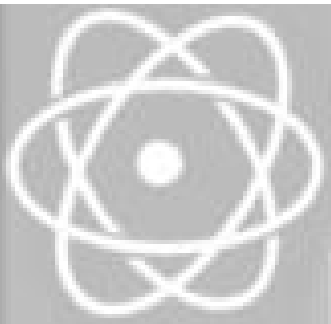


SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL5 No1
MARCH 2021

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 1-8 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

შეჭრის აღმოჩენის სისტემა 5G-სათვის

INTRUSION DETECTION SYSTEM FOR 5G

მაქსიმ იავიჩი, კავკასიის უნივერსიტეტი
Maksim Iavich, Caucasus University
გიორგი იაშვილი, კავკასიის უნივერსიტეტი
Giorgi Iashvili, Caucasus University
ავთანდილ გაგნიძე, კავკასიის უნივერსიტეტი
Avtandil Gagnidze, Caucasus University
შალვა ხუხაშვილი, სამეცნიერო კიბერ უსაფრთხოების ასოციაცია
Shalva Khukhashvili, Scientific Cyber Security Association
სერგეი სიმონოვი, სამეცნიერო კიბერ უსაფრთხოების ასოციაცია
Sergei Simonovi, Scientific Cyber Security Association

აბსტრაქტი

სატელეკომუნიკაციო ინდუსტრია მნიშვნელოვნად ვითარდება 5G ქსელების დასანერგად. ახალმა სტანდარტმა უნდა დააკმაყოფილოს ამჟამინდელი და მომავალი მომხმარებლების მოთხოვნები. მომხმარებლებსა და კლიენტებს ესაჭიროებათ მომსახურების უკეთესი ხარისხი და უსაფრთხოების მაღალი დონე, რათა უსაფრთხოდ გადაეცემოდეს მონაცემები და უხარვეზოდ მუშაობდეს სხვა შიდა სერვისები. შესაბამისად, წამყვანმა მობილურმა ოპერატორებმა უნდა უზრუნველყონ ბევრად უკეთესი სამომხმარებლო ხარისხი და უსაფრთხოება, ასევე უნდა გაუმჯობესდეს მათ მიერ შემოთავაზებული სერვისები. 5G-ს შემოთავაზებულ ახალ მეთოდიკას სჭირდება ქსელური, სერვისის დანერგვისა და მონაცემთა დამუშავების ახალი მიდგომები. აღნიშნულ მიდგომებს ახასიათებთ უსაფრთხოების გარკვეული ნაკლოვანებები, რაც ასევე კრიტიკული იქნება 5G ქსელებისთვის. ამ კუთხით მომუშავე მსოფლიოს წამყვანმა მკვლევარებმა უკვე საჯაროდ განაცხადეს 5G ქსელების ამჟამინდელ პრობლემებზე. ჩვენ მიერ წარმოდგენილი ანაზილი ცხადყოფს 5G-ს არსებული პრობლემების დეტალურ მიზეზებს, რაც შემტევს აძლევს საშუალებას სისტემაში ჩააშენოს მავნე კოდი და წარმატებით განახორციელოს შემდეგი შეტევები: MiTM, MNmap და Battery drain.

ჩვენ შევიმუშავეთ ახალი სისტემა შეტევების ამოსაცნობად, რომელიც დაფუძნებულია მანქანური და ღრმა დასწავლის უახლეს მეთოდებზე. ჩვენ ვთავაზობთ IDS-ის ინტეგრაციას 5G-ს არქიტექტურაში.

ABSTRACT

The telecommunications industry is evolving significantly to implement 5G networks. The new standard must meet the requirements of current and future users. Customers and clients need better quality of service and a high level of security in order for data to be transmitted securely and other internal services to work flawlessly. Consequently, leading mobile operators need to ensure much better customer quality and security, as well as improve the services they offer. The new methodology proposed by 5G requires new approaches to networking, service deployment, and data processing. These approaches are characterized by certain security vulnerabilities that will also be critical for 5G networks. The world's leading researchers working in this field have already publicly stated the current problems of 5G networks. Analysis presented by us reveals the detailed causes of 5G problems, which allows the attacker to install malicious code in the system and successfully carry out the following attacks: MiTM, MNmap and Battery drain.

We have developed a new system for detecting attacks based on the latest methods of machine and in-depth learning. We propose the integration of IDS into the 5G architecture.

საკვანძო სიტყვები: *5G ქსელი, 5G უსაფრთხოება, ფიჭური ქსელები*

KEYWORDS: *5G network, 5G security, cellular networks*

1. შესავალი

უსადენო ქსელებით გადაცემული ტრაფიკის რაოდენობა და მობილური მოწყობილობების რაოდენობა (IoT-ის ჩათვლით) არის ძალიან სწრაფად მზარდი, რაც გამოწვეულია რამდენიმე ფაქტორით. სატელეკომუნიკაციო ინდუსტრია განიცდის ძირითად ტრანსფორმაციას 5G ქსელების დასანერგად და მომხარებელთა არსებული და სამომავლო მოთხონილებების დასაკმაყოფილებლად. შესაბამისად, უსადენო 5G ქსელი მოიაზრება მონაცემთა გადაცემის ძალიან მაღალი სისწრაფის მქონედ და უკეთესი ხარისხის მქონედ, რაც გამყარებულია სიგნალის მიმღები სადგურების მჭიდრო განლაგების კონცეფციით, მომსახურების გაუმჯობესებული ხარისხით (QoS) და უკიდურესად მცირე შეყოვნებით. ყოველივე ზემოთქმულის განსახორციელებლად საჭიროა უახლესი ტექნოლოგიების დანერგვა და გამოყენება ქსელების, სერვისების, მარაგებისა და მონაცემთა დამუშავების მხრივ. ეს ტექნოლოგიები წარმოშობს ახალ გამოწვევებს 5G კიბერ უსაფრთხოების სისტემების ფუნქციონალობაში.

5G დააკავშირებს კრიტიკულ ინფრასტრუქტურებს, რისთვისაც საჭიროა მეტი დაცულობა არა მხოლოდ ინფრასტრუქტურის შიგნით, არამედ მთელ საზოგადოებაში. მაგალითად, უსაფრთხოების ხარვეზი ელექტროენერგიის კვების სისტემებში იქნება საზიანო გლობალურად და არა მხოლოდ რაიმე კერძო სექტორისათვის. შესაბამისად, აუცილებელია, რომ გამოვიკვლიოთ და აღმოვაჩინოთ მნიშვნელოვანი პრობლემები 5G ქსელებში და მოვიძიოთ უკვე არსებული გადაწყვეტილებები, რომლებიც აუმჯობესებს უსაფრთხოების ხარისხს. მკველვარები და დეველოპერები თავდაუზოგავად მუშაობენ ამ საკითხების

გამოსაკვლევად და იმისათვის, რომ 5G გახადონ უფრო დაცული. ქვემოთ მოვიყვანთ უკვე ცნობილ ხარვეზებს, რომლიც აქვს 5G-ს.

2. 5G-ს უსაფრთხოების პრობლემები

მკვლევარებმა აჩვენეს, რომ 5G-ს ჯერ კიდევ აქვს უსაფრთხოების პრობლემები[1-4]. ჩვენ გავაანალიზეთ და გამოვავლინეთ რიგი მიზეზებისა:

- 5G ქსელი არის დაუცველი პროგრამული უზრუნველყოფით განხორციელებული შეტევების მიმართ, აქვს ბევრი სუსტი ადგილი, რომლებსაც იყენებენ ჰაკერები. ამის მიზეზია ის, რომ მთლიანად სისტემა დიდწილად დაფუძნებულია პროგრამულ უზრუნველყოფაზე.
- იქიდან გამომდინარე, რომ 5G-ს ქსელურმა არქიტექტურამ მიიღო უფრო დიდი ფუნქცია, ქსელის სტრუქტურის გარკვეული ნაწილები იქნება გაცილებით მგრძნობიარე შეტევების მიმართ. საბაზო სადგურები და ქსელის გასაღების განაწილების ფუნქციები შეიძლება გახდეს ჰაკერების სამიზნე.
- ის ფაქტი, რომ მობილური ქსელების ოპერატორები დამოკიდებულები არიან მომმარაგებლებზე, შეიძლება გახდეს საფრთხის შემცველი, გაზარდოს შეტევისაგან მიყენებული ზიანი.
- ბევრი კრიტიკული IT აპლიკაცია გამოიყენებს 5G ქსელს, ამიტომ აპლიკაციის ხელმისაწვდომობა და მთლიანობა უსაფრთხოებისათვის საყურადღებო საკითხი იქნება.
- 5G ქსელში ჩართული ბევრი მოწყობილობის გამო, შეიძლება მნიშვნელოვნად გაიზარდოს DoS და DDoS ტიპის შეტევები.
- ქსელის შრეებად დაყოფა (Network Slicing) ასევე საყურადღებო საკითხია უსაფრთხოების მხრივ, რადგან შეიძლება შემტევმა იძულებით გამოაყენებინოს გარკვეულ მოწყობილობას შრე,სადაც მას არ აქვს დაშვების უფლება.

ბოლო წლებში, 5G-ს მკვლევარებმა აღმოაჩინეს სისუსტეები, რომელთა გამოყენებითაც შეიძლება მავნე კოდის ჩაყენება სისტემაში და მისი გამოყენება მომხმარებელთათვის საზიანო მიზნებისათვის. მაგალითად:

1. **MNmap**
   მკვლევართა გუნდა სნიფერით მოიპოვა ინფორმაცია, რომელიც ქსელში გაშვებული იყო დაუშიფრავად, ღია ტექსტის სახით. ამის მეშვეობით, მათ აღადგინეს მოწყობილობათა „რუკა“, რომლებიც მიერთებული იყო ამ ქსელთან. მეცნიერებმა შეძლეს დაედგინათ მოწყობილობის მწარმოებელი, მოდელი, ოპერაციული სისტემა და სხვა კერძო მახასიათებლები.

