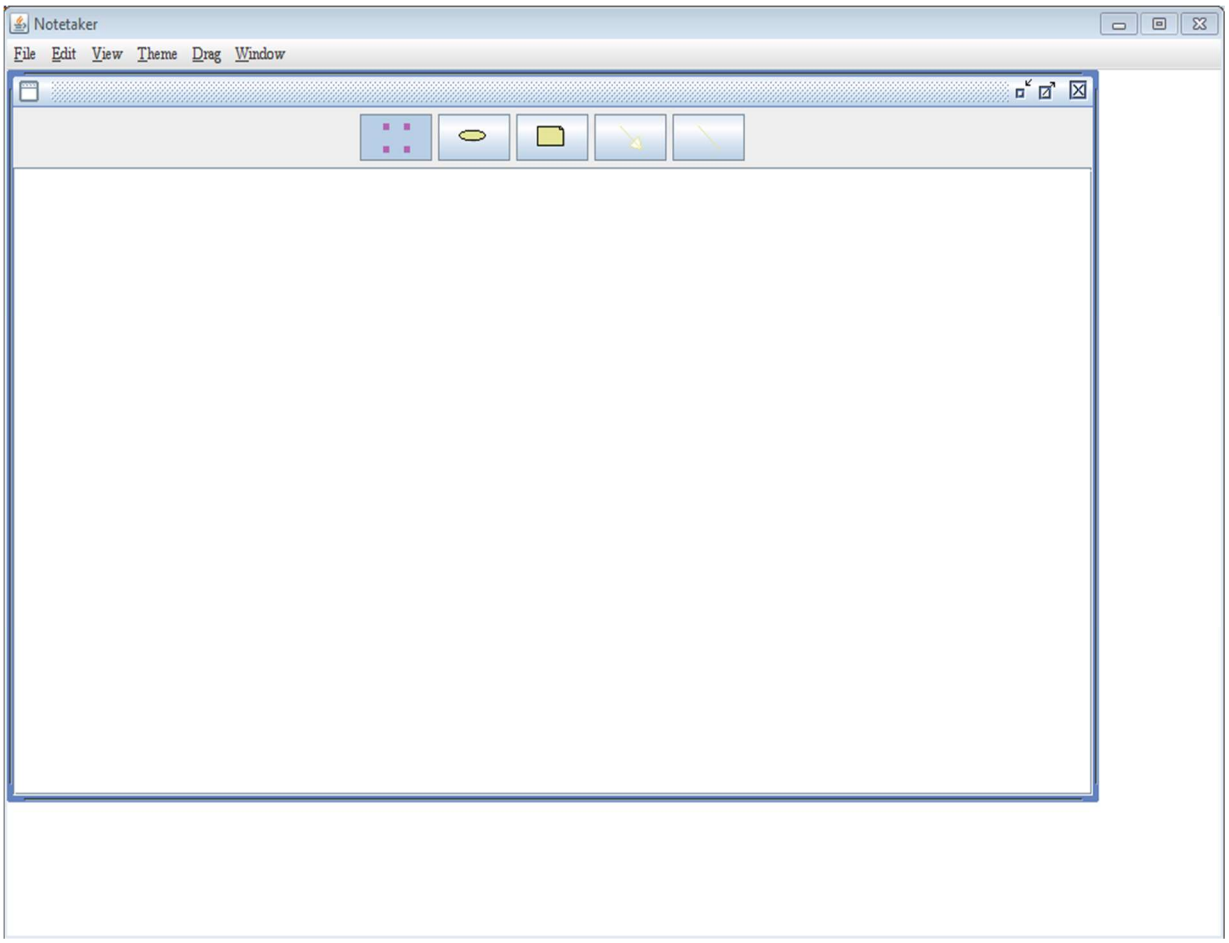


Note Taker view

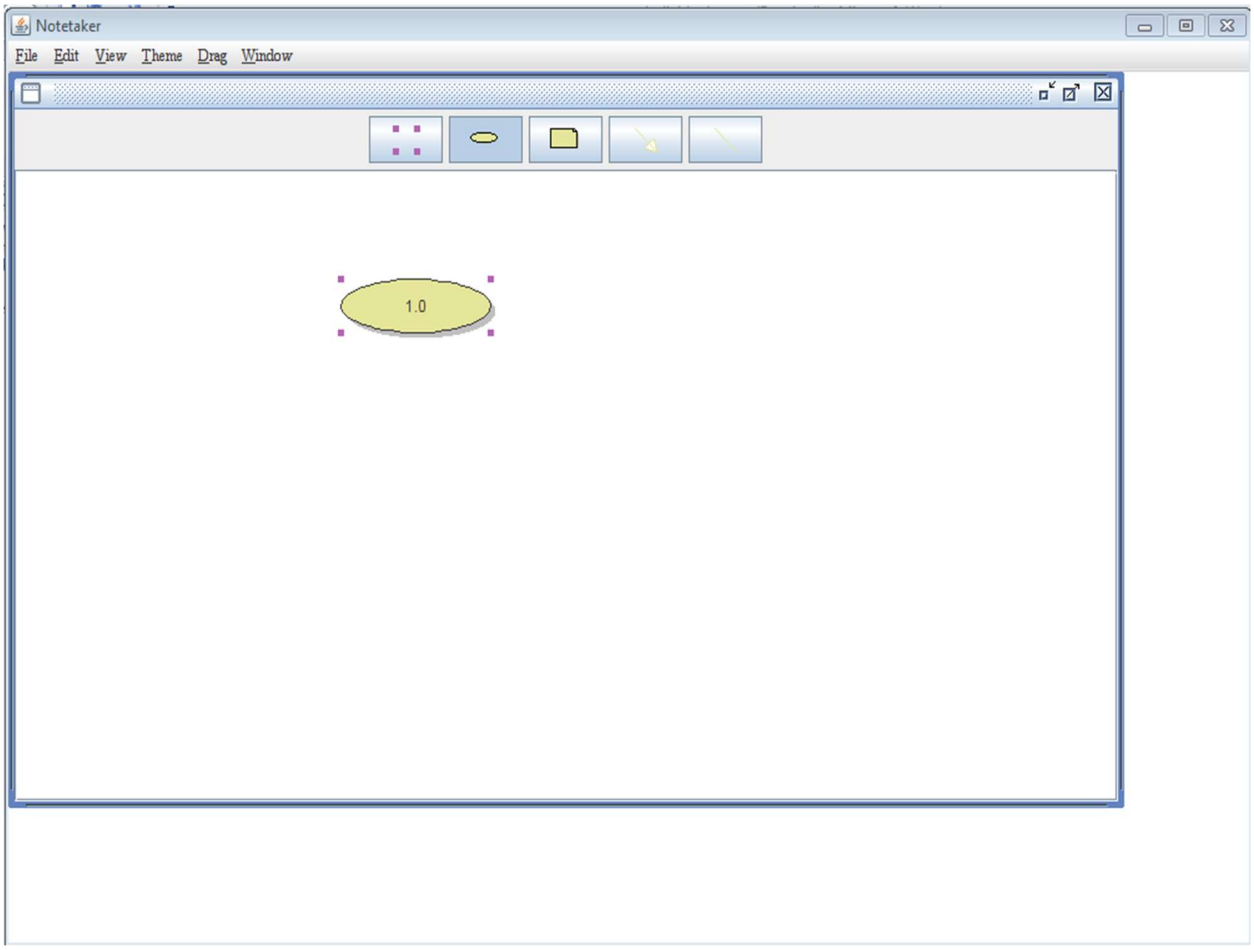
The file Menu has sub-menus like New, Open, Recent files, Save, Save as, Export image, Print and Exit.

Open a new note page by clicking File-->New-->Note or

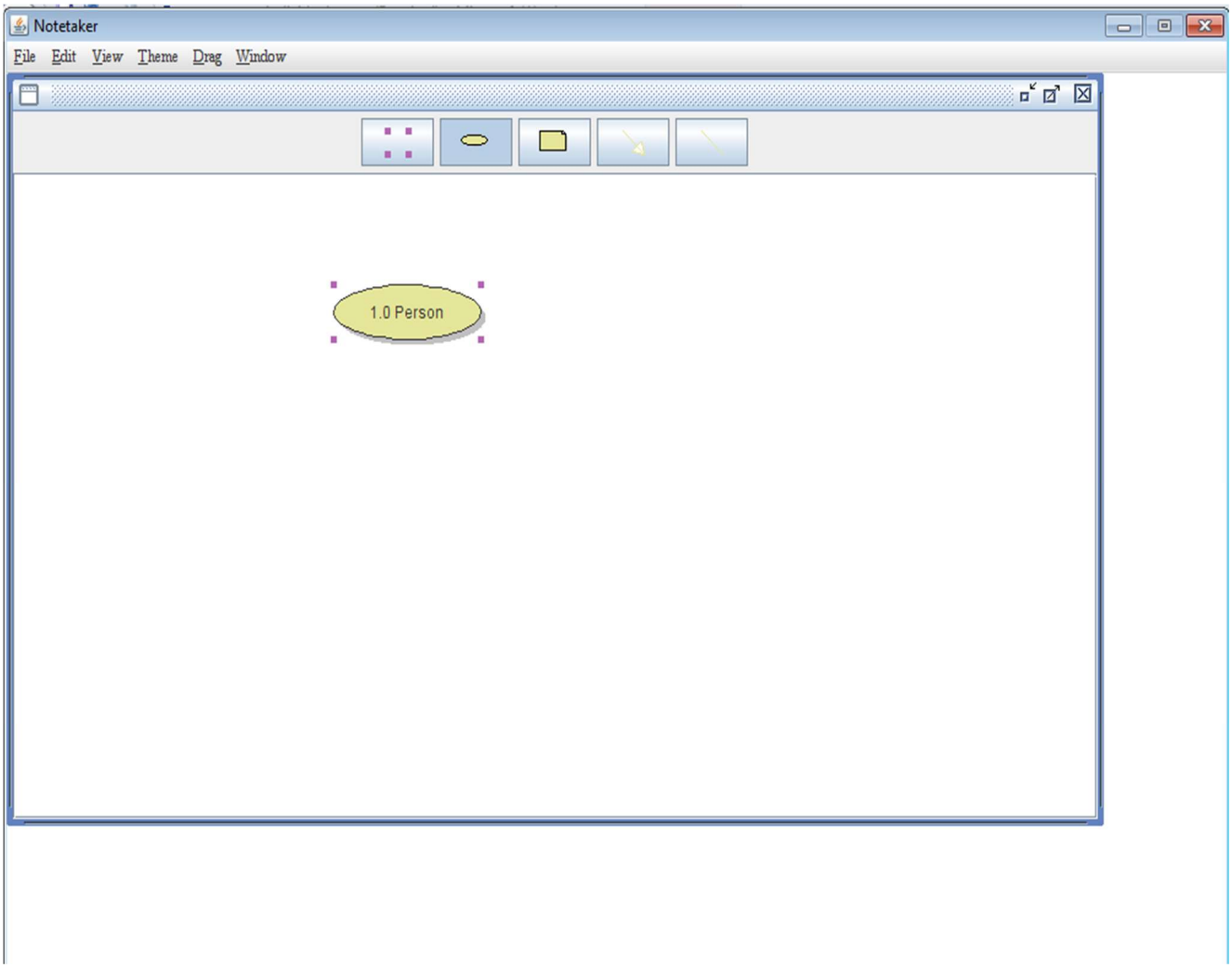
Use the following key combination: ALT+ F, ALT+N, and ALT+ N



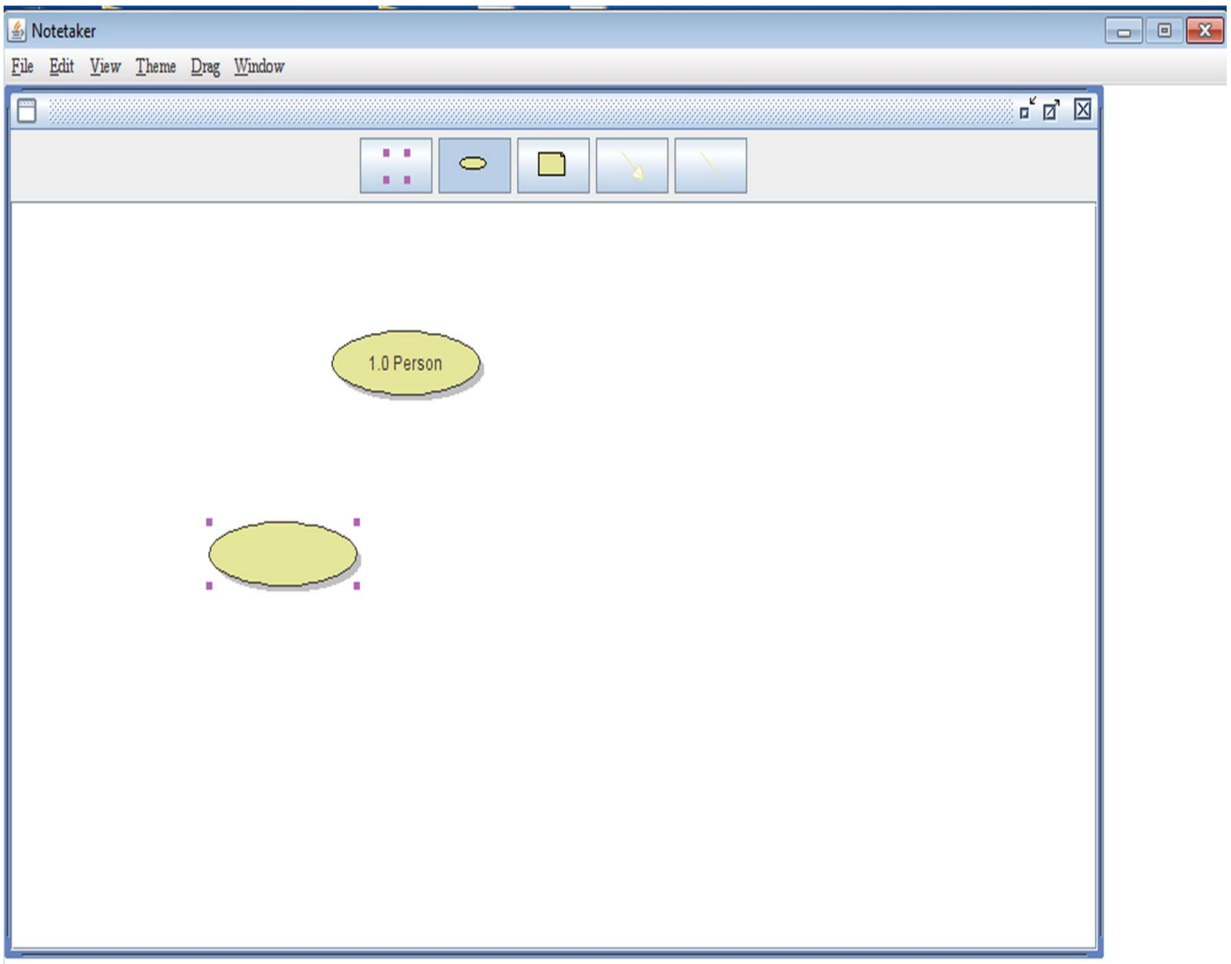
Note Taker new note view



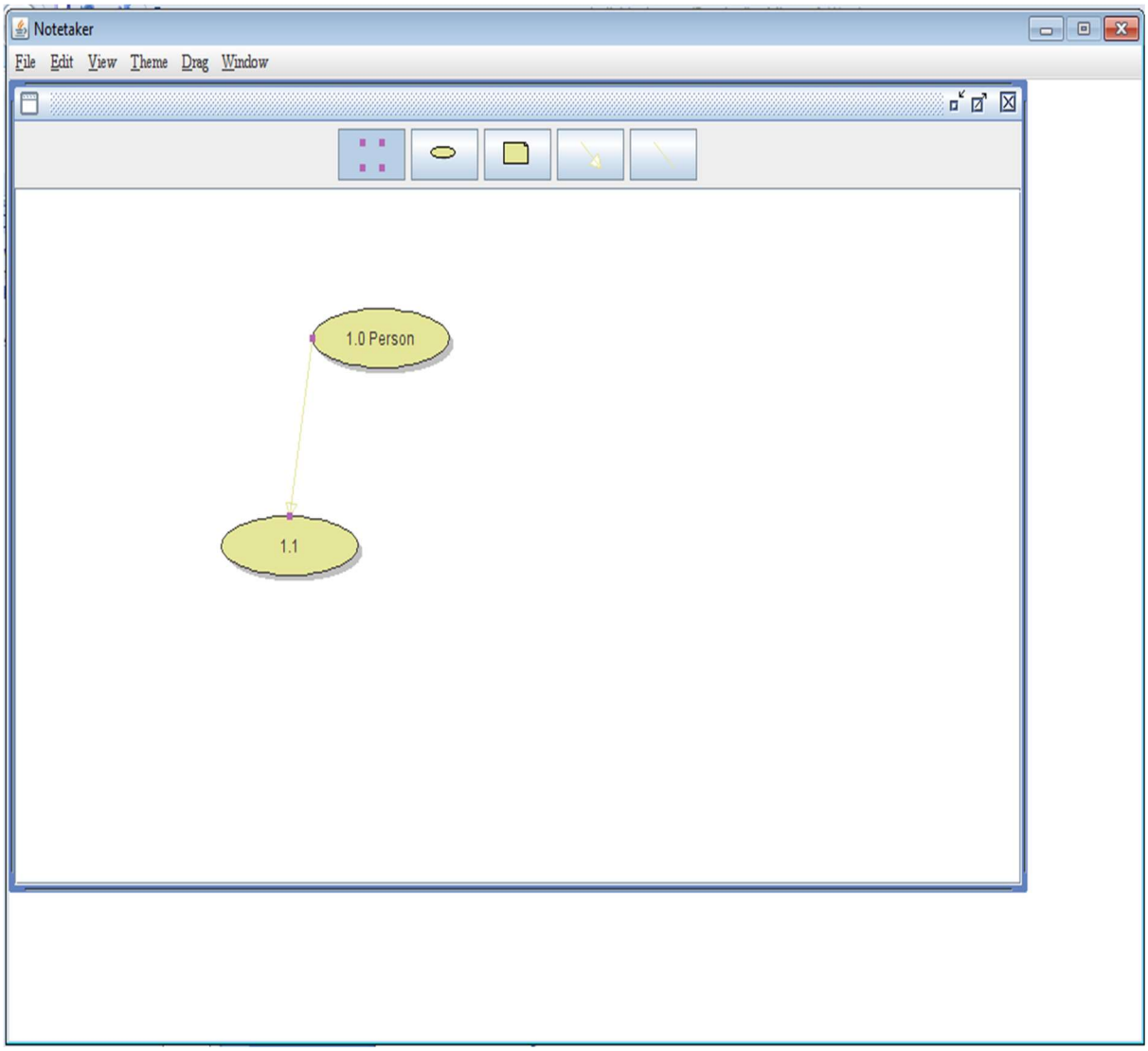
Note Taker new note view adding ellipse- after ellipse button is selected and first ellipse pasted, it is numbered automatically as 1.0.



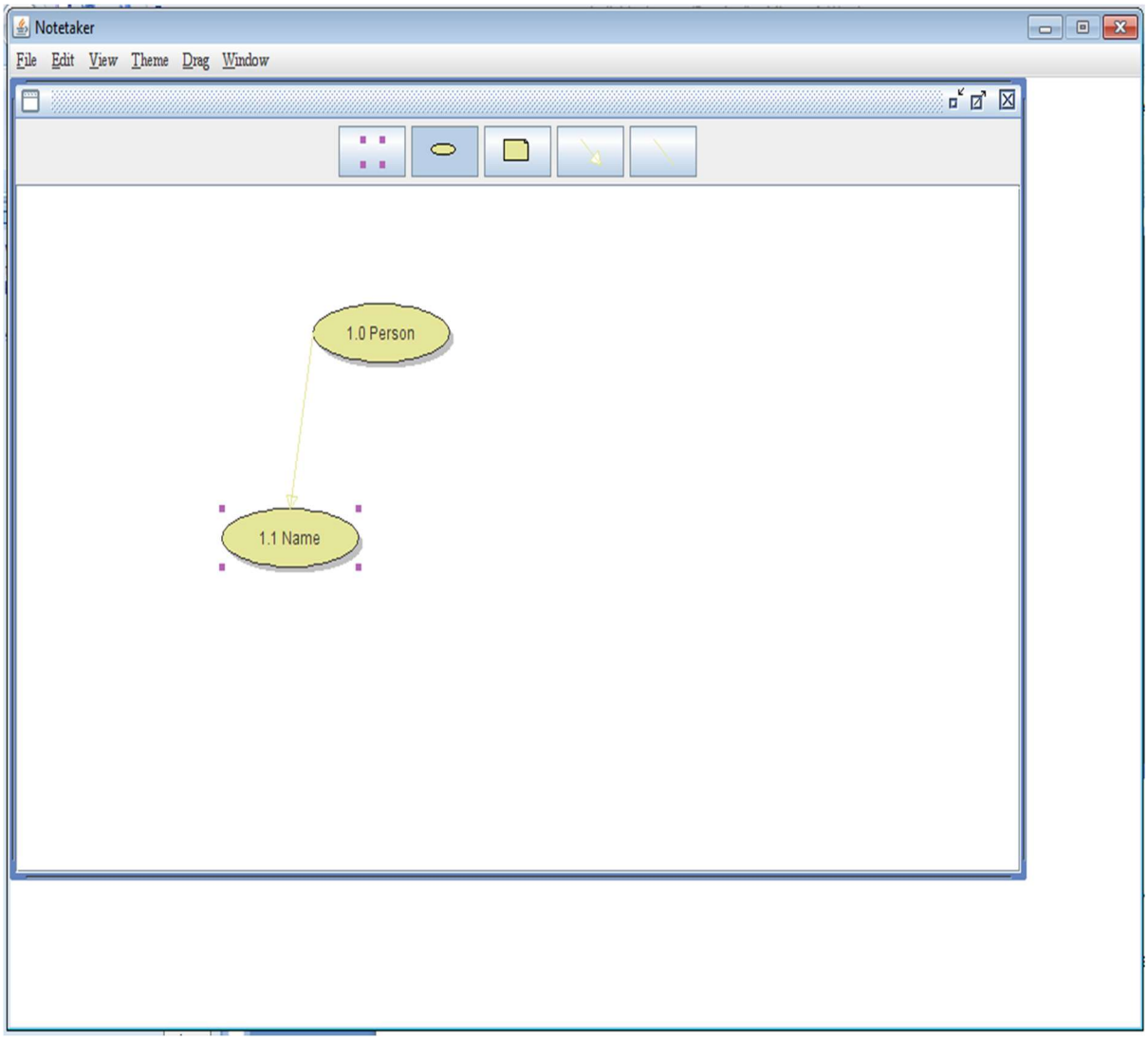
Note Taker new note view adding ellipse - after selected automatically numbered 1.0 ellipse is double clicked and the central idea, “Person” written on it in assumption of being in a meeting.



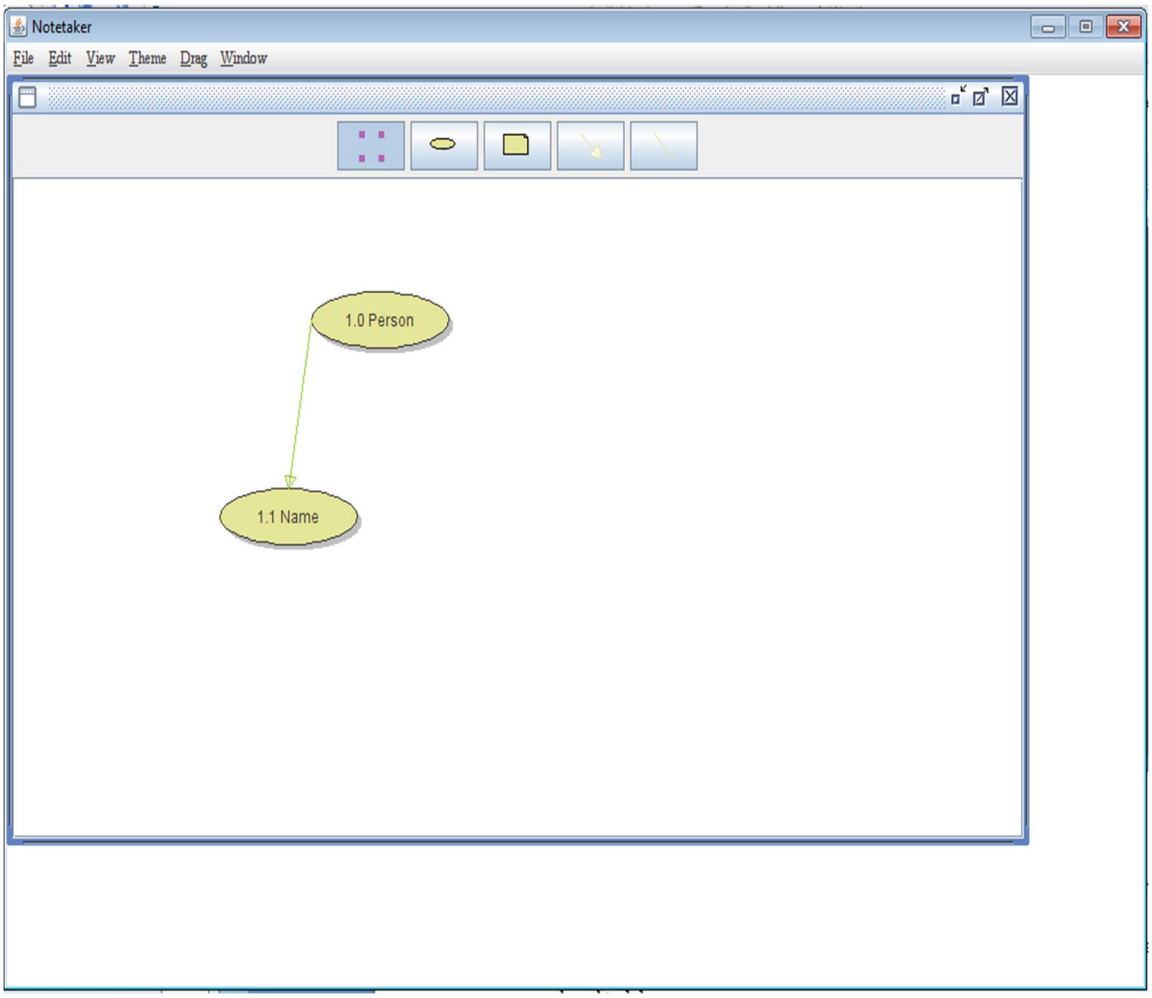
Note Taker new note view adding ellipse - after ellipse button is selected and second ellipse pasted.