2. **MiTM**
   ახლანდელ 5G-ზე შეიძლება ასევე MiTM შეტევის განხორციელება. MiTM-ის გამოყენებით შეიძლება ასევე განხორციელდეს bidding-down დაbattery drain შეტევები. შემტევს შეუძლია მიმღები სადგურიდან ამოიღოს MIMO. ეს არის ნაწილი, რომელიც

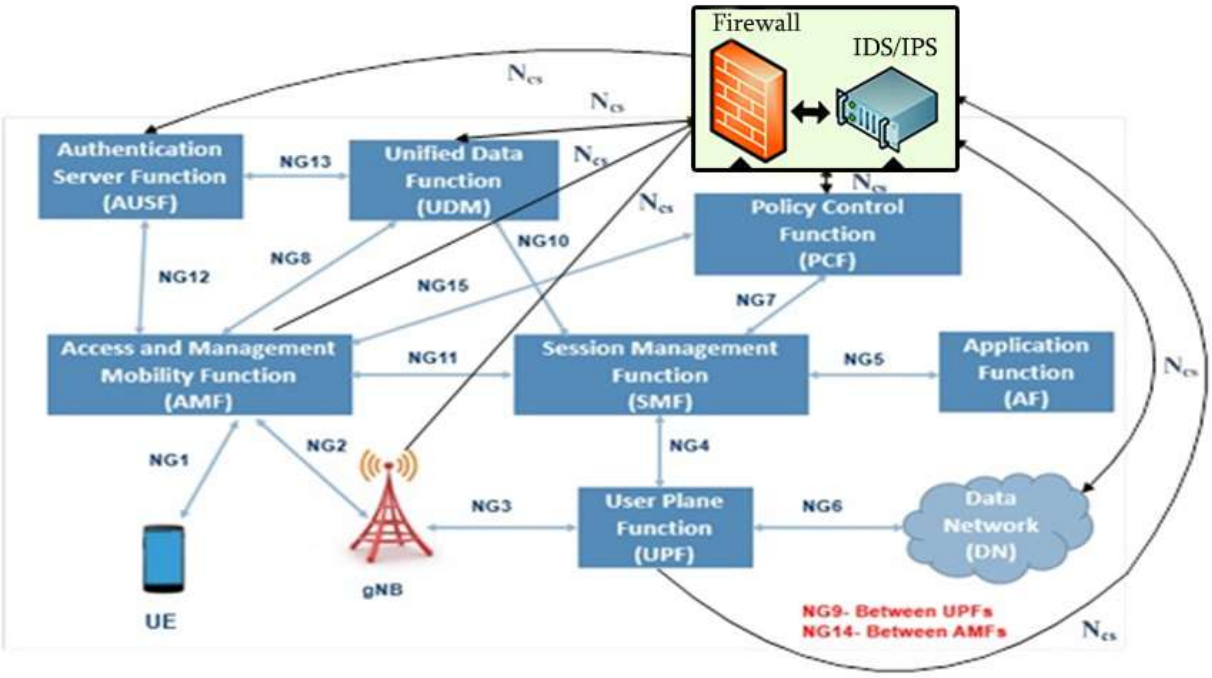
პასუხისმგებელია 5G-ს ძალიან მაღალ სიჩქარეზე. MIMO-ს გარეშე შეიძლება იგივე შეტევების განხორციელება, რაც ჩვეულებრივ ხდება 2G/3G ქსელებზე.

3. **Battery drain attack**
   ბატარეის გამოფიტვის შეტევა მიმართულია NB-IoT მოწყობილობებზე. ეს მოწყობილობები დროგამოშვებით აგზავნიან სიგნალებს და მოკლე ხანში შეიძლება დახარჯონ იმ რაოდენობის ენერგია, რაც ბატარეას ეყოფოდა 10 წელი PSM მდგომარეობაში. ჰაკერს შეუძლია ისე დაარეგულიროს PSM, რომ მსხვერპლი მიუერთდეს ჰაკერისათვის სასურველ ქსელს და გამოიყენოს მისი მოწყობილობა საზიანოდ.

ყოველივე ზემოთქმულის გათვალისწინებით, აუცილებელია ახალი არქიტექტურის შექმნა 5G და მომავალი 6G ქსელებისათვის, რათა ინტეგრირდეს უახლეს AI/ML კონცეფციებზე დაფუძნებული ალგორითმები, რაც ,თავის მხრივ, უზრუნველყოფს უსაფრთხოების უმაღლეს დონეს ყველა მისი მომხმარებლისათვის.

3. მეთოდოლოგია

ჩვენ ვთავაზობთ, რომ 5G-ს თითოეულ სადგურზე ჩაყენდეს კიბერ უსაფრთხოების ფუნქცია, როგორც დამატებითი სერვერი. ამ სერვერს ექნება Firewall და IDS/IPS. იდეა გრაფიკულად გამოსახულია ნახ.2-ზე.



ნახ. 2. კიბერ უსაფრთხოების ფუნქცია

ჩვენი კვლევიდან ჩანს, რომ 5G ქსელისათვის საფრთხის შემცველია Probe, DoS და პროგრამულ უზრუნველყოფასთან დაკავშირებული შეტევები. IDS-ის თავდაპირველი ვერსია დაფუძნებულია მანქანური სწავლების ალგორითმებზე. იმისათვის რომ IDS გაუმკლავდეს აღნიშნულ შეტევებს ის გავავარჯიშეთ შეტევების სხვადასხვა მონაცემების მიხედვით.

პირველი ბაზაა KDD99 [5-7]. ხაზგასასმელია ის ფაქტი, რომ აკადემიურ წრეებში IDS-ის პროტოტიპების შექმნისას მიღებულია KDD99-ის გამოყენება.

KDD99 არის ყველაზე ცნობილი მონაცემთა ნაკრები ანომალიების დასადგენად. ეს ბაზა შექმნილია DARPA'98 IDS პროგრამის ფარგლებში. ზემოხსენებული არის დაახლოებით 4 გიგაბაიტის ზომის პირველადი მონაცემები, რომელიც მიღებულია 7 კვირის განმავლობაში TCPDump-დან. 2 კვირის შესაბამისი მონაცემები შეიცავს დაახლოებით 2 მილიონ ჩანაწერს. მთლიანი ფაილი მოიცავს დაახლოებით 5 მილიონ ნიმუშს, რომლიც დაყოფილია როგორც შეტევა ან როგორც უსაფრთხო ტრაფიკი. ყველა შეტევა იყოფა 4 ძირითად ჯგუფად:

1) Denial of Service Attack (DoS): შეტევა, როდესაც იგზავნება ძალიან ბევრი მოთხოვნა, გადაივსება კომპიუტერის რესურსები და აღარ შეუძლია დააკმაყოფილოს მომხმარებლის მოთხოვნები.
2) User to Root Attack (U2R): შეტევის კლასი, როდესაც შემტევს ხელი მიუწვდება მომხმარებლის ლეგიტიმურ ანგარიშზე და შეუძლია ამ გზით შეაღწიოს შიდა სისტემაში,რის შედეგადაც მიიღებს სრულ წვდომას და გამოიყენებს შიგნით არსებულ სისუსტეებს.
3) Remote to Local Attack (R2L): შეტევის კლასი, როდესაც შემტევს არ აქვს ანგარიში კომპიუტერში, მაგრამ დისტანციურად შეუძლია გააგზავნოს პაკეტები და მიიღოს სრული წვდომა როგორც მომხმარებლი ლოკალურ კომპიუტერზე.
4) Probing Attack: შეტევა მიმართულია ქსელის შესახებ ინფორმაციის შეგროვებისაკენ, რათა გვერდი აუაროს უსაფრთხოების მექანიზმებს.

KDD-ს მთლიანი მონაცემები გაყოფილია გასავარჯიშებელ და გასატესტ შეტევის ტიპებად, შესაბამისად 24 და 14 მახასიათებელით.ეს მახასიათებლები შეიძლება გავყოთ 3 ჯგუფად:

1) ძირითადი მახასიათებლები: ყველა ინფორმაცია, რომელიც შეიძლება მივიღოთ TCP/IP კავშირის ანალიზის შედეგად. მათი აღმოჩენისას შეიძლება იყო პატარა შეყოვნება.
2) ტრაფიკის მახასიათებლები იყოფა 2 ჯგუფად:

2.1) "Same host" მახასიათებლები: მოწმდება ბოლო 2 წამში მომხდარი კავშირები, რომელთაც აქვთ იგივე მიმართულება (destination) რაც აქვს კონკრეტულ კავშირს. დამატებით ეს მახასიათებლები ითვლის სერვისის, პროტოკოლისა და სხვა სტატისტიკებს.

2.2) “Same service” მახასიათებლები: მოწმდება ბოლო 2 წამში მომხდარი კავშირები, რომლთაც აქვთ იგივე სერვისები რაც კონკრეტულ კავშირს. არსებობს შეტევების გარკვეული ტიპები, სადაც არ იყენებენ ინტერვალად 2 წამს და იყენებენ მაგალითად 1 წუთს. ამგვარი პრობლემის გადასაჭრელად, “same host” და“same service” მახასიათებლები მოწმდება ყოველ 100 კავშირზე.

3) კონტენტის მახასიათებლები: DoS და Probe შეტევები მოითხოვს მრავალ კავშირს მოკლე დროის განმავლობაში ერთსა და იმავე ჰოსტთან. თუმცა, R2L და U2R ტიპის შეტევები ამას არ საჭიროებენ. R2L და U2R შეტევები იგზავნება მონაცემთა პაკეტებთან ერთად და საჭიროებს მხოლოდ ერთ დაკავშირებას. ამ ტიპის შეტევების აღმოსაჩენად, ჩვენ უნდა გამოვიკვლიოთ საეჭვო ქმედებებები მონაცემთა კონკრეტულ პაკეტებში. მაგალითად: არასწორი პაროლის შეყვანის მცდელობათა რაოდენობა.

როგორც ვხედავთ, KDD99-ის მონაცემები იყოფა 4 ძირითად კატეგორიად: DOS, R2L, U2R და PROBE. DOS კატეგორია შეიცავს შემდეგ ქვეკატეგორიებს: APACHE2, PROCESSTABLE, UDPSTORM, BACK, LAND, NEPTUNE, POD, SMUR, MAILBOMB და TEARDROP. U2R კატეგორია შეიცავს შემდეგ ქვეკატეგორიებს: BUFFER_OVERFLOW, PS, SQLATTACK, XTERM, PERL, LOADMODULE, და ROOTKIT. R2L კატეგორია შეიცავს შემდეგ ქვეკატეგორიებს: FTP_WRITE, GUESS_PASSWD, HTTPTUNNEL IMAP, MULTIHOP, NAMED, SENDMAIL, SNMPGETATTACK, SNMGUESS, WXLOCK, XSNOOP, PHF, SPY, WAREZCLIENT და WAREZMASTER. ბოლო კატეგორია, PROBE, კი შეიცავს შემდეგ ქვეკატეგორიებს: IPSWEEP, NMAP, PORTSWEEP, NMA, MSCAN, SAINT და SATAN. R2L და U2R შეტევები მიმართულია პროგრამული უზრუნველყოფის სისუსტეებისადმი. შესაბამისად, IDS-ის დატრენინგება KDD-ს მონაცემებით 5G-სათვის არის ძალიან ხელსაყრელი, რადგან აღნიშნული შეტევები ფარავს 5G-სათვის კრიტიკული შეტევების აბსოლუტურ უმრავლესობას.

ასევე, ჩვენ დამატებით დავატრენინგეთ ჩვენი IDS DOS-ის შეტევების ორ ბაზაზე. პირველი შეიცავს ინფორაციას შემდეგ შეტევებზე: 'LDAP', 'MSSQL', 'NetBIOS', 'Syn', 'UDP', 'UDPLag' და მისი ზომაა 380 MB. მას აღვნიშნავთ DOS1-ით. მეორე კი შეიცავს მხოლოდ „Portmap“ შეტევას და არის 85 MB, მას აღვნიშნავთ როგორც DOS2. აღსანიშნავია, რომ მონაცემები არის საკმაოდ დიდი მოცულობის.

ჩვენ გავყავით KDD99-ის მონაცემები სატესტო და გასავარჯიშებელ ნაწილებად. სატესტო ნაწილი არის მთლიანი ბაზის 10%, გასავარჯიშებელი კი - 90%. იგივე პროცედურა ჩავატარეთ DOS1 და DOS2 ფაილებზე, გავყავით 20%-80% შესაბამისი თანაფარდობით. ასეთი განაწილება გვაძლევს შეტევის ამოსაცნობი სიზუსტის ძალიან მაღალ მაჩვენებელს. KDD99-ის შემთხვევაში არის 0.9611049372916336, DOS1-ის შემთხვევაში არის 0.9937894736842106, ხოლო DOS2-ის შემთხვევაში კი - 0.9998956703182055.

გავარჯიშების შემდეგ, მოდელი ელოდება მონაცემებს ქსელის სნიფერისგან. თავდაპირველად, მონაცემები მოწმდება შედის თუ არა KDD99-ში. თუ შეტევა იდენტიფიცირდება, გადაეცემა IPS-ს (შეღწევისგან დასაცავ სისტემას). თუ შეტევა არაა იდენტიფიცირებული, შემდეგ ავტომატურად გადაეცემა DOS1-ის მონაცემებში შესამოწმებლად, ინდენტიფიცირების შემთხვევაში გდაეცემა IPS-ს. წინააღმდეგ შემთხვევაში,

ავტომატურად მოწმდება DOS2-ის მონაცემებში და იდენტიფიცირებისას გადაეცემა IPS-ს. თუ IDS მაინც ვერ დაადგენს შეტევას, აღნიშნული ტრაფიკი ჩაითვლება უსაფრთხოდ და გააგრძელებს შემდეგი მონაცემების დამუშავებას ზემოაღნიშნული ეტაპებით.

4. დასკვნა

ზემოთ აღწერილი 5G-ს კიბერ უსაფრთხოების ფუნქცია, გავარჯიშებულია შეტევების აბსოლუტურ უმრავლესობაზე, რომელსაც შეუძლია გატეხოს ახლანდელი 5G სისტემა. ჩვენი მიდგომა არსებითად განსხვავებულია ამ მიმართულებაში უკვე არსებული მიდგომებისგან. სხვა სტატიებში IDS-ს ძირითადად ავარჯიშებენ მხოლოდ KDD99-ის მონაცემებით, თუმცა ჩვენს მოდელში KDD99 გამოყენებულია ერთ-ერთ მონაცემთა ბაზად, გარდა ამისა ვიყენებთ სხვა ტიპის შეტევების შემცველ მონაცემთა ბაზებსაც. ჩვენი ჩატარებული ექსპერიმენტებიდან ჩანს, რომ აღნიშნულ მოდელს შეუძლია ამოიცნოს განხორციელებული შეტევების აბსოლუტური უმრავლესობა.

ამ დროისათვის მიღებული ექსპერიმენტალური შედეგები არის საწყისი და ჩვენ ვმუშაობთ სატესტო ლაბორატორიის განვითარებაზე, რათა შევქმნათ მაქსიმალურად ზუსტი და კომპლექსური შეტევის ვექტორები. ამის შემდეგ, ჩვენი მიზანი იქნება შეტევების საკუთარი მონაცემების დაგენერირება ჩვენს სატესტო ლაბორატორიაში და IDS-ის გავარჯიშება ახალი მონაცემებით. ხოლო შემდეგ კი, დავიწყებთ IDS-ის ტესტირებას რეალური 5G გარემოში.

5. Acknowledgment

აღნიშნული კვლევა დაფინანსებულია შოთა რუსთაველის ეროვნული სამეცნიერო ფონდის

მიერ და განხორციელდა PHDF-19-519 გრანტის ფარგლებში.

ბიბლიოგრაფია

1. The analysis of the difference of 4G and 5G securities; M. Iavich, G. Iashvili, A. Gagnidze, L. Nachkebia, S. Khukhashvili; Scientific and practical cyber security journal, (SPCSJ) 4(3); 2020.
2. Y. Sun, Z. Tian, M. Li, C. Zhu and N. Guizani, "Automated Attack and Defense Framework toward 5G Security," in *IEEE Network*, vol. 34, no. 5, pp. 247-253, September/October 2020, doi: 10.1109/MNET.011.1900635.
3. Park S., Cho H., Park Y., Choi B., Kim D., Yim K. (2020) Security Problems of 5G Voice Communication. In: You I. (eds) Information Security Applications. WISA 2020. Lecture Notes in Computer Science, vol 12583. Springer, Cham. https://doi.org/10.1007/978-3-030-65299-9_30
4. LIU Jianwei, HAN Yiran, LIU Bin, YU Beiyuan. Research on 5G Network Slicing Security Model[J]. Netinfo Security, 2020, 20(4): 1-11.

5. Ullah I., Mahmoud Q.H. (2020) A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In: Goutte C., Zhu X. (eds) Advances in Artificial Intelligence. Canadian AI 2020. Lecture Notes in Computer Science, vol 12109. Springer, Cham. https://doi.org/10.1007/978-3-030-47358-7_52
6. Ullah I., Mahmoud Q.H. (2020) A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In: Goutte C., Zhu X. (eds) Advances in Artificial Intelligence. Canadian AI 2020. Lecture Notes in Computer Science, vol 12109. Springer, Cham. https://doi.org/10.1007/978-3-030-47358-7_52
7. Kumar, V., Sinha, D., Das, A.K. *et al.* An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset. *Cluster Comput* **23,** 1397–1418 (2020). https://doi.org/10.1007/s10586-019-03008-x

Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 9-15 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

A PROPOSED NOVEL LOW COST GENETIC-FUZZY BLOCKCHAIN-ENABLED INTERNET OF THINGS (IoT) FORENSICS FRAMEWORK

Faisal A. Garba, Department of Computer Science Education, Sa'adatu Rimi College of Education, Kano
Kabiru I. Kunya, Department of Computer Science Education, Sa'adatu Rimi College of Education, Kano
Zahrau Ahmad Zakari, Kunya, Department of Computer Science Education, Sa'adatu Rimi College of Education, Kano
Shazali A. Ibrahim, Kunya, Department of Computer Science Education, Sa'adatu Rimi College of Education, Kano
Abubakar Abba, Department of Computer Science, Federal College of Education, Zaria
Jameel Shehu Yalli, Federal University Gusau
Zaharaddeen Karami Lawal, Department of Computer Science, Federal University Dutse
Aliyu Lawan Musa. Department of Computer Engineering Technology, School of Technology, Kano State Polytechnic

ABSTRACT

Practitioners of network forensics often employ automated software and hardware tools for the collection and preservation of data, however, the process of performing a forensic examination is not well defined. This has resulted in the emergence of various digital forensic frameworks, which determine the correct course of action during an investigation, separating the process into autonomous stages and suggesting appropriate tools and techniques for each task. Even though many forensic frameworks have been proposed, existing solutions give emphasis on acquisition and neglect examination and analysis. Privacy is also a key element in maintaining the confidentiality of data in forensics as it may lead to exposure of personal identifiable information. Furthermore, accountability is one of the IoT forensics challenges. The widespread adoption of an estimated 30.9 billion IoT devices by 2025 (Statista, 2021), as well as the increasing interconnectivity of those devices to traditional networks, not to mention to one another with the advent of fifth generation (5G) networks, underscore the need for IoT forensics. This work proposed a novel low cost IoT forensic framework to tackle: (a.) the examination and analysis phase of IoT forensics using genetic-fuzzy expert system (b.) the issue of guarding the privacy and chain of custody of IoT forensics data using hyperledger fabric, private-permissioned blockchain that is both free and open source. The framework will be implemented and evaluated with related works using BoT-IoT dataset. The BoT-IoT dataset includes Distributed Denial of Service (DDoS), Denial of Service (DoS), Operating System (OS) and Service Scan, Keylogging and Data exfiltration attacks, with the DDoS and DoS attacks further organized, based on the protocol used. The genetic-fuzzy IoT forensics framework will be compared against related work and Network Forensics Analysis Tool (NFAT) to evaluate the performance and accuracy of the proposed framework. The private permissioned blockchain IoT forensics framework will be compared against a related work to evaluate the security and cost of the proposed private permissioned blockchain framework. The genetic-fuzzy blockchain-enabled IoT forensic framework will be compared with, related works and NFATs to evaluate the speed and accuracy performance of the proposed framework. The result of this study is a low cost genetic-fuzzy blockchain-enabled IoT forensics framework.

KEYWORDS*: IoT, forensics, blockchain, genetic-fuzzy*

INTRODUCTION

Internet of Things (IoT) will soon be present in all areas of our life. While it is true that this development makes the lives of humans easier, said development also gives rise to numerous

issues related to digital forensics and security (Atlam *et al.,* 2020). Computer or digital forensics is the practice of investigating computers, digital media, and digital communications for potential artifacts. In this context, the word artifact indicates any object of interest (Messier, 2017). Network forensics is one of the sub-branches of digital forensics where the data being analyzed is the network traffic going to and fro the system under observation. The purposes of this type of observation are collecting information, obtaining legal evidence, establishing a root-cause analysis of an event, analyzing malware behavior, and so on (Jaswal, 2019). Unlike other areas of digital forensics, network forensic investigations deal with volatile and dynamic information (Datt, 2016). IoT forensics comprises three digital forensics schemes in total: network forensics, device-level forensics, and cloud forensics (Atlam *et al*., 2020; Zawoad and Hasan, 2015). As the majority of the IoT devices are characterized by low storage and computational capability, any data which is produced by the IoT network and IoT device is kept and sorted in the cloud. IoT infrastructures are made up of different kinds of networks, such as Wide Area Networks (WAN), Body Area Network (BAN), Home/Hospital Area Networks (HAN), Personal Area Network (PAN), and Local Area Networks (LAN). Crucial pieces of evidence can be gathered from any one of the above-mentioned networks. If a vital piece of evidence must be gathered from the IoT devices, device-level forensics comes into play. The device level forensics scheme is employed when there is the need to collect, from the IoT devices, a vital piece of evidence (Zawoad and Hasan, 2015). IoT forensics remains in the process of maturing, particularly since there are numerous challenges in existence and fewer studies in the field. Accountability is a major requirement in IoT forensics (Lutta *et al.,* 2020; Singh *et al.,* 2018). IoT forensics framework at network level has been proposed to handle the accountability issues with the use of public-permissionless blockchain. Public-permissionless blockchain however, comes at a cost which is usually paid in the form of cryptocurrency (for instance Bitcoin or Ether depending on the platform used) to the miners as an incentive for validating a transaction. Aside from being not free (since gas fee is paid for transaction validation), with public-permissionless blockchain there is no control and restriction to who should join the blockchain. Anyone can join the blockchain platform. This research work therefore proposed a private permission blockchain framework which preserves provenance of IoT forensic data.