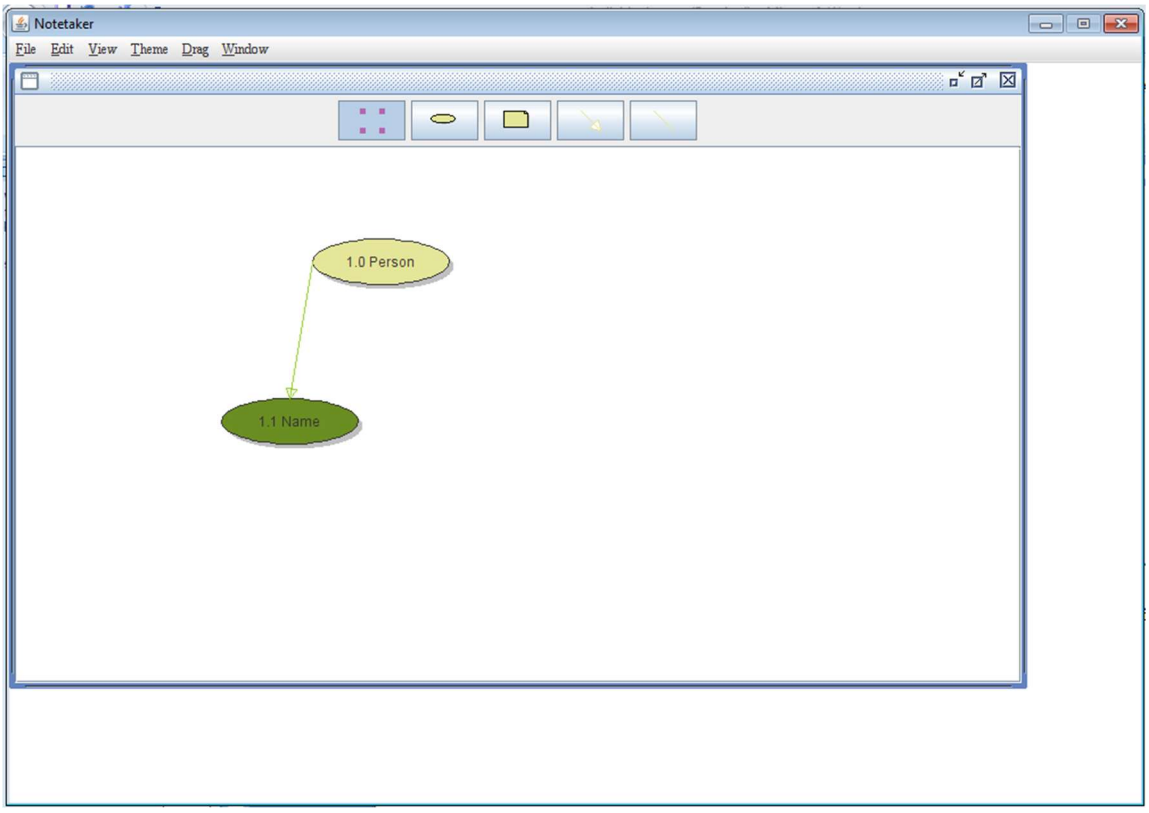
Note Taker new note view connecting ellipses with line - after line button is selected and second ellipse automatically numbered to 1.1.



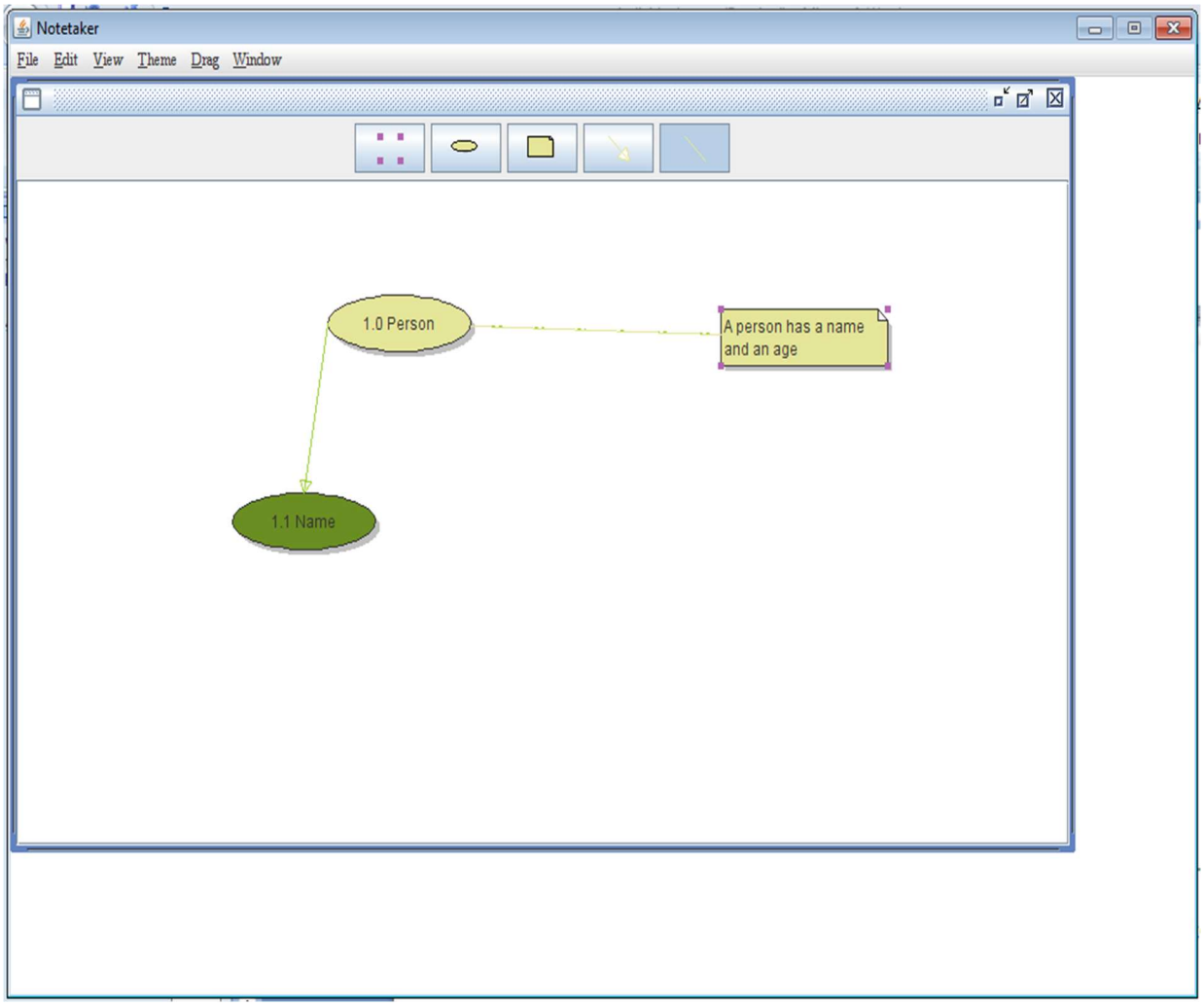
Note Taker new note view naming ellipse - after selected automatically numbered 1.1 ellipse is double clicked and “Name”, a sub idea written on it with the joining line between the two ellipses showing relationship.



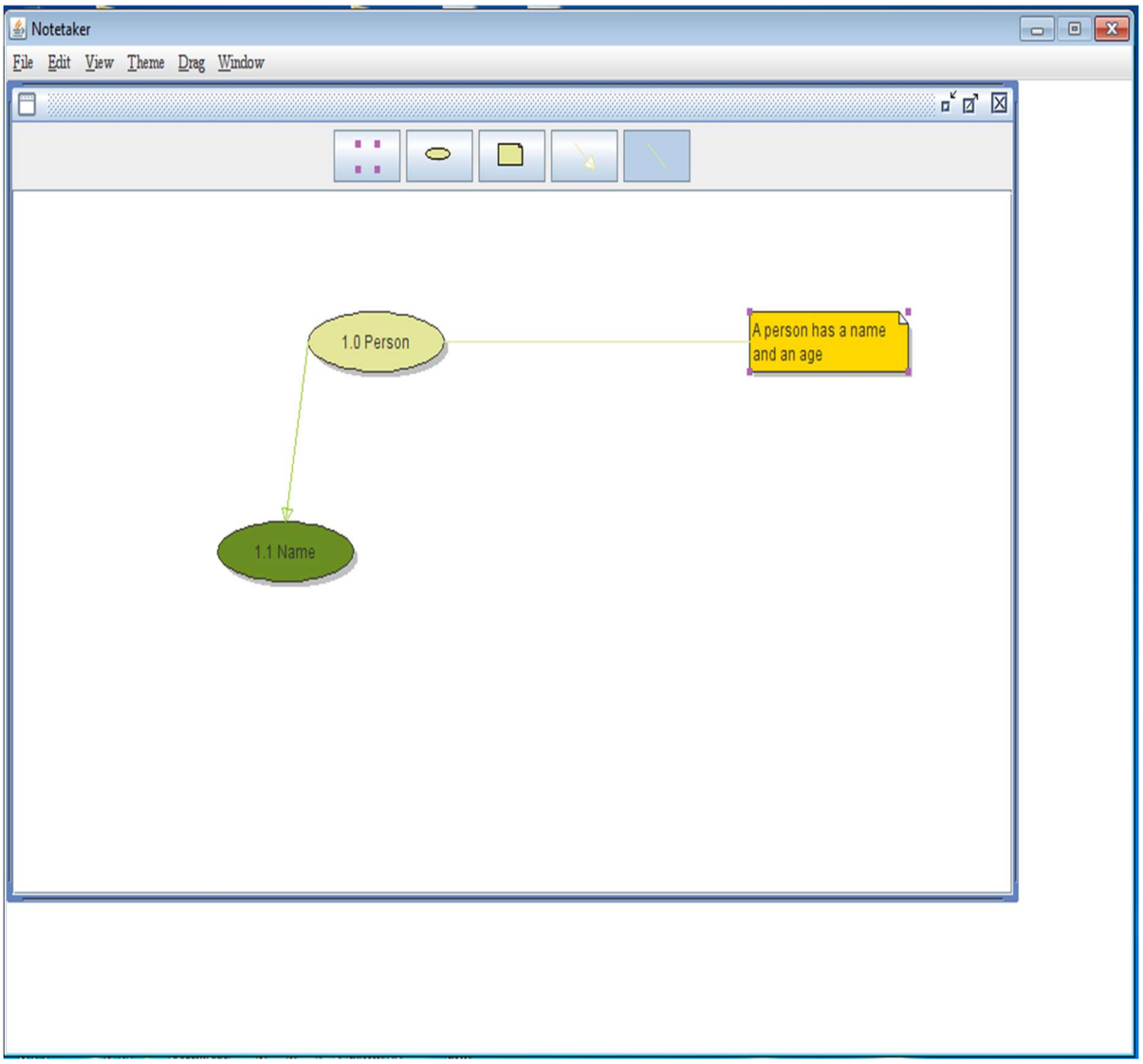
Note Taker new note view changing line color- after selecting line, the edit menu is clicked and the color sub menu is selected and color is change from yellow to green by selecting from the color drop down.