Even though many forensic frameworks have been proposed existing solutions neglect examination and analysis and instead give more emphasis on acquisition (Koroniotis and Moustafa, 2020). In the examination phase, evidence collected is searched methodically to extract specific indicators of the crime. These indicators of crime are then classified and correlated to deduce important observations using the existing attack patterns during the analysis phase. Statistical, soft computing and data mining approaches are used to search the data and match attack patterns. The attack patterns are put together, reconstructed and replayed to understand the intention and methodology of the attacker (Pilli *et al*., 2010). Soft computing is viewed as a foundation component for the emerging field of computational intelligence (Cabrera *et al*., 2009). According to Mankad (2013) soft computing is a good option for complex systems where: the required information is not available; the behavior is not completely known; and the existence of measure of variables is noisy. Soft computing is a consortium of computing methodologies that provides a foundation for the conception, design, and deployment of intelligent systems to provide economical and feasible solutions with reduced complexity (Mankad, 2013). Members of this consortium include: Fuzzy Logic (FL), Neural Network (NN), Evolutionary Computations (EC) and Probabilistic Reasoning (PR). Each of these techniques has their own strengths and limitations. Integration of two or more techniques can provide significant advantages for intelligent system design. The hybridization of major constituents of Soft Computing can be represented as EC-FL, EC-NN, PR-FL and PR-NN. Fuzzy logic is used to process human-like classification of things into groups with the representation of fuzzy linguistic variable. Hybridization of genetic algorithm with other soft computing components, results in natural evolution of a solution. It has been observed that genetic algorithm provides the following major advantages: genetic algorithm can be easily interfaced to obtainable simulations and models; genetic algorithm is easy to

hybridize and easy to understand; genetic algorithm uses little problem specific code; genetic algorithm is modular, separate from application; genetic algorithm is capable to obtain answers always and gets better with time; and genetic algorithm is inherently parallel and easily distributed (Williams, 2020). The major limitations of fuzzy systems are: inability of self-learning, adaption or parallel computation; cannot support optimization; answers obtained once cannot get better with time. In order to solve the stated problems, the use of genetic algorithm to find optimized values for the membership function parameters, particularly when manual selection of their values becomes difficult or takes too much time to attain has been proposed (Mankad, 2013). Liao *et al.,* (2009) and Kim *et al.,* (2004) have both proposed a fuzzy expert system network forensics investigation. Liao *et al.,* (2009) evaluated the fuzzy expert network forensic system performance with DARPA 2000 dataset and compared the proposed fuzzy expert network forensic system with other proposed studies that utilizes Support Vector Machine (SVM), Naïve Bayes Algorithm (NB), C4.5 and SMO algorithm (another training algorithm for SVM) to which the proposed fuzzy expert network forensic system outperform them all in attack detection accuracy. Kim *et al.,* (2004) on the other hand uses DARPA 1998 dataset and the proposed fuzzy expert network forensic system has a detection accuracy of 92% but no performance comparison with other related study was done. Mankad (2013) successfully applied genetic-fuzzy to measure multiple intelligence. In this work we seek to employ a similar approach to use genetic algorithm to improve fuzzy expert system performance in examination and analysis of IoT network traffic data. We intend to use Bot-IoT dataset (Koroniotis *et al*., 2019) to evaluate the performance of the proposed Genetic- Fuzzy IoT Network Forensic Framework.

STATEMENT OF THE PROBLEM

Privacy is a key element in maintaining the confidentiality of forensics data as it may lead to exposure of personal identifiable information (Lutta *et al.,* 2020). Singh *et al.,* (2018) mentioned accountability as one of the IoT forensics challenges. Singh *et al.,* (2018) stress that this is because different entities manage the composition and the interactions between the IoT components. The distributed and immutable characteristics of blockchains suit the demands of IoT Forensics. An ideal solution for IoT Forensics is a private-permissioned blockchain where the number of nodes is restricted and access is only provided to selected users as suggested by Sadineni *et al*., (2019). Even though many forensic frameworks have been proposed existing solutions give emphasis on acquisition and neglect examination and analysis (Koroniotis and Moustafa, 2020) In the examination phase, evidence collected is searched methodically to extract specific indicators of the crime. These indicators of crime are then classified and correlated to deduce important observations using the existing attack patterns during the analysis phase. Statistical, soft computing and data mining approaches are used to search the data and match attack patterns. The attack patterns are put together, reconstructed and replayed to understand the intention and methodology of the attacker (Pilli *et al*., 2010). Soft computing is viewed as a foundation component for the emerging field of computational intelligence (Cabrera *et al*., 2009). According to Mankad (2013) soft computing is a good option for complex systems where: the required information is not available; the behavior is not completely known; and the existence of measure of variable is noisy. Soft computing is a consortium of computing methodologies that provides a foundation for the conception, design, and deployment of intelligent systems to provide economical and feasible solutions with reduced complexity (Mankad, 2013). Members of this consortium include: Fuzzy Logic (FL), Neural Network (NN), Evolutionary Computations (EC) and Probabilistic Reasoning (PR). Each of these techniques has their own strengths and limitations. Integration of two or more techniques can provide significant advantages for intelligent system design. The hybridization of major constituents of Soft Computing can be represented as EC-FL, EC-NN, PR-FL and PR-NN. Fuzzy logic is used to process human like classification of things into group with the representation of fuzzy linguistic variable. Hybridization of genetic algorithm with other soft computing components, results in natural

evolution of a solution. It has been observed that genetic algorithm provides the following major advantages: genetic algorithm can be easily interfaced to obtainable simulations and models; genetic algorithm is easy to hybridize and easy to understand; genetic algorithm uses little problem specific code; genetic algorithm is modular, separate from application; genetic algorithm is capable to obtain answers always and gets better with time; and genetic algorithm is inherently parallel and easily distributed (Williams, 2020). The major limitations of fuzzy systems are: inability of self-learning, adaption or parallel computation; cannot support optimization; answer obtained once cannot get better with time. In order to solve the stated problems, the use of genetic algorithm to find optimized values for the membership function parameters, particularly when manual selection of their values becomes difficult or takes too much time to attain has been proposed (Mankad, 2013).

AIM AND OBJECTIVES

The aim of this research is to develop a novel low cost fuzzy-genetic blockchain enabled network forensics framework to address the preservation of digital provenance, examination and analysis challenges of IoT forensics.

The specific objectives of this work are to:

a. design a blockchain fuzzy-genetic IoT forensics framework
b. implement a blockchain fuzzy-genetic IoT forensics framework
c. evaluate the blockchain fuzzy-genetic IoT forensics framework with related works.

SIGNIFICANCE OF THE STUDY

It has been proven that IoT devices are vulnerable to both well established and new IoT-specific attack vectors. In a 2018 report by Symantec regarding the security threats found in the Internet, it was reported that the total number of attacks targeting IoT devices for 2018 exceeded 57,000, with more than 5,000 attacks being recorded each month. Hackers have compromised vulnerable, unpatched or unencrypted IoT devices in order to steal sensitive data, corrupt the device's normal operation, spread malware infections or even compromise the security of a smart home by disabling smart locks and garage doors (Koroniotis and Moustafa, 2020). The widespread adoption of an estimated 30.9 billion IoT devices by 2025 (Statista, 2021), as well as the increasing interconnectivity of those devices to traditional networks, not to mention to one another with the advent of fifth generation (5G) networks, underscore the need for IoT forensics (Zhang *et al*., 2020).

REVIEW OF PROPOSED IoT NETWORK FORENSICS FRAMEWORKS

Mercan *et al*., (2020) proposed "A Cost-efficient IoT Forensics Framework with Blockchain". The study claimed to be cost effective and reliable digital forensics framework that achieves this by exploiting multiple inexpensive blockchain networks as a temporary storage before the data is committed to Ethereum. To reduce Ethereum costs, they utilize Merkle trees which hierarchically store hashes of the collected event data from IoT devices. They evaluated the approach on popular blockchains such as EOS, Stellar and Ethereum by conducting a cost analysis. The results indicates cost savings resulting from using the proposed 'Cost-efficient IoT Forensics Framework with Blockchain'. The proposed work of Mercan *et al*., (2020) has some limitations. First, the use of public-permissionless blockchain platform in this case Etherium to preserve forensic evidence is not recommended. This is because in a public blockchain everyone can join the network and have access to all the blocks in the network. An ideal solution for IoT Forensics is a private-permissioned blockchain where the number of nodes is restricted and access is only provided to selected users (Sadineni *et al*., 2019). Secondly, the use of Ethereum blockchain comes at a cost in the form of 'gas fees' that is paid to the miners as an incentive for validating a block. There are alternative private-permissioned

blockchain platforms that are open source and free to use. One such instance is the Hyperledger Fabric which this research work intends to use to preserve forensic evidence.

Li *et al.,* (2019) proposed "Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems". A blockchain-based digital forensic investigation framework in the Internet of Things (IoT) and social systems environment is proposed, which can provide proof of existence and privacy preservation for evidence items examination. The work has some limitations. The use of blockchain would of course guards the provenance of the forensic digital evidence, however the proposal did not go into detail to specify which type of blockchain it intends to use to implement the proposal –whether private-permission blockchain or public-permissionless blockchain. Secondly, the proposal is just a theoretical presentation, there was no implementation and evaluation to show how it advanced the state of the art.

Brotsis *et al*., (2019) proposed "Blockchain Solutions for Forensic Evidence Preservation in IoT Environments". This study presented a blockchain-based solution, which is designed for the smart home domain, dealing with the collection and preservation of digital forensic evidence. The system utilizes a private forensic evidence database, where the captured evidence is stored, along with a permissioned blockchain that allows providing security services like integrity, authentication, and non-repudiation, so that the evidence can be used in a court of law. The blockchain stores evidences' metadata, which are critical for providing the aforementioned services, and interacts via smart contracts with the different entities involved in an investigation process, including Internet service providers, law enforcement agencies and prosecutors. The proposed work of Brotsis *et al*., (2019) however has not been implemented and there was no evaluation to show how it has advanced the state of the art.

Hossain *et al.,* (2018) propose FIF-IoT – a forensic investigation framework using a public digital ledger to find facts in criminal incidents in IoT-based systems. FIF-IoT collects interactions that take place among various IoT entities (clouds, users, and IoT devices) as evidence and store them securely as transactions in a public, distributed and decentralized blockchain network which is similar to the Bitcoin network. A limitation to the work of Hossain *et al.,* (2018) is that the use of public blockchain to preserve forensic evidence is not recommended. This is because in a public blockchain everyone can join the network and have access to all the blocks in the network. An ideal solution for IoT Forensics is a private-permissioned blockchain where the number of nodes is restricted and access is only provided to selected users as suggested by Sadineni *et al*., (2019).

From the related works we have reviewed, it can be seen that most of them (Mercan *et al*., (2020), Li *et al.,* (2019), Ryu *et al.,* (2019), Brotsis *et al*., (2019), Hossain *et al.,* (2018)) are concentrated on the preservation process of the IoT digital forensics investigation thereby neglecting the other process of the IoT digital forensics investigation such as preparation, collection, detection, incidence response, examination, analysis, investigation and presentation. There is a need for more research on the other aspects of the IoT digital forensic investigation. This work therefore proposed a genetic fuzzy network forensic framework that will cater for the examination and analysis stage of the IoT forensics investigation. Even though the reviewed works have looked into the use of both public-permissionless and private-permissioned blockchain to guard digital evidence provenance, there is still a room for improvement. Permissioned-public blockchain has been suggested as the most ideal for guarding digital evidence provenance (Sadineni *et al*., 2019). This has been proposed theoretically by Brotsis *et al*., (2019). However, the work of Brotsis *et al*., (2019) has not been implemented and evaluated to show how it has advanced the state of the art. This research proposal therefore proposed a low cost private-permissioned blockchain IoT forensics framework that will ensure the digital evidence provenance is well preserved.

A PROPOSED LOW COST NOVEL GENETIC-FUZZY BLOCKCHAIN-ENABLED INTERNET OF THINGS (IoT) FORENSICS FRAMEWORK

This section proposes a novel low cost Genetic-Fuzzy IoT Blockchained-Enabled IoT Forensics Framework as seen in Figure 1. This novel low cost IoT Forensics Framework will use genetic algorithm for fuzzy rules optimization and Fuzzy Expert System for attack identification. The fuzzy expert system maps to the examination & analysis and presentation section of the forensic investigation process. The research will make use of the Bot-IoT dataset by Koroniotis *et al.,* (2019) to evaluate the framework. A software prototype will be developed in Python 3 programming language to implement the proposed Fuzzy-Genetic IoT Forensics Framework. The prototype will be evaluated with Network Forensic Analysis Tools that carries out examination and analysis of forensics data to see how the proposed fuzzy-genetic expert system has advanced the state of the art in the IoT Forensics subdomain using results accuracy as a metric. It is a low cost private permissioned blockchain enabled IoT forensics framework in the sense that it uses a completely free and open source private-permissioned blockchain platforms unlike the work of Mercan *et al*., (2020) that uses Ethereum, a public blockchain where a cost is incurred in the form of 'gas fees'. The study will implement the blockchain component using Hyperledger Fabric and will evaluate the proposed framework in term of cost and security with the work of Mercan *et al*., (2020). The research will make use of the Bot-IoT dataset by Koroniotis *et al.,* (2019) to evaluates it's performance with Network Forensic Analysis Tools using accuracy and performance as a yardstick to see how it has advanced the state of the art. The dataset's source files are provided in different formats, including the original pcap files, the generated argus files and csv files. The files were separated, based on attack category and subcategory, to better assist in labeling process. The captured pcap files are 69.3 GB in size, with more than 72,000,000 records. The extracted flow traffic, in csv format is 16.7 GB in size. The dataset includes DDoS, DoS, OS and Service Scan, Keylogging and Data exfiltration attacks, with the DDoS and DoS attacks further organized, based on the protocol used (Koroniotis *et al.,* 2019).

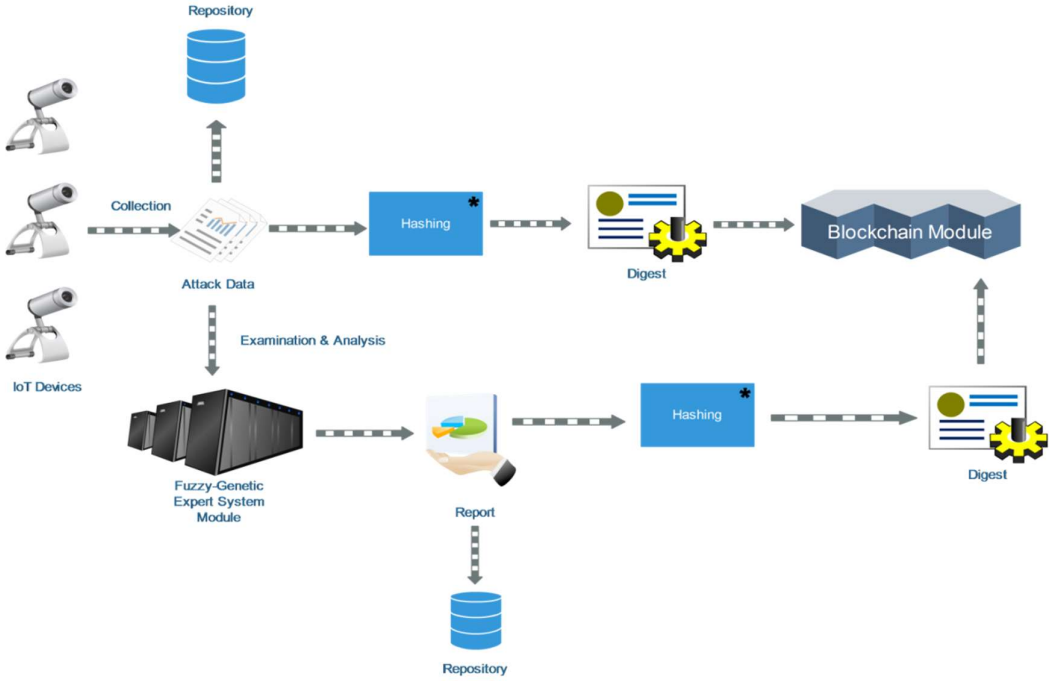


Figure 1: Proposed Fuzzy-Genetic Blockchained Enabled IoT Forensics Framework

CONCLUSION

The widespread adoption of an estimated 30.9 billion IoT devices by 2025 (Statista, 2021), as well as the increasing interconnectivity of those devices to traditional networks, not to mention to one another with the advent of fifth generation (5G) networks, underscore the need for IoT forensics (Zhang *et al*., 2020). This paper has proposed a novel low cost genetic-fuzzy blockchain-enabled Internet of Things (IoT) Forensics Framework. This novel low cost IoT Forensics Framework will use genetic algorithm for fuzzy rules optimization and Fuzzy Expert System for attack identification. It is a low cost private permissioned blockchain enabled IoT forensics framework in the sense that it uses a completely free and open source private-permissioned blockchain platforms unlike the proposed literature that uses Ethereum, a public blockchain where a cost is incurred in the form of 'gas fees'. The study will implement the blockchain component using Hyperledger Fabric and will evaluate the proposed framework in term of cost and security with related works.

REFERENCES

1. Atlam, H., Alenezi, A., Alassafi, M. O., Alshdadi, A. A., & Wills, G. B. (2020). Security, Cybercrime and Digital Forensics for IoT. In S.-L. Peng, & S. Pal, Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm (pp. 551 -). Cham, Switzerland: Springer Nature Switzerland AG.
2. Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., & Pavu´e, C. (2019). Blockchain Solutions for Forensic Evidence Preservation in IoT Environments. IEEE NetSoft 2019 - 1st Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-Defined (pp. 110-114). IEEE.
3. Cabrera et al. (2009) Fuzzy Logic, Soft Computing, and Applications.
4. Liao et al. (2009) Network forensics based on fuzzy logic and expert system
5. Datt (2016) et al. Learning network forensics https://www.packtpub.com/product/learning-network-forensics/9781782174905
6. Hossain, M., Karim, Y., & Hasan, R. (2018). FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger. 2018 IEEE International Congress on Internet of Things (ICIOT). IEEE.
7. Jawal et al. (2019) Hands-On Network Forensics
8. Koroniotis, N., & Moustafa, N. (2020). Enhancing Network Forensics with Particle Swarm and Deep Learning: The Particle Deep Framework. arXiv, 1-20.
9. Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset. Future Generation Computer Systems, 779–796.
10. Li, S., Qin, T., & Min, G. (2019). Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems. IEEE Transactions on Computational Social Systems, 1-9.
11. Lutta, P., Sedky, M., & Hassan, M. (2020). The Forensic Swing of Things: The Current Legal and Technical Challenges of IoT Forensics. World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering, 14(5), 159-165.

Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 16-21 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

AUDITORS' PROFESSIONAL COMPETENCIES ASSESSMENT MODELS

Kateryna Mokliakova , Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine
Tetiana Babenko, Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine
Andrii Bigdan, Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine
Vira Ignisca Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine

ABSTRACT: In this article, we describe an approach to mitigate information security auditors hiring process with usage of different models combination. A method of assessing the professional competencies of information security auditors that work with critical infrastructure facilities based on certification built using Rush models and Binary selection of personnel using the logistics function, and automated with artificial network application.

KEYWORDS*: information security auditor, personnel evaluation, critical infrastructure facilities, Rush model, Binary selection with logistic function, artificial neural networks.*

I. INTRODUCTION

The profession of information security auditor is design to impartially evaluate the effectiveness of information protection methods usage. The responsibility of knowledge requirements defining, certification (re-certification) of information security auditors is imposed on the public services that deals with information protection and/or special connection regulation. However, the problem of the uncertainty in professional competencies assessment methodology persists in many countries. For example, according to the Regulation [1], the State Service for Special Communications and Information Protection of Ukraine: ensures the implementation of the information security audit system at critical infrastructure facilities, sets requirements for information security auditors, their certification (re-certification); coordinates, organizes and conducts audit of security of communication and technological systems of critical infrastructure objects. Nonetheless, there is some uncertainty about the methodology for assessing the professional competencies of information security auditors in Ukraine.

Common competencies assessment methods are described in ISO 19011 [2]. Evaluation criteria includes: specialized educational level, work experience in the information security field, professional qualification (certification), experience in audit conducting, reviews of auditing activities, test results and interviews. As we can observe those methods has different quality measures: some can be represented as binary variables while the others not.

II. EMPLOYEE HIRING PROCESS

According to the research of Zinchenko [3], each organization during employees hiring process should go through two main stages: selection and election of the candidate. At the selection stage, you need to analyze the needs and scope of the organization, study the market for potential candidates and consider a strategy for finding the right person. In terms of information security audit of state institutions and critical infrastructure facilities, at the selection stage such criteria should be defined as: the need for the candidate to have access to information with limited access (by law regulation), minimum work experience or educational level, the need for professional certification (e.g. Certified information security auditor (CISA) ISACA [4], Certified internal auditor (CIA) IIA [5]).

The election stage is divided into stages: analysis of candidates' applications and information provided by them – that is considered as preliminary selection; conducting interviews and testing. Therefore, when analyzing applications, auditors who do not meet the requirements formed during the selection phase will be eliminated. Interviews and testing focus on assessing the professional competencies of the information security auditor. Interviews themselves take a subjective assessment of a person as a professional worker, and testing takes an objective site.

III. CERTIFICATION

Testing is an objective method of an auditor's qualifications determining. For the authority of the test, government agencies should follow one structure. It will make it easier for either public or private organizations who are looking for the right person to lead an information security audit. Thus, it makes sense to create a general

national certification of information security auditors. To do this, it is necessary to develop a database of questions that are created using the approaches of ISACA organization, ISO 27000 standards family [6], PCI DSS [7], etc., as leading international methods of training and education of auditors and specialists in the field of IS.

To determine the threshold for passing the certification test and the appropriate levels of qualification, a model for assessing the complexity of the questions should be chosen. The item response theory (IRT), also known as the latent response theory refers to a family of mathematical models that attempt to explain the relationship between latent traits (unobservable characteristic or attribute) and their manifestations (i.e. observed outcomes, responses, or performance). Unlike classical test theory [8], which takes the test as the unit of analysis, item response theory focuses on the item as analysis unit. It establishes a link between the properties of items on an instrument, individuals responding to these items, and the underlying trait being measured. IRT assumes that the latent construct (e.g. stress, knowledge, attitudes) and items of a measure are organized in an unobservable continuum. Therefore, its main purpose focuses on establishing the individual's position on that continuum [9]. Simply saying during the test process it worth considering the surface of other factors than knowledge.