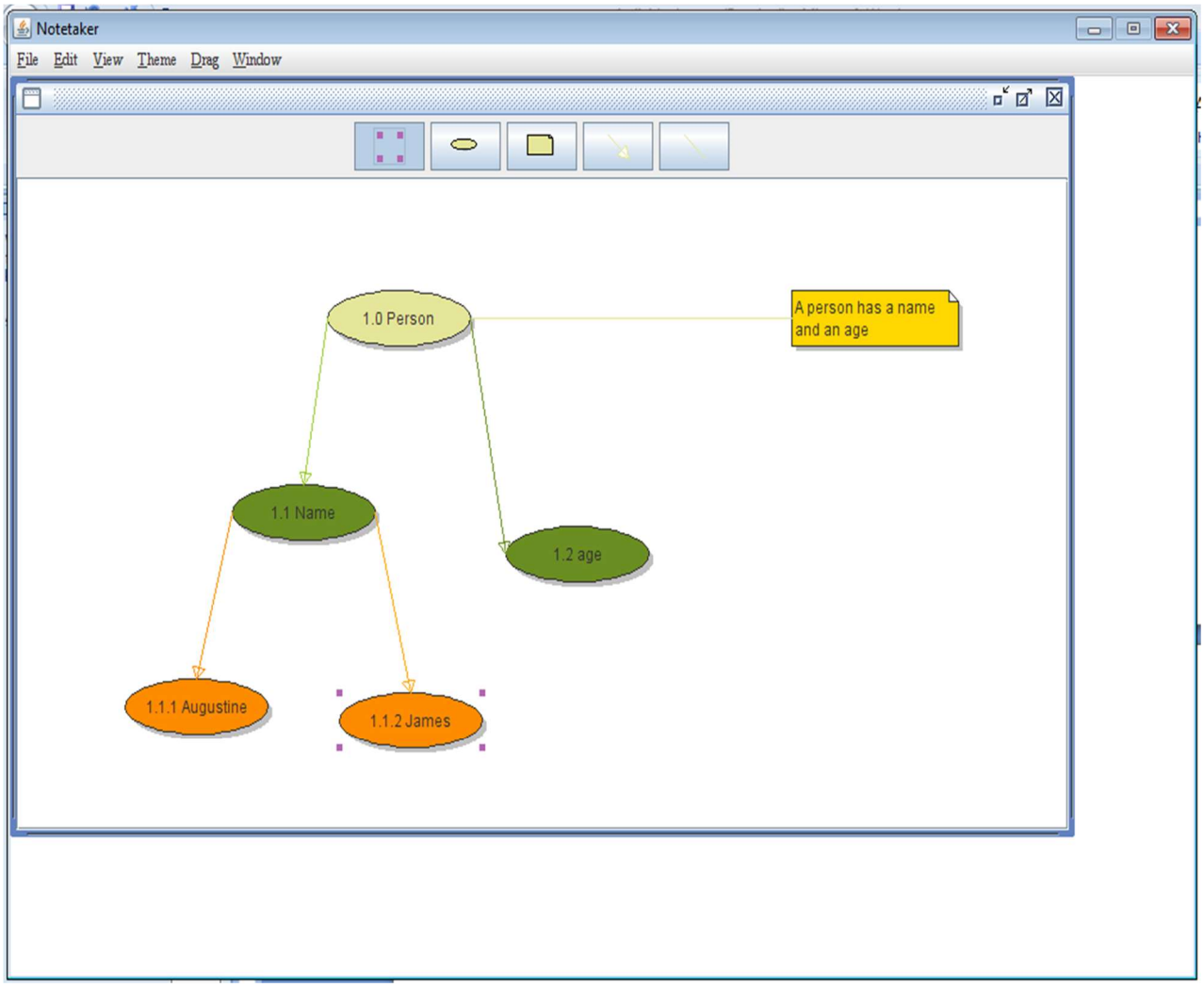
Note Taker new note view changing ellipse color- after selecting ellipse “1.1 Name”, the edit menu is clicked and the color sub menu is selected and color is change from yellow to green by selecting from the color drop down.



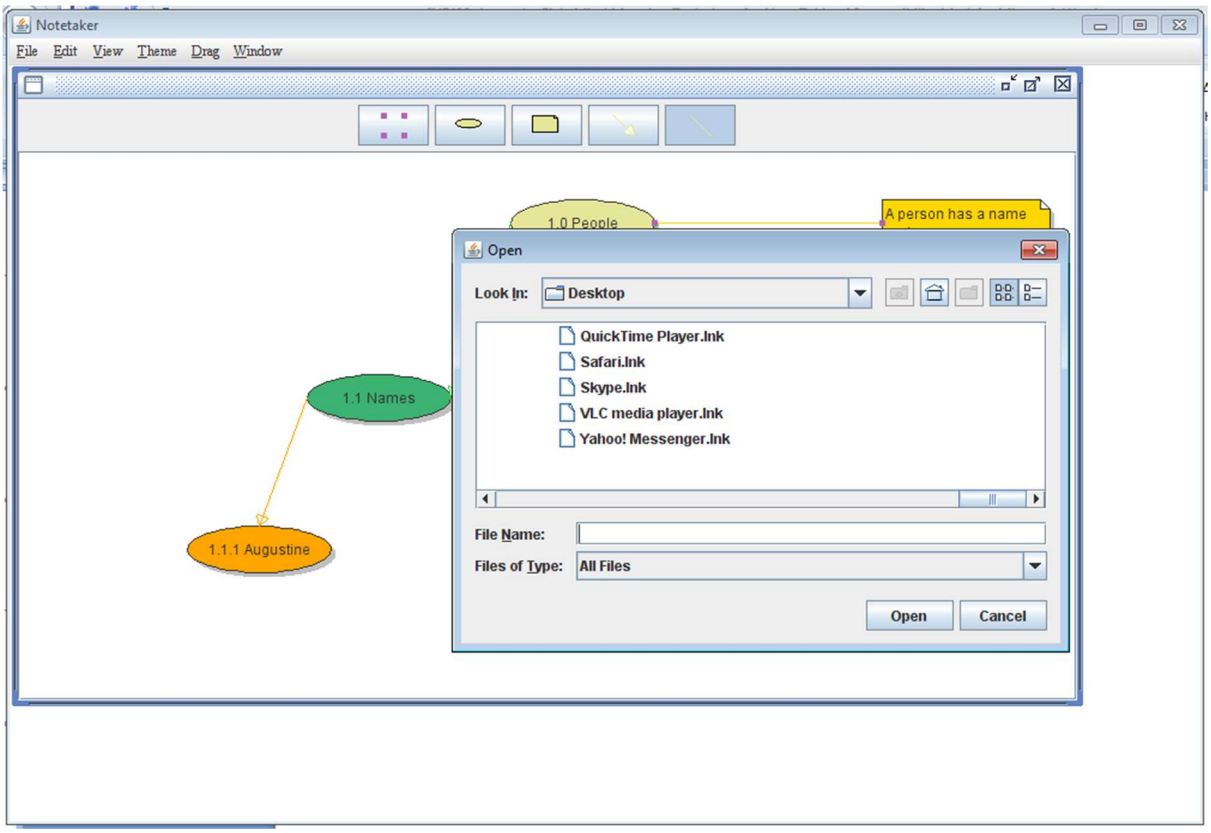
Note Taker new note view adding rectangle - after rectangle button is selected and rectangle pasted. After line button is selected and drag from the ellipse to the pasted rectangle. The rectangle is doubled clicked and text written on it.



Note Taker new note view changing rectangle's color- After the line drag from the ellipse to the pasted rectangle or the rectangle itself is selected, the edit menu is clicked and the color sub menu is selected and color is change from yellow to green by selecting from the color drop down.



Note Taker new note view fully mapped- With various combination of the procedure describe above, a mind mapping of a meeting discussion about the topic person would look like the diagram shown above.



Note Taker new note view to open saved file- To open saved files follow the path below

File →Open or

Use the following key combination: ALT+ F, ALT+O

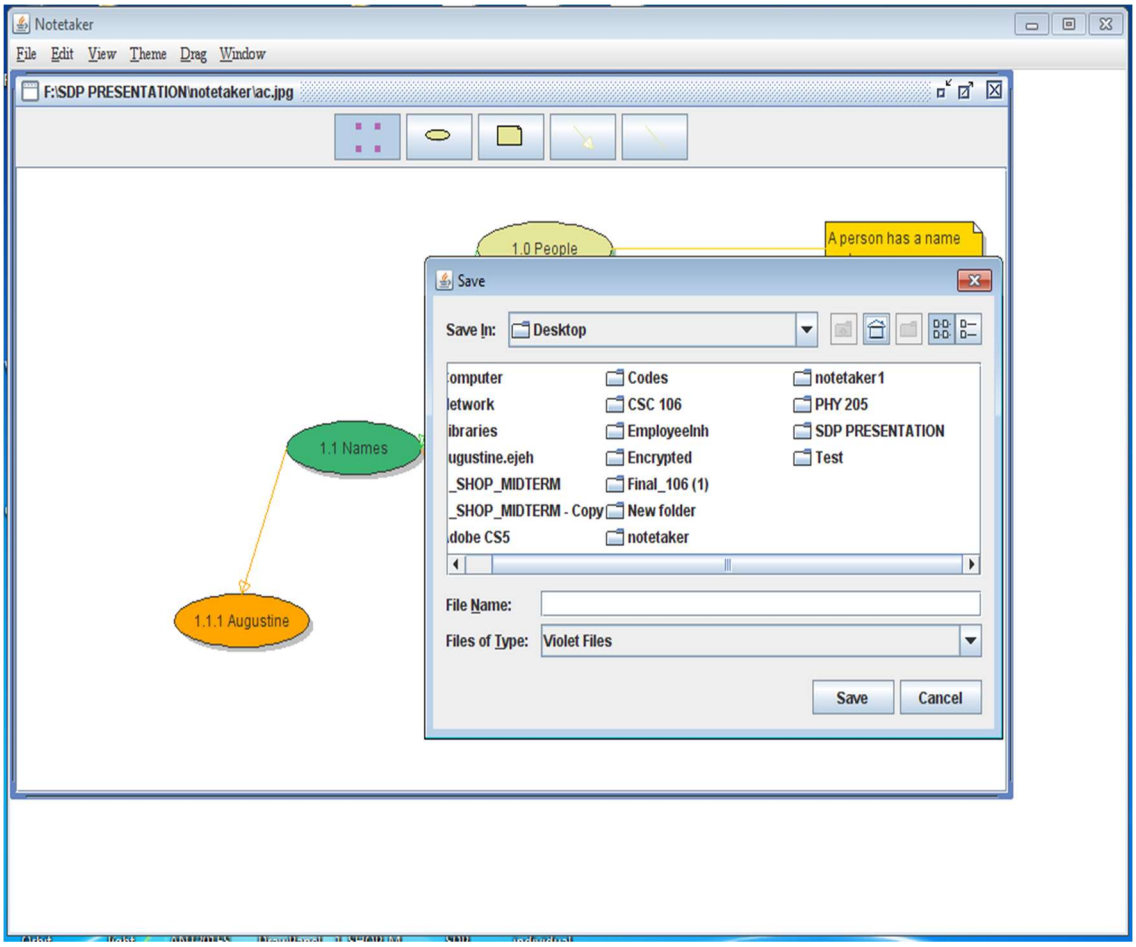
which presents the option-view above for viewing selected saved image.

Recent files can also be opened by following the path below

File →Recent files or

Use the following key combination: ALT+ F, ALT+R

which present the option-view above for viewing selected saved image.



Note Taker new note view to saved files- To saved files follow the path below

File →Save or

Use the following key combination: ALT+ F, ALT+S

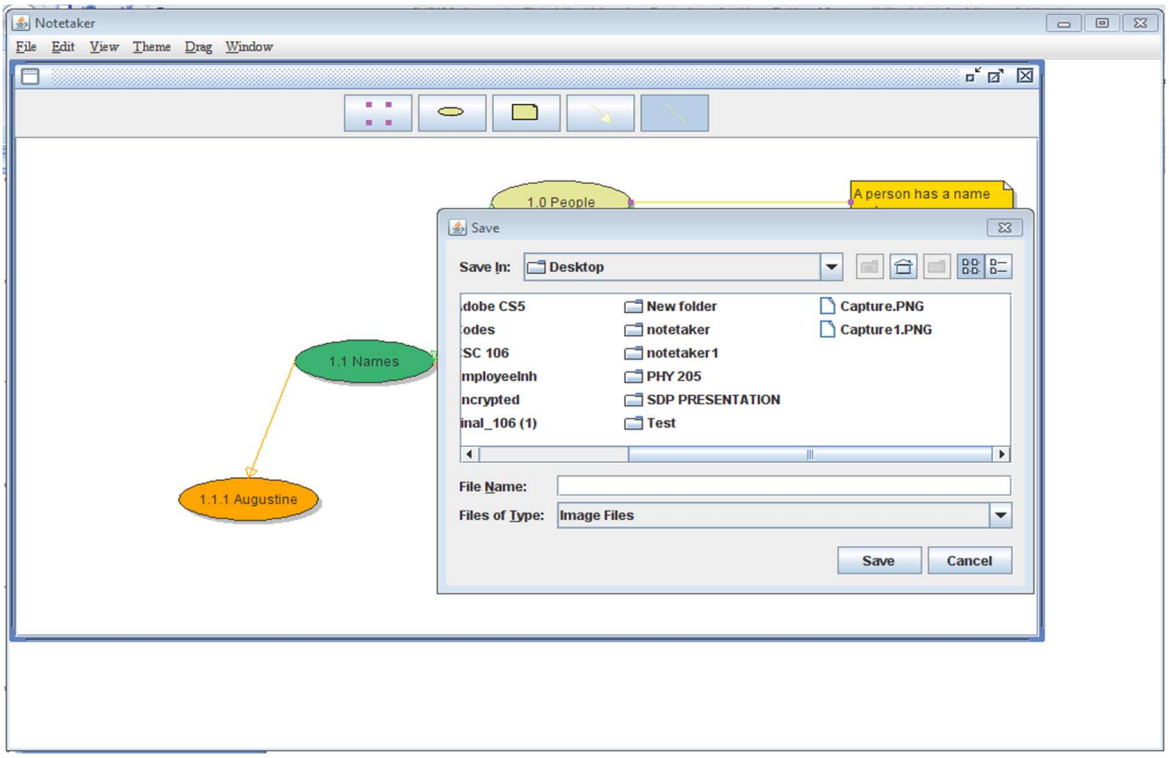
which presents the option-view above to select location to saved image.