Item response theory takes several assumptions:

- Monotonicity – The assumption indicates that as the trait level is increasing, the probability of a correct response also increases
- Unidimensionality – The model assumes that there is one dominant latent trait being measured and that this trait is the driving force for the responses observed for each item in the measure
- Local Independence – Responses given to the separate items in a test are mutually independent given a certain level of ability.
- Invariance – We are allowed to estimate the item parameters from any position on the item response curve.

Therefore, we can estimate the parameters of an item from any group of subjects who have answered the item.

In this case, it is proposed to use the Rasch model [10] for ability estimating, which provides valid results by using adequacy statistics, diagnostic information and a correlation map of the level of complexity of tasks with the level of competencies of the certified person.

Requirements for questions, according to the model of Rasch are:

- A measure of the level of preparation of any candidate $t_i \in (0; \infty)$ (regardless of the level of complexity of test tasks);
- The probability of the correct answer P_i- depends on the level of preparedness of the subject and the level of complexity of the test task $b(0; \infty)$ (ie the quantitative characteristics of the test task, which does not depend on the sample and is defined on a scale on a particular section for a particular field of knowledge), or $P = f(t, b)$.

To build a scale of measurements, it is convenient to depict the level of readiness t and the level of complexity b on the logarithmic scale: $\theta = \ln(t), \beta = \ln(b)$, where θ and β are the values of levels of readiness and complexity measured on a logarithmic scale (logits).

Thus, the mathematical function of the probability of "victory" of the subject when answering the questions calculates as (1)

$$P_j(\theta) = \{x_{ij} = 1 \,|\beta_j\} = \exp\frac{\theta - \beta_j}{1 + \exp(\theta - \beta_j)} \qquad (1)$$

Therefore, when constructing a test, the distribution of the ratio of preparedness logits and the complexity of one question should increase logarithmically. The adequacy of the questions is determined by the degree of deviation of the empirical points from the characteristic curve (Fig.1). The reason why should we rely on the characteristic curve is because it is used in the method of characteristics for solving partial differential equations.

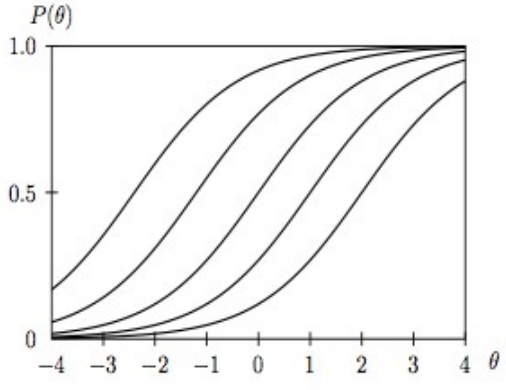


Fig. 1. *Characteristic curve of the ratio of probability and ability of a person to answer questions where* $P(\theta)$ *– probability,* θ *- ability [4]*

Based on the participants certification results, it is possible to determine the lower edge of the test score for each proficiency level (low, medium, high), and it is advisable to set a threshold of 60% correct answers as minimum requirement for the test. The division is made to robust categorize process. Therefore, based on certified level organizations can set a minimum degree requirements to gain the best outcome from the desired audit. The quality and level critical infrastructure security depends on the audit results, so the auditor must have a high level of competence. If the applicant has not "passed" the threshold - the test is considered not passed and requires examination retake.

In addition, the education path should be developed for information security auditors with practical and theoretical parts that can prepare young specialists for the entry-level auditor's work. Further implementation of those programs in higher education schools is something to keep in mind as it simplifies the education vector of the need for personnel.

IV. AUDITORS ELECTION METHOD

Next to testing, we can identify the following indicators by which the IS auditor is elected: age, higher education, profile (humanitarian/technical), work experience, professional certification, number of organizations and audits, etc. Since the election model must contain a large number of indicators, it is worth using a binary election model with a logistic distribution function, because the value of the parameters is endogenous (takes the value 0 or 1).

Suppose that the variable Y - the possibility or impossibility of taking the position of auditor IB has 2 values of $y = \{0; 1\}$. The probability that it will take one of the values is expressed as a function of several factors $x^T = \{x_1, x_2, \dots x_i\}$ (2), (3):

$$P(Y = 1|x) = F(x^T\beta) \quad (2)$$

$$P(Y = 0|x) = 1 - F(x^T\beta) \quad (3)$$

The set of parameters β is the effect of changes in each factor on the final probability. Thus, it is necessary to find an adequate function in the right part of the equation. The logits model of binary search uses the function of the logistic distribution (4):

$$P(Y = y|x) = \exp(x^T\beta)/(1 + \exp(x^T\beta)) = \Lambda(x^T\beta) \quad (4)$$

Where $\Lambda(x^T\beta)$ - lambda function of the regression vector (model factors) and function parameters. Estimation of β parameters is carried out by the method of maximum likelihood [11] (5):

$$P(Y_1 = y_1, \dots Y_n = y_n|X) = \prod_{y_i=0}[1 - F(x_i^T\beta)]\prod_{y_i=1}F(x_i^T\beta) \quad (5)$$

The logarithmic likelihood function - L for n observations [12] will have the following form (6):

$$L(\beta|data) = \prod_{i=1}^{n}[F(x_i^T\beta)]^{y_i}[1 - F(x_i^T\beta)]^{1-y_i}. \quad (6)$$

Now the likelihood equation, according to the likelihood function and partial functions - f_i, is (7):

$$\frac{dLnL}{d\beta} = \sum_{i=1}^{n}[\frac{y_i f_i}{F_i} \; | \; (1 \quad y_i)\frac{-f_i}{(1-F_i)}]x_i = 0. \quad (7)$$

Since these equations are nonlinear, numerous methods are used to solve them, such as a multidimensional interpretation of Newton's method (8):

$$\beta^{j+1} = \beta^j - H^{-1}(\beta^j)gradL(\beta^j) \quad (8)$$

Where L - Lagrangian function (method for finding the conditional extremum of a function), which basic idea is to convert a constrained problem into a form such that the derivative test of an unconstrained problem can still be applied. H - Hessian matrix [13] (square matrix of second-order partial derivatives) that describes the local curvature of a function of many variables. j – Scalar field coordinate (a scalar field associates a scalar value to every point in a space – possibly physical space).

Features of the binary regression usage to assess the candidate is based on the need for quantitative interpretation of qualitative variables. For example, audit experience may include an assessment of the organizations where it was conducted.

V. POSSIBLE PRACTICAL IMPLEMENTATION OF DESIRABLE MODEL

As been shown, classification tasks involve the assignment of available samples to certain classes. In each sample, the attribute description is assigned - a vector whose components represent various quantitative and qualitative characteristics. Thus, the task of the classification algorithm is to assign an arbitrary object to one of the classes.

To calculate the result, it is advisable to use artificial neural networks. An artificial neural network is a mathematical model and its software implementation, built on the principle of the organization and functioning of networks of neurons in the brain of a living organism [14]. An artificial neural network is a system of interconnected and interacting simple processors - artificial neurons. They can approximate functions, which allows you to build a distribution surface of great complexity, and, consequently, to effectively classify. For instance, it is possible to use the McCulloch-Pitts Neuron model [15], which is the first math model of a biological neuron. Taking several inputs $x = (x_1, x_2, \dots x_n)$ it provides a single function result of transfer function *f* (Fig.2).

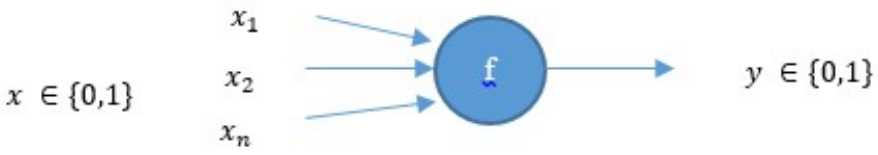


Fig. 2. *McCulloch Neuron model*

Mathematical model of McCulloch Neuron model (9)

$$y = f(u), \text{ where } u = \sum_{j=1}^{n} w_{kj} x_j + w_0 x_0 \quad (9)$$

Where x_j is the signal on the neuron input and w_j is the weight of input, function u is called induced local field and finally, $f(u)$ is the transfer function. Additional data - input x_0 and its weight w_0 are used for neuron initialization. Here the initialization means a displacement of the activation function of a neuron along the horizontal axis, that is, the formation of a neuron's sensitivity threshold [16].

Transfer function determines the dependence of the signal at the output of the neuron on the weighted sum of signals at its inputs. There are several possible transfer functions: linear, threshold (Heaviside step function), sigmoid (for instance, logistic) etc. The use of sigmoidal functions made it possible to switch from binary outputs of a neuron to analog [17]. The introduction of functions of the sigmoidal type was due to the limited nature of neural networks with a threshold activation function of neurons - with such an activation function, any of the network outputs is either zero or one, which limits the use of networks not in classification problems.

One of the disadvantages of intelligent neural networks is that they do not show exactly how individual factors affect the classification. However, related studies [3] show that in the artificial neural networks learning process it is the logit models of binary choice that shows the best result. Receiver operating characteristic (ROC) [19] also known as error curve helps to estimate the quality of binary classification. A quantitative interpretation of ROC is provided by the AUC indicator (area under ROC curve) - the area bounded by the ROC curve and the axis of the proportion of false-positive classifications. The higher the AUC indicator, the better the classifier. While the value of 0.5 demonstrates the unsuitability of the selected classification method (corresponds to random fortune-telling). A value less than 0.5 means that the classifier acts exactly the opposite: if positive are called negative and vice versa, the classifier will perform better. Therefore, the logit model helps to get an accurate result if an information security auditor should be chosen for conducting an audit. The neural network of this configuration carries out the correct classification for all workers and does not give uncertain estimates.

While take a look at Logit model (10), an artificial network should handle measures indicated in CV: age, gender, work experience (years), profile, number of organizations candidate has worked with, number of responsibilities indicated, knowledge of foreign languages, computer skills, desired salary, etc. with ratios (table 1)

$$P(Y=1|x)=\frac{e^{x}}{1+e^{x}} \quad (10)$$

Table 1 *Variables ratio*

β_0	-16,867
Gender of candidate	0,956
Age	-0,094
Higher education presence	9,472
Profile	-1,8603
Work experience (years)	0,436
Number of organizations the candidate worked in	-0,588
Responsibilities from prior work	-0,009
Knowledge of foreign languages (English)	9,859
Knowledge of foreign languages (other than English)	0,937
Computer skills	0,524
Level of desired salary	-0,00001

From the point of view of the regression quality, it is not necessary that all of the listed factors will contribute to the quality of the predictions made by the model. The statistical significance of the group of repressors is checked using the likelihood ratio statistics. On the other hand, the change in the McFadden coefficient [18] of determination after the inclusion of a new factor in the model can also indicate an improvement (deterioration) in the quality of the model. It means that further determination of precise criteria is crucial to get an adequate selection model.

Nonetheless, as mentioned earlier, the great advantage of artificial neural networks when using classification problems is due to their exceptional ability to simulate nonlinear relationships with a large number of variables.

VI. Conclusion

Therefore, to assess the professional competencies of information security auditors and to proceed election of right candidates for critical infrastructure and government agencies audits we need to complete next requirements:

- Creation of standardized certification with database of questions built based on international standards and selected according to the Rasch model.
- Usage of a binary selection model to select an information security auditor who will fit the most to conduct a specific audit, including various categories and indicators.
- Automated interpretation of the mathematical model of search using an artificial neural network, based on McCulloch-Pitts neuron model with logit function, with previous learning.

With the usage of different models, it is possible to determine the hiring process with automation and adequacy, which can be applied while speaking about choosing a candidate to lead an information security audit at critical infrastructure objects.

As a result, the further researches specified on question database creation and development of neural network with its learning is needed to achieve a comprehensive combined model of information security auditors' professional competencies assessment.

REFERENCES

1. Cabinet of Ministers of Ukraine, "Regulations on the Administration of the State Service for Special Communications and Information Protection of Ukraine", Normative document, [Online]. Available: https://www.kmu.gov.ua/npas/40371778
2. ISO/IEC 19011, Normative document, 2018, [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:19011:ed-3:v1:en
3. ZINCHENKO A. A., Modeling of processes of selection and assessment of personnel - Moscow, 2016 [Online]. Available:http://old.fa.ru/dep/ods/autorefs/Dissertations/%D0%97%D0%B8%D0%BD%D1%87%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%90.%D0%90.%20(18.02.2016)%20c0a4020b0353bfea4e08f2dec19bc0b3.pdf
4. ISACA: organization [Online]. Available: https://www.isaca.org/
5. The Institute for internal auditors [Online]. Available: https://na.theiia.org/Pages/IIAHome.aspx
6. ISO 27000 standards family [Online]. Available: https://www.itgovernance.co.uk/iso27000-family
7. Payment Card Industry Data Security Standard (PCI DSS) [Online]. Available: https://www.pcisecuritystandards.org/
8. Carlo Magno, Demonstrating the Difference between Classical Test Theory and Item Response Theory Using Derived Test Data 2009 at The International Journal of Educational and Psychological Assessment [Online]. Available: https://files.eric.ed.gov/fulltext/ED506058.pdf
9. Item Response Theory [Online]. Available: https://www.publichealth.columbia.edu/research/population-health-methods/item-response-theory
10. DEMENCHENKO O.G. Mathematical foundations of Rasch Measurement // Pedagogical Measurements, №1, 2010
11. GREENE W. H. Econometric Analysis / W. H. Greene. – New Jersey : Prentice Hall, 2012. – 802 p
12. IZENMAN A. J. Modern Multivariate Statistical Techniques: Regression, Classification, and Manifold Learning Springer / A.J. Izenman. – New York: Springer-Verlag, 2008. – 760 p.
13. Kamynin L.I. Mathematical analysis. T. 1, 2. – 2001, [Online]. Available: https://obuchalka.org/2014112580869/kurs-matematicheskogo-analiza-tom-1-kaminin-l-i-2001.html
14. V.V. Kruglov, V.V. Borisov Artificial neural networks. Theory and practice, 2002, [Online]. Available: https://www.twirpx.com/file/955659/
15. Snehashish Chakravert, Deepti Moyi Sahoo, Nisha Rani Mahato: McCulloch-Pitts Neuron model, 2019 , [Online]. Available: http://link-springer-com-443.webvpn.fjmu.edu.cn/chapter/10.1007%2F978-981-13-7430-2_11
16. Yasnitsky L.N. Introduction to artificial intelligence, 2005, [Online]. Available: https://www.studmed.ru/yasnickiy-ln-vvedenie-v-iskusstvennyy-intellekt_48d6e6cb970.html
17. Terekhov V.A., Efimov D.V., Tyukin I.Yu.: Neural network control systems, 2002, [Online]. Available: https://www.twirpx.com/file/273937/
18. Daniel McFadden: Conditional logit analysis of qualitative choice behaviorm, 1973, [Online]. Availabel: https://eml.berkeley.edu/reprints/mcfadden/zarembka.pdf
19. Tom Fawcett: An introduction to ROC analysis, 2006 [Online]. Available: https://people.inf.elte.hu/kiss/13dwhdm/roc.pdf

Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 22-34 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

CONFLICT SITUATIONS AND INTERACTIONS OF THE PARTIES

Volodymyr Khoroshko, National Aviation University, Doctor in Technical Sciences, Professor, Kyiv, Ukraine,
Serhii Zybin, National Aviation University, Doctor in Technical Sciences, Professor, Kyiv, Ukraine,

Nikolay Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor, Kyiv, Ukraine,
Yuliia Khokhlachova, National Aviation University, PhD in Engineering Science, Associate Professor, Kyiv, Ukraine

ABSTRACT. The article reveals the application of game theory in the analysis of information warfare. It can significantly reduce the errors and omissions that occur in information security management. That, in turn, minimizes the negative and undesirable political, social and financial consequences for the subjects of information confrontation. The solution of the problems of information confrontation is impossible without the development of new theoretical and methodological principles for the analysis of confrontation processes. The authors studied the scheme of finding sustainable strategies, which ensure neutralization of the enemy. The scheme for finding sustainable strategies always turns out to be useful in many problems and, in particular, in the game theory with a choice of a moment in time.

KEYWORDS: *game theory, payoff function, cyberspace, sustainable strategy, cyberwar, hybrid war, counteraction, neutralize, a moment in time, attack on information, conflict management*.

Introduction

In recent years, due to the rapid development of operations research in solving practical problems of systems engineering, it has become possible to study conflict situations taking into account reality and, first of all, taking into account situations of uncertainty.

The theoretical basis for the study of conflict situations is game theory. Information warfare and cyberwarfare contributed to the widespread adoption of game theory [1]. New forms and methods of counteraction have appeared. The classic forms of confrontation have been replaced by hybrid methods. They are of a hidden nature and are carried out mainly in the political, economic, informational and other spheres. Solving the problems of information protection, countering attacks and information impacts remain relevant for the entire world community.

Currently, game-theoretic methods [2] are successfully used to solve a wide variety of problems. The application of game theory in solving problems of various conflicts in information wars, information and information-psychological confrontation in information and geopolitical spaces gives especially great benefit.

Game theory is a mathematical theory of conflict situations. In these situations, the interests of two or more parties collide, which pursue different, opposite goals. The direct subject of study the game theory is the mathematical analysis of a formalized model of conflict, which takes into account the peculiarities of a real conflict situation. The technique itself is the formalization of a specific conflict situation does not apply to the mathematical theory of games. It is within the competence of specialists in the field, which is affected by this conflict situation.

Each conflict situation that is considered in practice is a difficult situation. Its analysis is hampered by many secondary factors. Therefore, in order to make possible a mathematical analysis of the situation, it is necessary to abstract from these incidental factors and build a simplified, formalized model of the situation. At the same time, the formalization should be

such that the possible ways of behaviour of the participants and the results are visible to which all possible combinations of actions of all participants in the conflict lead.

Literature survey

Following modern research trends can be identified in this area: building influence models (information cascades (IC) [3]; linear thresholds (LT) [4], probabilistic models [5]; construction of effective algorithms for maximizing the impact (based on the apparatus of submodular functions (greedy algorithm) and its improvement, CELF [6], CELF ++ [7]); using local properties of the graph (LDAG [8], SimPath [9]); thinning the graph [10]; simulated annealing [11]; network monitoring optimization algorithms [6]; variations of the influence maximization problem and solution algorithms (maximizing influence blocking [12], maximizing influence taking into account time [13], thematic distribution of influence [14]); game-theoretic models of information influence [15, 16].

The purpose and objectives of the study

The analysis of scientific and technical literature [17 - 21] showed that to date the following issues of application of game theory have not been solved within the problem of information protection: the task of information protection has not been structured; no areas of quantitative estimates have found; no guaranteed assessments of the level of information security were found; optimal strategies for attacking and protecting information have not been found; the solution of information protection problems described by stochastic models is not fully found; the behaviour of information attacks during the duration of information conflicts has not been studied.

Modelling of information attack processes involves the reflection in the developed models of dynamic properties due to the conflict nature and related ideas about the optimal distribution of information resources of players [22].

Mathematical modelling of physical processes by methods of game theory is based on the following factors that verbally determine the essence of this theory [23]: the presence of a system of differential equations, which describes the change over time in the parameters of the processes being modelled; definition of admissible controls of players, in the form of a class of functions on which the corresponding restrictions are imposed; goals of players in the form of functionalities; information that is available to players at the beginning of the game and in the process.

Thus, the use of game theory in information confrontation requires detailed research, which is the purpose of the article.

Solutions of games with a choice of time

Tasks related to the timing of actions occur in many problems of information confrontation, which use game theory applications [24]. In such tasks, to the players are set in advance. During the action, the goal is set by strategic decisions of the players (the attacker and the defending side). In general, the payoff function of such games has the following form [25]

$$M(x,y) = \begin{cases} K(x,y)\ for\ x < y, \\ I(x)\ for\ x = y, \\ L(x,y)\ forx > y \end{cases} \quad (1)$$

here various restrictions can be imposed on the functions *K, I* and *L*. They are determined by the specific conditions of the problem being solved.

Many works [26, 27] devoted to the study of games with payoff function (1). The corresponding mutually exclusive classification of all types of games is given in Karlin's monograph [27]. Before stating the results, we introduce some notation. We denote the distribution function *P(x)*, which has a jump in α at zero and a jump in β at unity, by $P(x) = (\alpha I_0, P_{ab}(x), \beta I_1)$ where, the distribution density $P_{ab}(x)$ is a continuous function in the entire interval $[a, b] \subset [0,1]$.

Therefore, the following theorem is true.

Theorem 1 [27]. Let the payoff function of a continuous game has the following form:

$$M(x,y) = \begin{cases} K(x,y)\ for\ x < y, \\ L(x,y)\ for\ x > y, \\ K(x,y) = L(x,x) \end{cases} \tag{2}$$

The functions *K* and *L* satisfy the following conditions:

1) The functions $K(x,y)$ and $L(x,y)$ have continuous third partial derivatives in their domains of definition.

2) The derivatives $K_{xx}(x,y)$ and $K_{yy}(x,y)$ are strictly negative for $x \leq y$, and the derivatives $L_{xx}(x,y)$ and $L_{yy}(x,y)$ are strictly negative for $x \geq y$.

3) The function $K(x,y)$ strictly increases in *y* and strictly decreases in *x*, and the function $L(x,y)$ strictly increases in *x* and strictly decreases in *y*.