File →Save as or

Use the following key combination: ALT+ F, ALT+A

which presents the option-view above to select location to saved image in other chosen format.

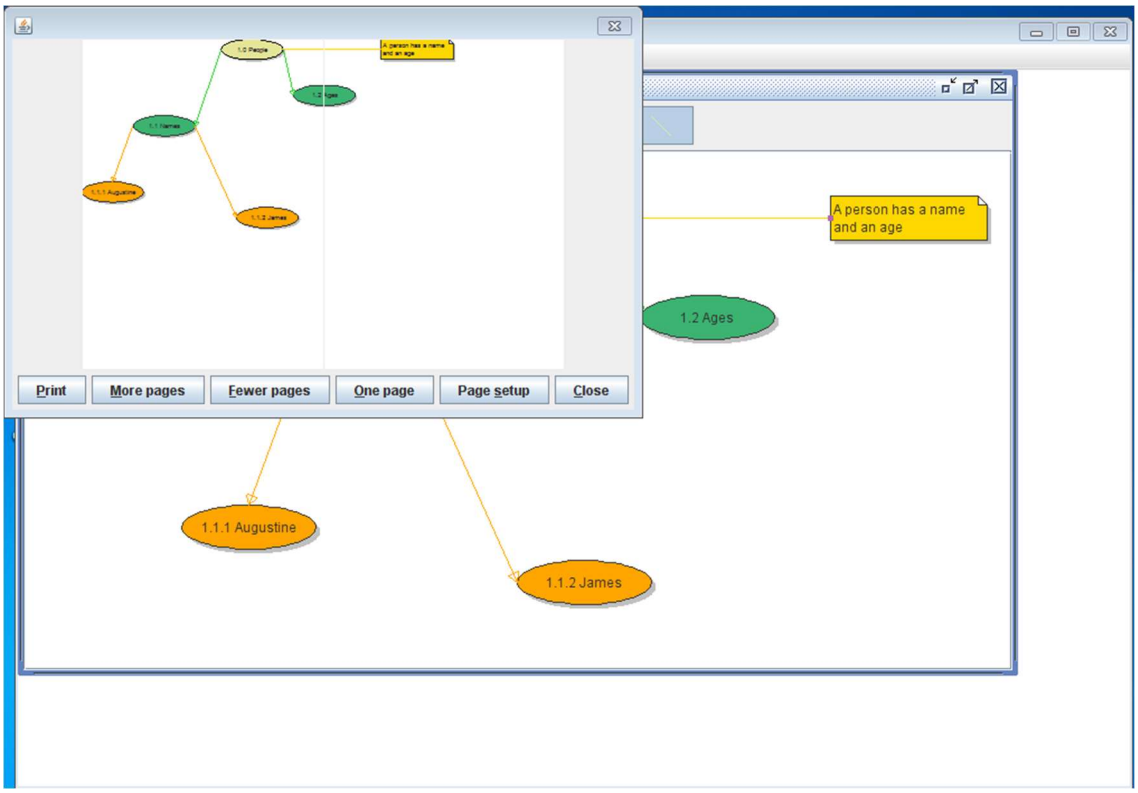
To enable the transition to electronic document, works can be printed, exported to image to be used on other application like Microsoft words, power point, etc.



Note Taker new note view to export image- To save the current note as image files either jpg or png or jpeg follow the path below

File →Export Image which presents the option view above for image saving in other format or

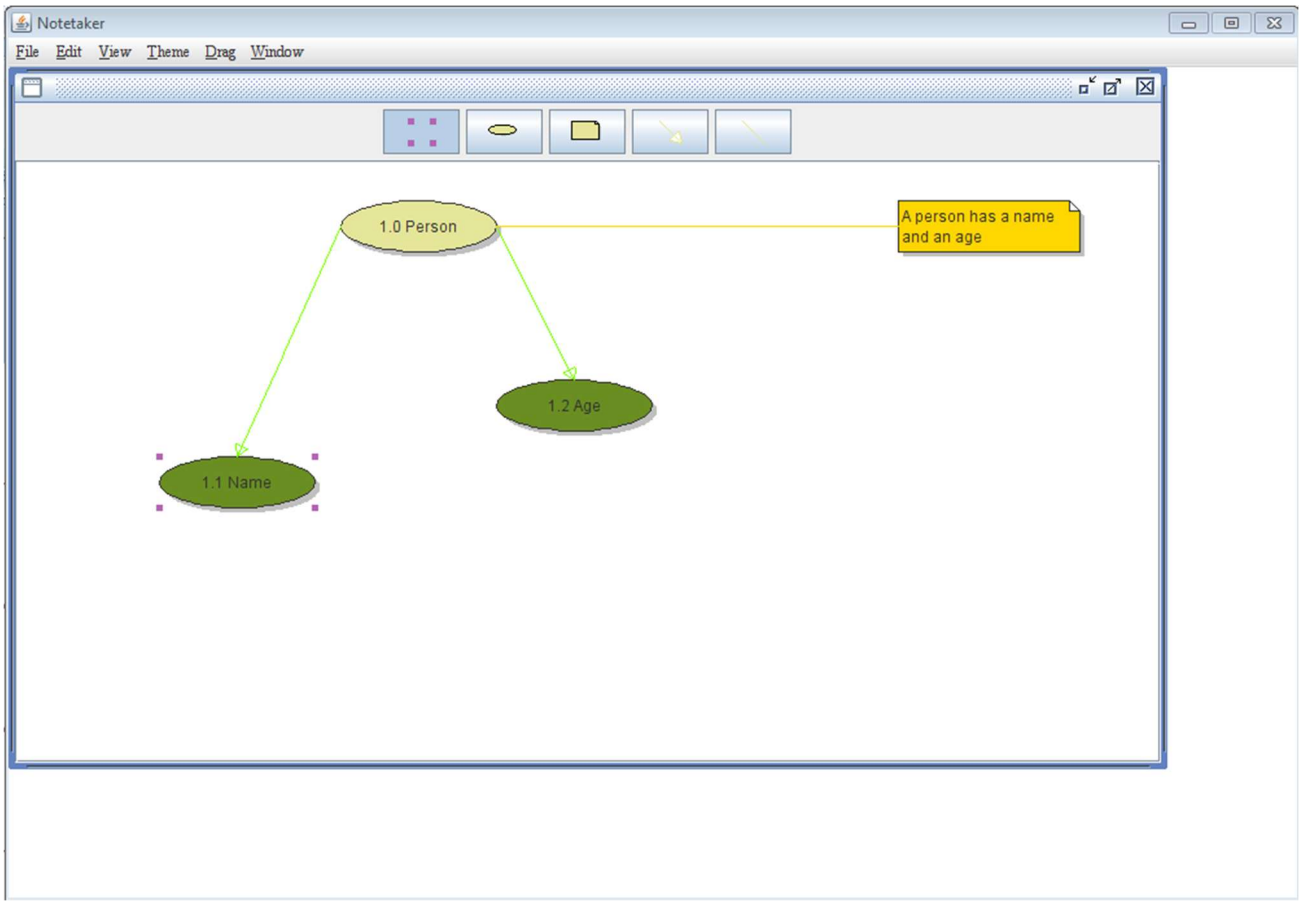
Use the following key combination: ALT+ F, ALT+E.



Note Taker new note view to print image- To sent the current note to printer follow the path below

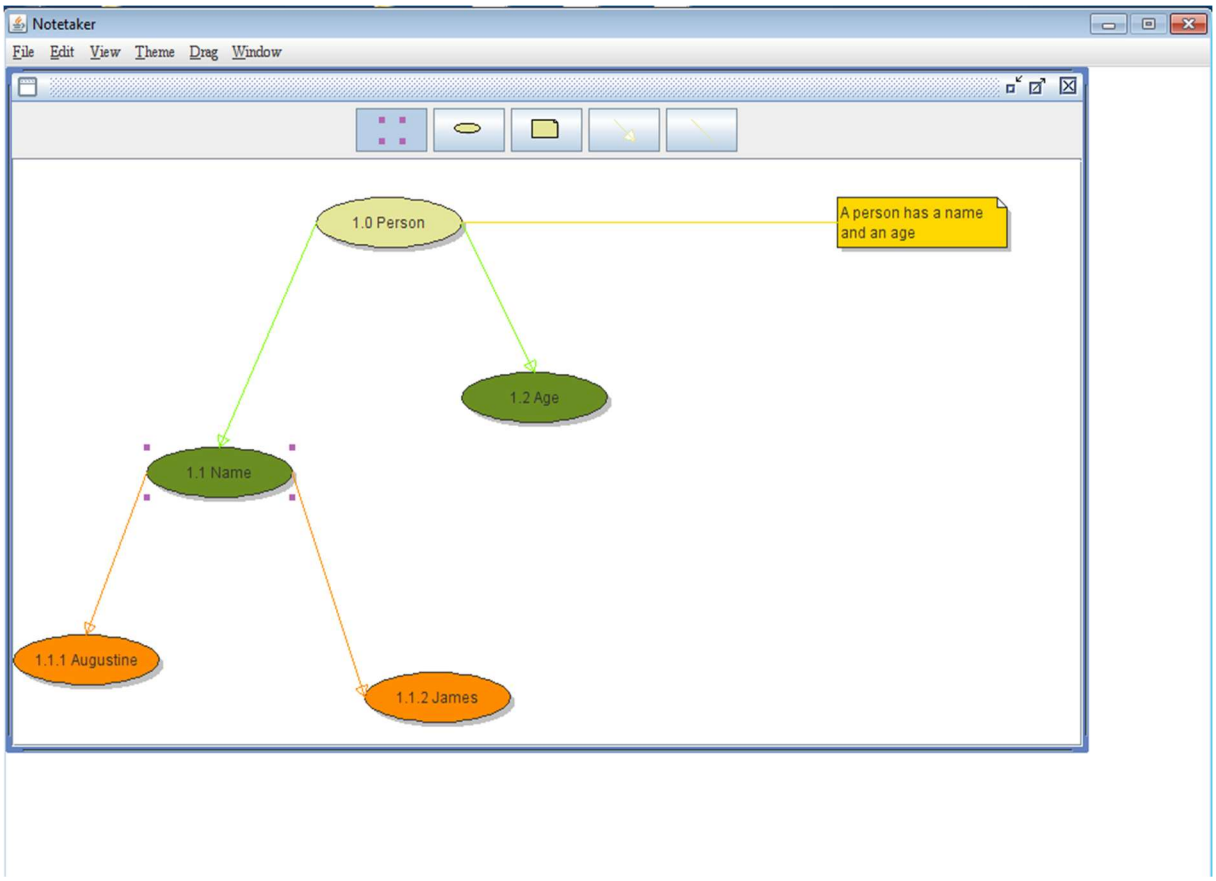
File →Print which presents the view above for printing option to be selected or

Use the following key combination: ALT+ F, ALT+P



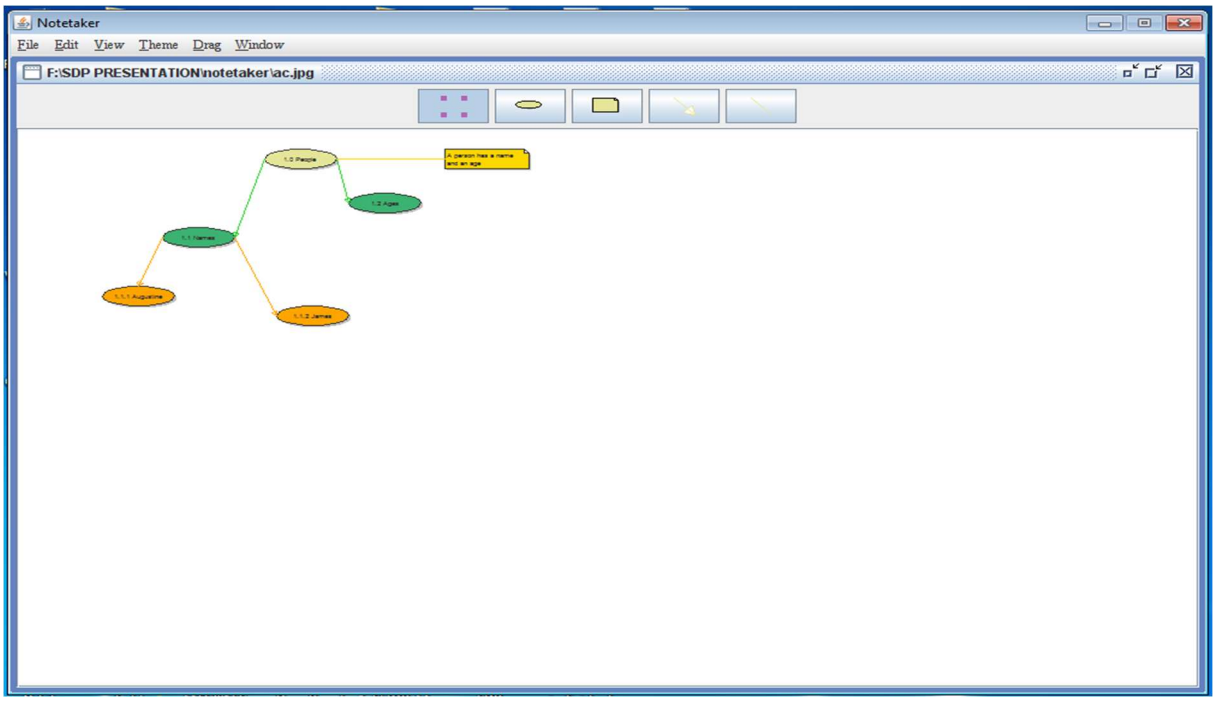
Note Taker new note view to collapse sub ideas- By following the path Edit→ Collapse or using the keyboard combination Ctrl + C

and selecting the ellipse whose sub-ellipse you want to collapse, for my case is label “1.1 Name”, the collapse sub menu can be used to collapse any sub-ideas except the main idea.



Note Taker new note view to expand collapsed sub-ideas- By following the path Edit→ Expand or using the keyboard combination Ctrl + E

and selecting the ellipse whose sub-ellipses was collapse, for my case is label “1.1 Name”, the expand sub menu can be used to expand any sub-ideas from the selected idea.

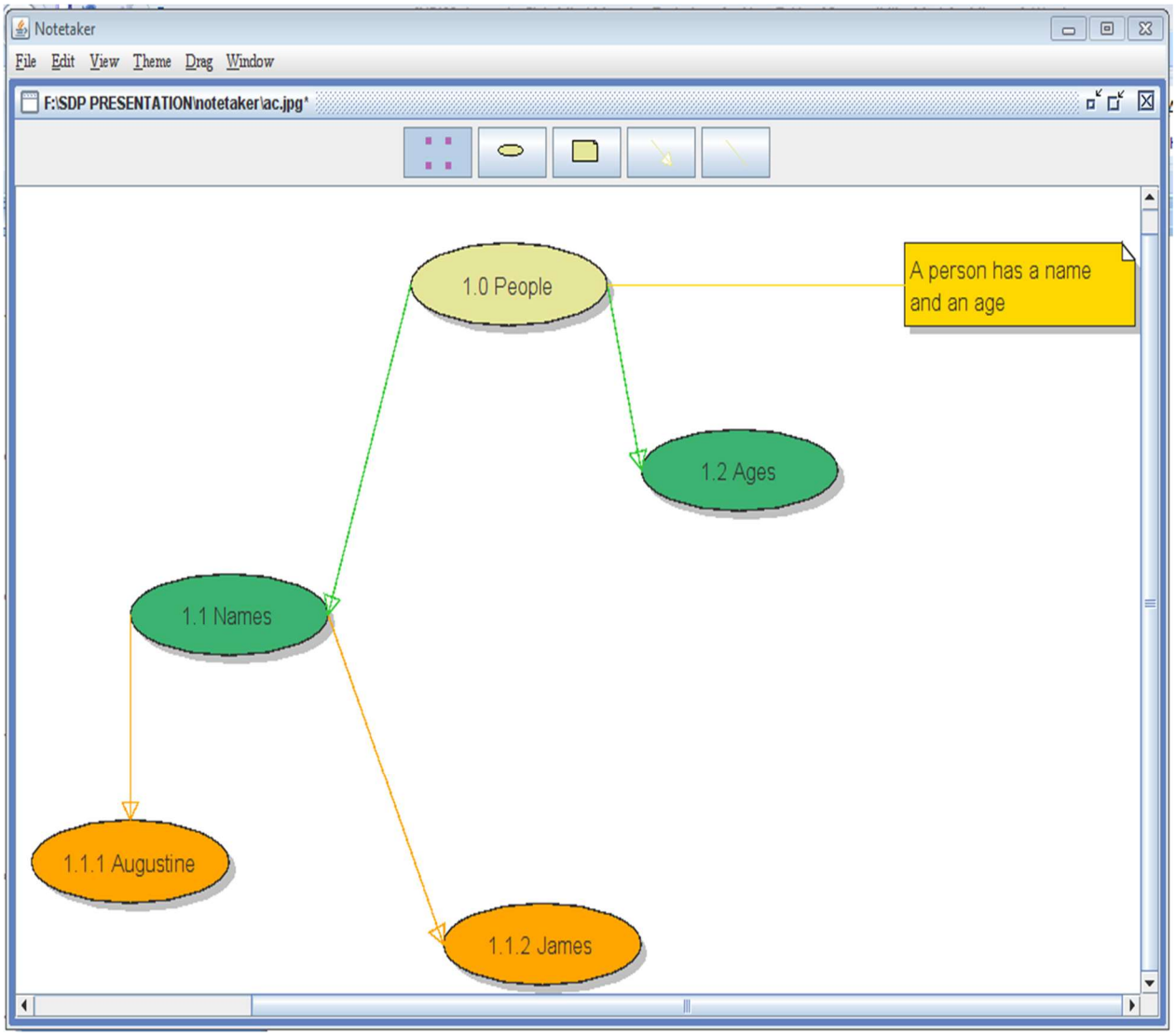


Note Taker new note view to zoom out- To reduce the size of the displayed image follow the path below.

File→View→Zoom out or

Use the following keyboard combination: ALT+ V, ALT+O or

Ctrl+ Minus

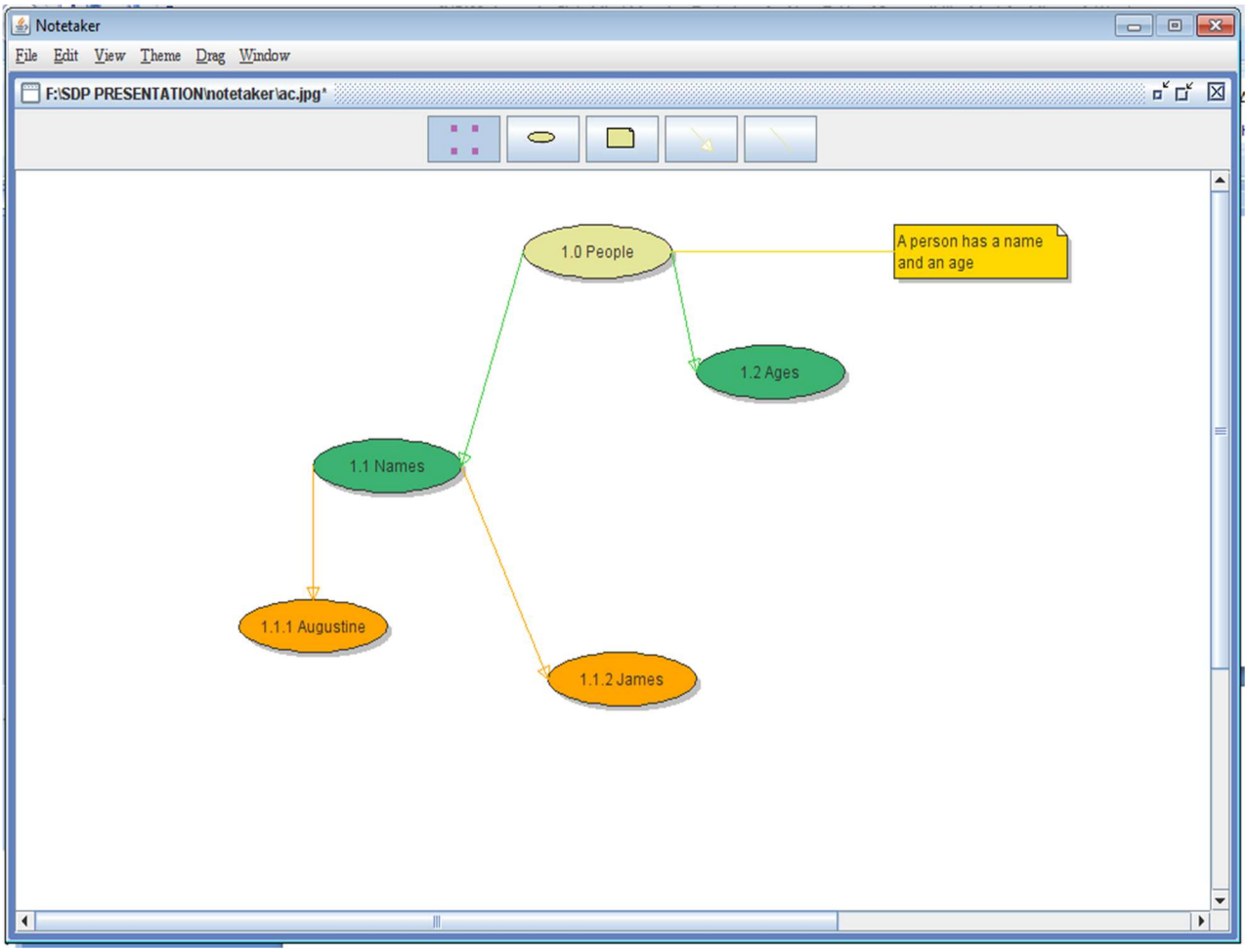


Note Taker new note view to zoom in- To increase the size of the displayed image follow the path below.

File→View→Zoom in or

Use the following keyboard combination: ALT+ V, ALT+I or

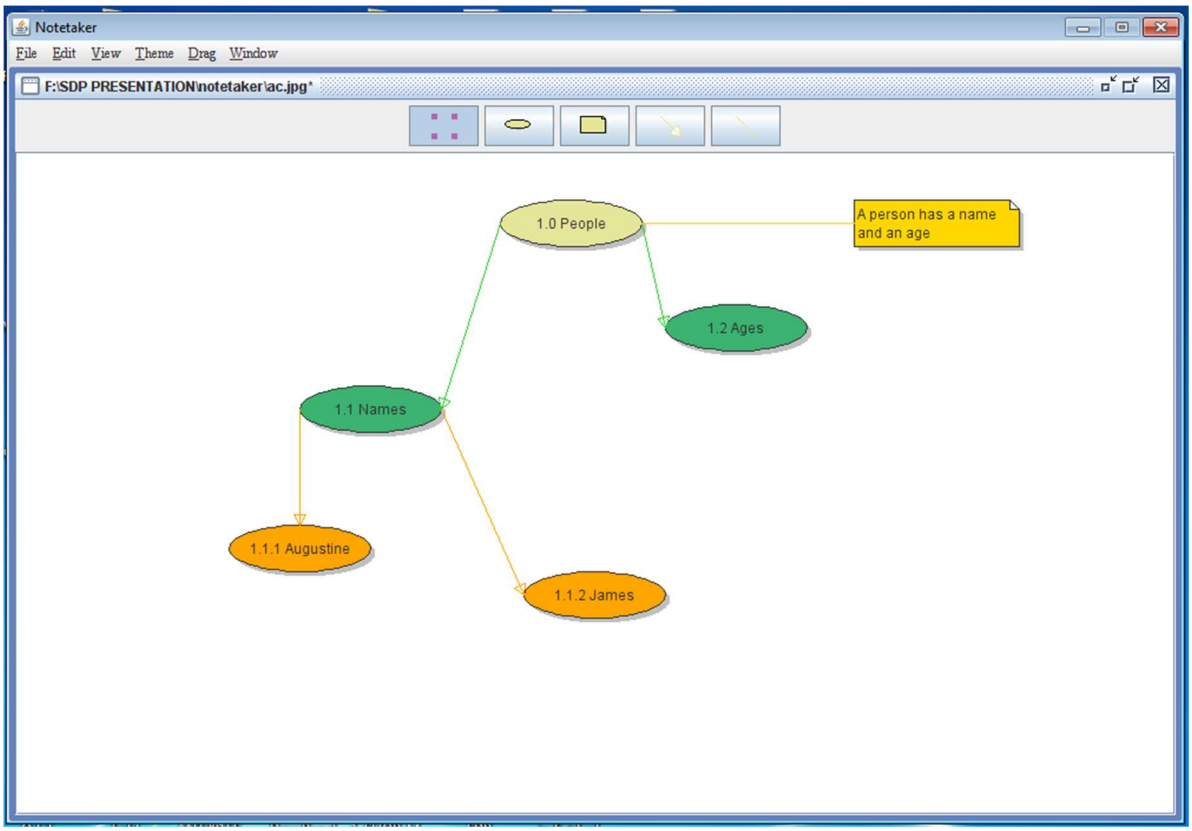
Ctrl+ Equals



Note Taker new note view to grow drawing area- To increase the size of the area to mind map follow the path below.

File→View→Grow drawing area or

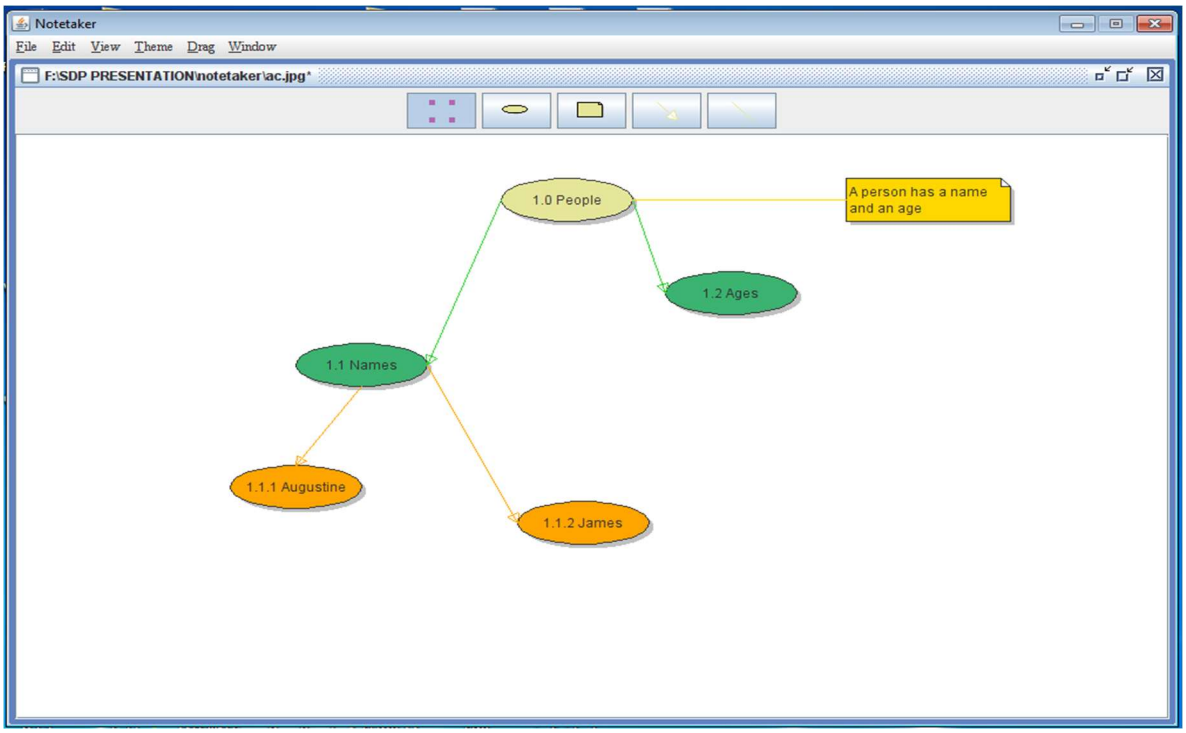
Use the following keyboard combination: ALT+ V, ALT+G



Note Taker new note view to clip drawing area- To reduce the size of the area to mind map follow the path below.

File→View→Clip drawing area or

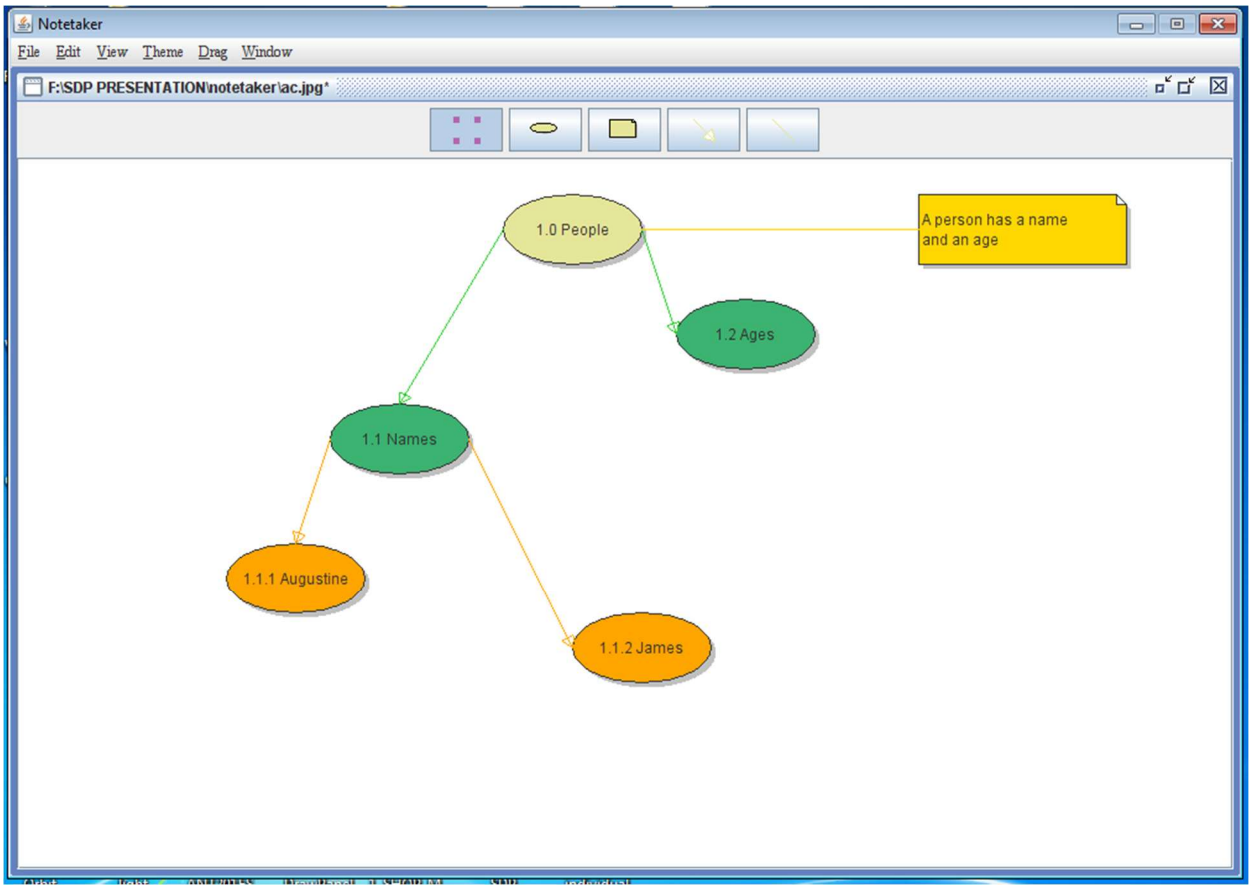
Use the following keyboard combination: ALT+ V, ALT+C



Note Taker new note view to reduce note grid- To reduce the grid of the area to mind map follow the path below.

File→View→Smaller grid or

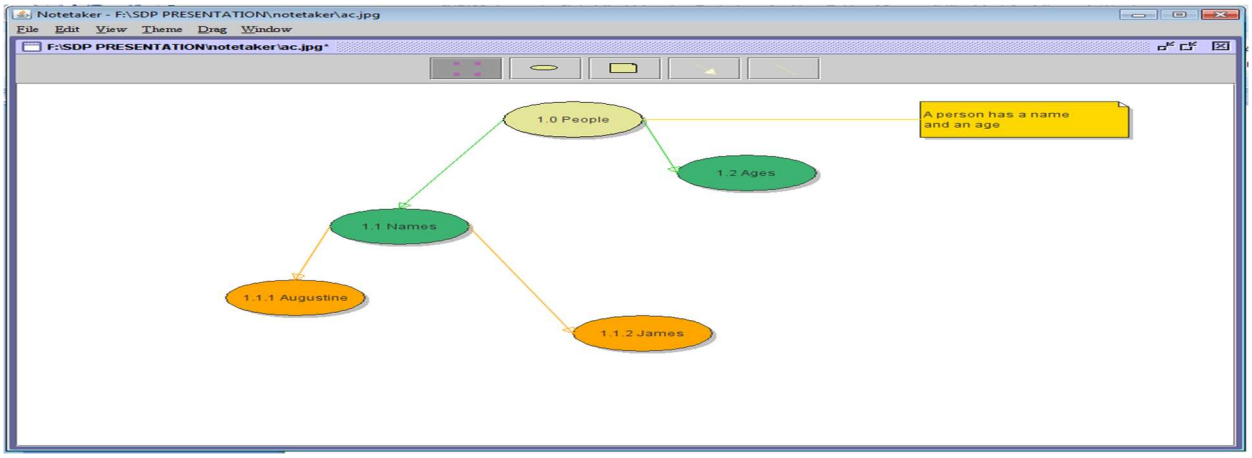
Use the following keyboard combination: ALT+ V, ALT+S



Note Taker new note view to increase note grid- To increase the grid of the area to mind map follow the path below.

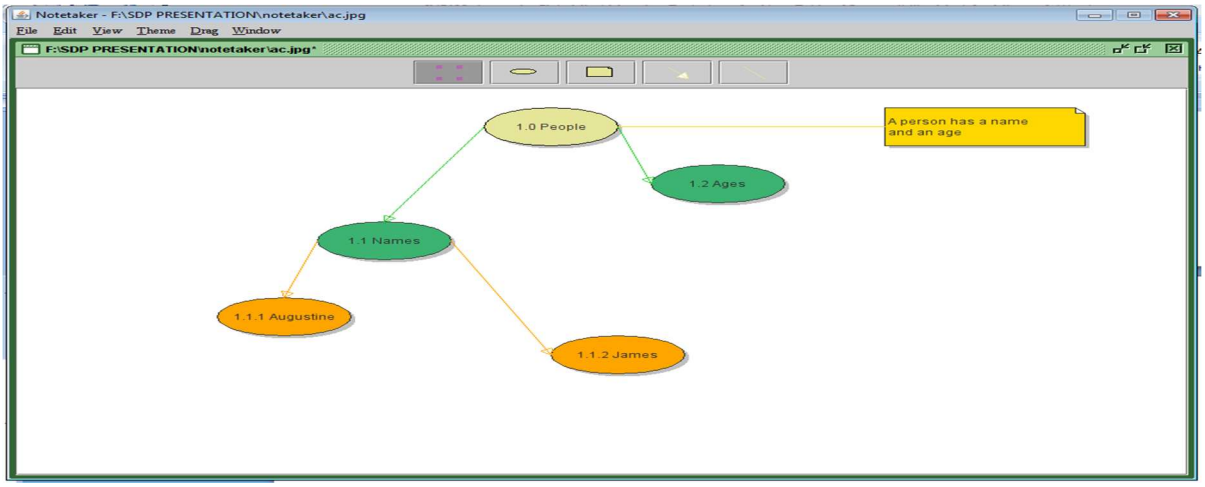
File→View→Larger grid or

Use the following keyboard combination: ALT+ V, ALT+L



Note Taker new note view to change to Steel theme- To change the theme of the note taker follow the path below.

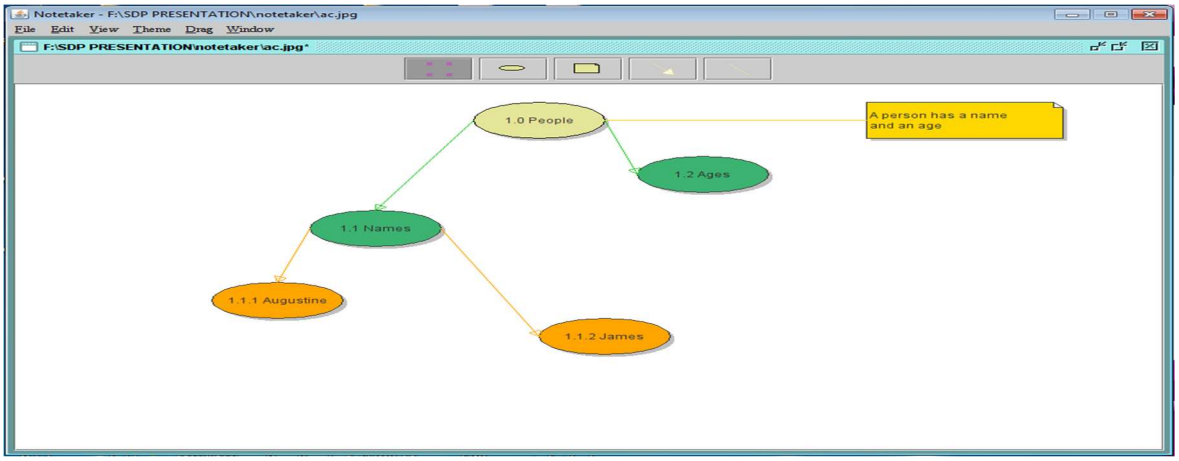
Theme→Steel or Use the following keyboard combination: ALT+ T, Select Steel



Note Taker new note view to change to Emerald theme - To change the theme of the note taker follow the path below.

Theme→Emerald or

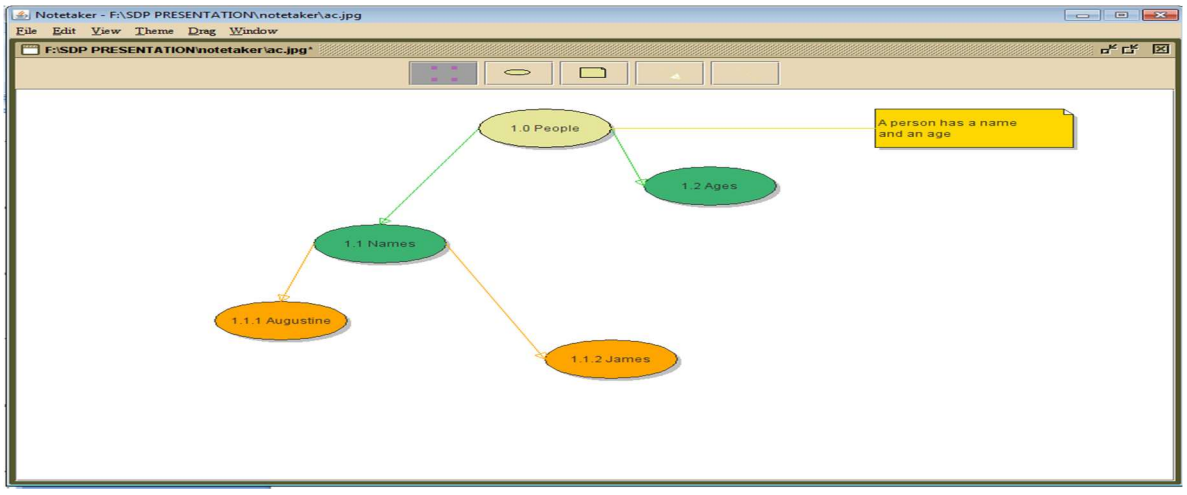
Use the following keyboard combination: ALT+ T, Select Emerald



Note Taker new note view to change to Oxide theme - To change the theme of the note taker follow the path below.

Theme→Oxide or

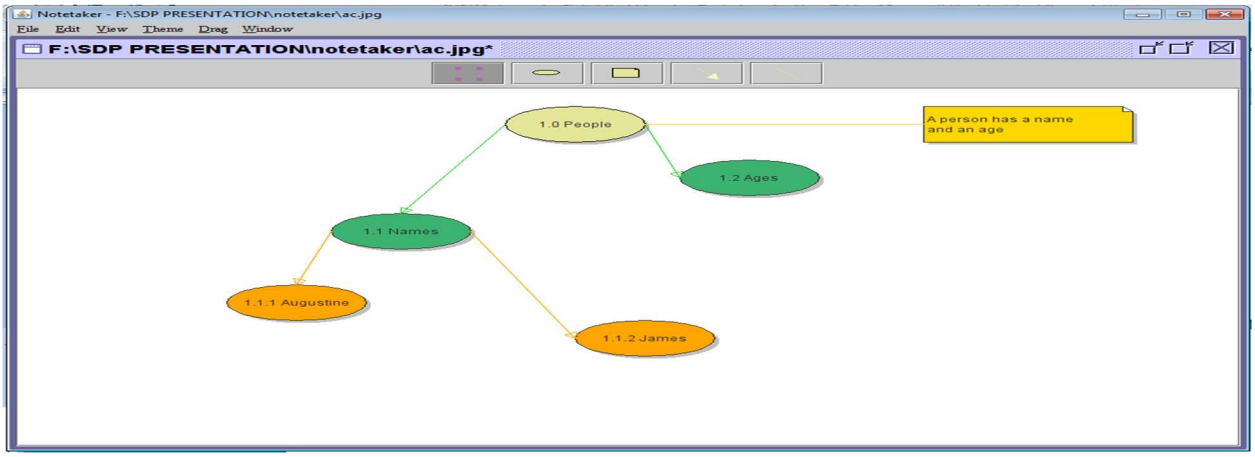
Use the following keyboard combination: ALT+ T, Select Oxide



Note Taker new note view to change to Sandstone theme - To change the theme of the note taker follow the path below.

Theme→Sandstone or

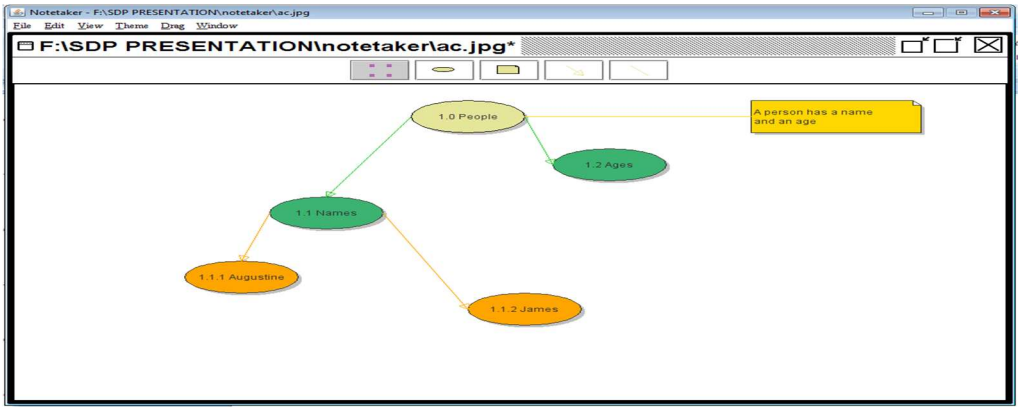
Use the following keyboard combination: ALT+ T, Select Sandstone



Note Taker new note view to change to Presentatiion theme - To change the theme of the note taker follow the path below.

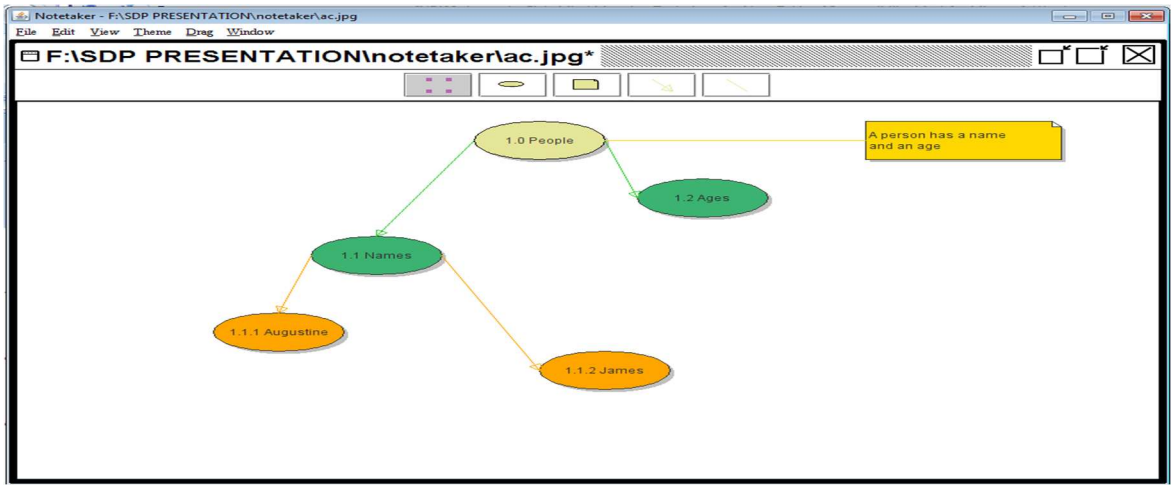
Theme→Presentation or

Use the following keyboard combination: ALT+ T, Select Presentation



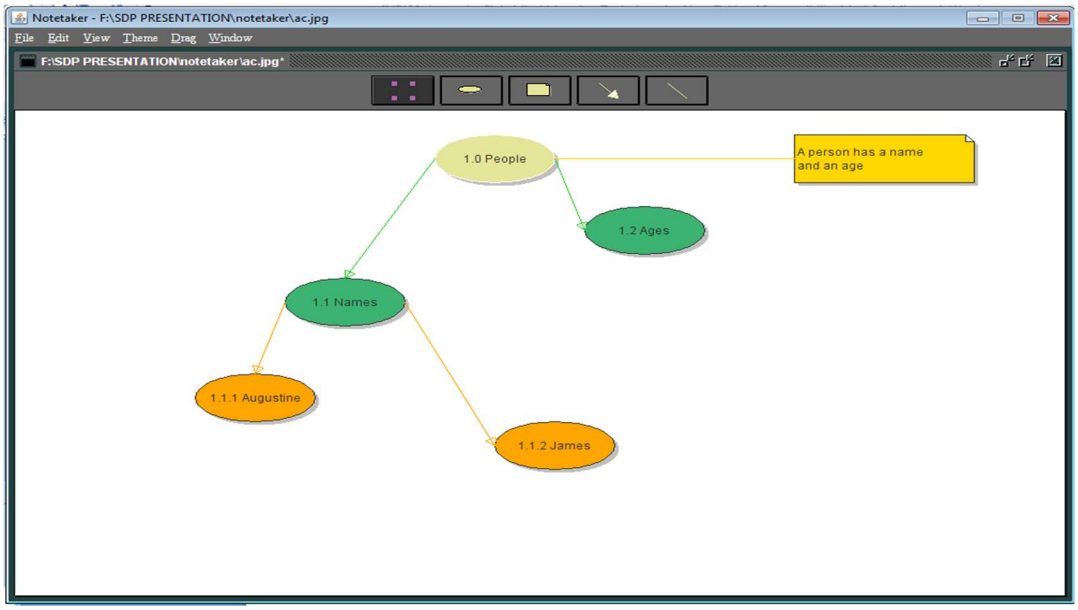
Note Taker new note view to change to contrast theme- To change the theme of the note taker follow the path below.

Theme→Contrast or Use the following keyboard combination: ALT+ T, Select Contrast



Note Taker new note view to change to Low Vision theme - To change the theme of the note taker follow the path below.

Theme→Low Vision or Use the following keyboard combination: ALT+ T, Select Low Vision.



Note Taker new note view to change to Charcoal theme - To change the theme of the note taker follow the path below.

Theme→Charcoal or Use the following keyboard combination: ALT+ T, Select Charcoal.

Running time for the program.

Total implicit running time for adding new node + adding new edge:

$O(1)+O(n)=O(n)$

Total average explicit running time for the whole program: 1579

Total implicit running time for the whole program: $O(n^2)$

CONCLUSION

When mind mapping technique is applied to speeches during meeting, it results to an effective study technique when revisited to be revised since it often contains the central concepts of the course and the material most likely to be included on exams if a students or being asked by the boss if a secretary (Academic Skill Center, 2011). It improves the way you record information as well as enables the quick identity and understanding of the structure of a subject being discussed since the as you map the note you are taken it is labeled in an hierarchically. Mind map also helps in information remembrance since it holds it in a format that your mind finds easy to recall and quick to review (Horstmann, C., 1996). However, consideration has to be given towards ways of motivating mind maps amongst users before mind maps are generally adopted as a study technique (Farrand, P., Hussain, F and Hennessy, E., 2002).

SUMMARY

The aim of this project which is to provide a mind mapping technique for note taking through the use of computers and other technologies has been set in motion by the implementation of the Note Taker System and the full purpose will be achieved in the future when the program is improved further following the previously mentioned future prospects.

The program mimics the way the brain and mind works. The GUI (Graphical User Interface) has been designed to be simple and well structured so as to provide better convenience for users of the system. Also the method of idea holder and idea connector holder selection has been made easier by the provision of grabber tools. This is to make the user think with the help of the program and to reduce time since it is hierarchically labeled as the note is taken mostly immediately and requires quick decision making.

REFERENCES

1. Academic Skill Center (2011). *Classes: Note taking, Listening, Participation*. Retrieved from http://www.dartmouth.edu/~acskills/success/notes.html. Retrieved on 13/11/2011.
2. Buzan, T., (1995). Use Your Head.
3. Dryden, G., Ves, J. (1999). *Mind Mapping: Improve your note-taking and creativity.* Retrieved from http://www.thelearningweb.net/mind-mapping.html.
4. Farrand, P.; Hussain, F.; Hennessy, E. (2002). *The efficacy of the mind map study technique: Medical Education* 36 (5): 426–431.doi:10.1046/j.1365-2923.2002.01205.x. PMID 12028392. Retrieved 2009-02-16.
5. Garret, C. (August 28, 2007). *Using Mind Maps for Creativity, Note-Taking and*
    a. *Productivity*. Retrieved from http://www.cogniview.com/convert-pdf-to-excel/post/using-mind-maps-for-creativity-note-taking-and-productivity/
6. Horstmann, C. (1996). *Mind Maps: A Powerful Approach to Note-Taking.* Retrieved from http://www.mindtools.com/pages/article/newISS_01.htm.
7. Horstmann, C (July, 2009). *Object-Oriented Design & Patterns.* Wiley. Retrieved from http://www.horstmann.com/design_and_patterns.html.

8. Hunt, A. (2009). Pragmatic Thinking and Learning: Refactor your Wetware.

9. Mind Mapping (2009). Retrieved from http://www.toolkitforthinking.com/creative-thinking/mind-mapping

10. Mohidin, F. (2010). *Using Mind Maps*. Retrieved from http://www.usingmindmaps.com/mind-map-notes.html.

11. NovaMind (May 29, 2011). *Mind Mapping for Students.* Retrieved from http://www.novamind.com/blog/2011/articles/mind-mapping-for-students/.

12. Pash, A. (2009). Life *Hacker Note taking: A Beginner's Guide to Mind Mapping Meeting*. Retrieved from http://lifehacker.com/288763/a-beginners-guide-to-mind-mapping-meetings.

13. Russel, P. (1996). *Spirit of Now.* Retrieved from http://www.peterrussell.com/MindMaps/Advantages.php.