Then both sides have unique optimal mixed strategies of the following form

$$F(x) = (\propto I_0, f(x), \beta I_1), \tag{3}$$

$$H(y) = (\gamma I_0, h(y), \delta I_1). \tag{4}$$

Here $f(x)$ and $f(y)$ are absolutely continuous in the entire interval [0,1] and are obtained as the only solutions of a pair of integral equations:

$$\propto p_1 + \beta p_2 = f + T_f, \tag{5}$$

$$\gamma p_1 + \delta p_2 = h + R_h \tag{6}$$

$$T_f = \int_0^y \frac{K_{yy}(x,y)}{K_y(y,y) - L_y(y,y)} f(x)dx + \int_y^1 \frac{L_{yy}(x,y)}{K_y(y,y) - L_y(y,y)} f(x)dx \tag{7}$$

$$R_h = \int_0^x \frac{L_{xx}(x,y)}{L_x(x,x) - K_x(x,x)} h(y)dy + \int_x^1 \frac{K_{xx}(x,y)}{L_x(x,x) - K_x(x,x)} h(y)dy \tag{8}$$

$$p_1 = -\frac{K_{yy}(0,y)}{K_y(y,y) - L_y(y,y)} \tag{9}$$

$$p_2 = -\frac{L_{yy}(1,y)}{K_y(y,y) - L_y(y,y)}$$

$$q_1 = -\frac{L_{xx}(x,0)}{L_x(x,x) - K_x(x,x)}$$
$$q_2 = -\frac{K_{xx}(x,1)}{L_x(x,x) - K_x(x,x)} \quad (10)$$

The constants $\propto, \beta, \gamma, \delta$ are determined from the following conditions:

$$\int_0^1 f(x)dx = 1 - \propto - \beta, (0 \leq \propto, \beta \leq 1) \quad (11)$$

$$\int_0^1 h(y)dy = 1 - \gamma - \delta, (0 \leq \gamma, \delta \leq 1) \quad (12)$$

Thus, the solution of the game under consideration is reduced to the solution of integral equations. This solution is a simple task. These equations are classic integral equations. In particular, we use the expansion of unknown functions *f* and *h* in a Neumann series in order to find analytical solutions.

There are general results that can be formulated as the following theorem [27]:

Theorem 2.

Let the payoff function of a continuous game has the following form:

$$M(x,y) = \begin{cases} K(x,y)\ for x < y, \\ l(x)\ for\ x = y, \\ L(x,y)\ for\ x > y \end{cases} \quad (13)$$

The functions *K, l, L* satisfy the following conditions:

1. The functions $K(x,y)$ and $L(x,y)$ are defined and have continuous second partial derivatives on closed triangles $0 \leq x \leq y \leq 1$ and $0 \leq y \leq x \leq 1$, respectively.

2. The $l(1)$ value lies between $K(1,1)$ and $L(1,1)$; the $l(0)$ value lies between $K(0,0)$ and $L(0,0)$.

3. $K_x(x,y) > 0$ and $L_x(x,y) > 0$ are located in the corresponding closed triangles with the possible exception of $L_x(1,1) = 0$; $K_y(x,y) < 0$ and $L_y(x,y) < 0$ in the corresponding closed triangles with the possible exception of $K_y(1,1) = 0$.

Then, both sides have optimal strategies of the following form

$$F(x) = \left(\propto I_0, f_{\propto_1}, \beta I_1\right),$$

$$H(y) = \left(\gamma I_0, h_{\propto_1}, \delta I_1\right),$$

The distribution densities $f_{\propto_1}$ and $h_{\propto_1}$ are determined as solutions of the following integral equations:

$$f_{a_1}(t) - \int_a^1 T_{a_1}(x,t) f_{\propto_1}(x)dx = \propto p_1(t) + \beta p_2(t); \tag{14}$$

$$h_{a_1}(u) - \int_a^1 U_{a_1}(u,y) h_{\propto_1}(y)dy = \gamma q_1(u) + \delta q_2(u); \tag{15}$$

$$T_{a_1}(x,t) = \begin{cases} \dfrac{-K_y(x,t)}{K(t,t) - L(t,t)}; \ a \le x < t \le 1; \\ \dfrac{-L_y(x,t)}{K(t,t) - L(t,t)}; \ \mathrm{a} \le t \le x \le 1; \end{cases} \tag{16}$$

$$U_{a_1}(u,y) = \begin{cases} \dfrac{L_x(u,y)}{K(u,u) - L(u,u)}; \ a \le y < u \le 1; \\ \dfrac{K_x(u,y)}{K(u,u) - L(u,u)}; \ a \le u \le y \le 1; \end{cases} \tag{17}$$

$$\begin{aligned} p_1(t) &= \frac{-K_y(0,t)}{K(t,t) - L(t,t)} \\ p_2(t) &= \frac{-L_y(1,t)}{K(t,t) - L(t,t)} \end{aligned} \tag{18}$$

$$\begin{aligned} q_1(u) &= \frac{L_x(u,0)}{K(u,u) - L(u,u)} \\ q_2(u) &= \frac{K_x(u,1)}{U(u,u) - L(u,u)} \end{aligned} \tag{19}$$

The constants $\propto, \beta, \gamma, \delta$ and a are determined from the following conditions

$$\int_a^1 f_{a_1}(x)dx = 1 - \propto - \beta, (0 \le \propto, \beta \le 1) \tag{20}$$

$$\int_a^1 h_{a_1}(y)dy = 1 - \gamma - \delta, (0 \le \gamma, \delta \le 1) \tag{21}$$

Remark 1.

It follows from the equation (13) that if $K(1,1) < L(1,1)$, then the point $x = 1$ and $y = 1$ is a saddle point for $M(x, y)$. This follows from condition (2) of the Theorem 1.

Corollary 1.

For the case $l(x) = 0$ and $-\mathrm{K(x,y)} = \mathrm{L(x,y)}$, the game is called symmetric.

The symmetric game is investigated for the case when the function $M(x, y)$ in the region $0 \leq (x \leq y \leq 1)$ is continuous in both variables and has continuous first-order partial derivatives $M_x(x, y) \geq 0, M_y(x, y) \leq 0$ for $x \leq y$ and the set of points for which $M_x(x, y) = 0$ or $M_y(x, y) = 0$ does not contain any interval of the form $x = const$, $\beta_1 < y < \beta_2$ or the form $y = const$, $\propto_1 < x < \propto_2$.

For $K(1,1,) \leq 0$, the optimal strategy is the unique and has the following form

$$F(x) = I_1 = \begin{cases} 0 \; for \; 0 \leq x < 1, \\ 1 \; for \; x = 1. \end{cases} \tag{22}$$

For $K(0,1,) > 0$, there is an optimal strategy of the following form:

$$F(x) = I_0 = \begin{cases} 0 \; for \; x = 0, \\ 1 \; for \; 0 < x \leq 1. \end{cases} \tag{23}$$

In the case $K(0,1,) < 0 < K(1,1)$, we can assume without loss of generality $K(x, x,) > 0$ for $0 < x \leq 1$. Then there is a uniquely defined interval of the form $[a, 1], 0 \leq a \leq 1$, such that the optimal strategy is as follows:

$$F(x) = \begin{cases} 0 \; for \; x = 0, \\ \propto for \; 0 < x \leq a, \\ \propto - \int_a^x f_{a_1}(z)dz \; for \; a < x \leq 1 \end{cases} \tag{24}$$

The function $f_{a_1}(x)$ is a continuous, positive function. The parameter $\propto$ is the jump of $F(x)$ at zero and is determined from the normalization equation:

$$\int_a^1 f_{a_1}(z)dz \; = 1 - \propto \tag{25}$$

From the Theorem 1 it follows that the optimal strategy $F(x)$ for a symmetric game in the case under consideration exists only if it is possible to find numbers $a, \propto$, that satisfy the conditions $0 \leq a, \propto < 1$ and such a continuous non-negative function $f_{a_1}(x)$ for $a < x < 1$ such that

$$aK(0, y) + \int_a^y K(x, y) f_{a_1}(x)dx \; - \int_y^1 K(y, x) f_{a_1}(x)dx \; = 0, (a < y < 1) \tag{26}$$

Remark 2.

The case of the function $M(x,y)$, which increases in y and decreases in x, using the substitution $z = 1 - x$, $\eta = 1 - y$ reduces to the case of increasing in x and decreasing in y, which was considered in the Theorem 1.

Remark 3.

If in the Theorem 1, instead of the condition (1), we assume that $\left(K_y(y,y) - L_y(y,y)\right) > 0$ and $\left(K_x(x,x) - L_x(x,x)\right) > 0$, then one can verify [27, 28] that the optimal strategies of both parties have the form of the distribution function $F(x) = (\propto I_a, f_{ab}(x), \beta I_b)$ and $H(y) = (\gamma I_a, h_{ab}(y), \delta I_b)$, where $\propto, \beta, \gamma, \delta \geq 0$, and the function $f_{ab}(x)$ and $h_{ab}(y)$ are obtained in the form of Neumann series in the eigenfunctions of the conjugate integral equations

$$f_{ab}(t) - \int_a^b T_{ab}(x,t) f_{ab}(x) dx \ = \propto p_1(t) + \beta p_2(t) \tag{27}$$

$$h_{ab}(t) - \int_a^b U_{ab}(u,y) h_{ab}(y) dy \ = \gamma q_1(u) + \delta q_2(u) \tag{28}$$

Next, consider a special class of symmetric games for which $M(x,y)$ is not necessarily continuous in the set of variables at the points (0,0) and (1,1), and it is only required that the following limits exist

$$K(0,0) = \lim_{y \to 0} K(0,y)\,; K(1,1) = \lim_{x \to 0} K(x,1). \tag{29}$$

We will assume that

$$K(x,y) = k\left(\frac{x}{y}\right), \tag{30}$$

The function *k (u)* is continuously differentiable in the interval $0 \leq u \leq 1$ and its derivative $k'(u)$ does not change sign on this interval. Moreover, the set of points u for which $k'(u) = 0$ does not contain any interval.

It is easy to see that for $k'(u) \geq 0$, the negative strategy is $F(x) = I_1$, for $k(1) \leq 0$ and $F(x) = I_0$, for $k(1) \geq 0$. The proof of this fact is based on the idea of finding sustainable strategies. For this, we write the equality

$$C_1(F, +0) = C_1(F, 0) + \propto K(0,0) = C_1(F, 0) + \propto k(0). \tag{31}$$

The validity of this equality is established using (29). Indeed, for $\delta > 0$ we have the following expression

$$C_1(F, \delta) = \int_0^{\delta - 0} K(x, \delta) dF(x) - \int_\delta^1 K(\delta, x) dF(x), \tag{32}$$

$$C_1(F,0) = -\int_{+\delta}^{1} K(0,x)dF(x). \tag{33}$$

Thus

$$C_1(F,\delta) - C_1(F,0) =$$
$$= \propto K(0,\delta) + \int_{+0}^{\delta-0} K(x,\delta)dF(x) - \int_{\delta}^{1} K(\delta,x)dF(x) + \int_{+\delta}^{1} K(0,x)dF(x) \tag{34}$$

The first term on the right-hand side of formula (34) as $\delta \to 0$, taking into account (29), tends to $\propto K(0,0)$. In order to estimate the integrals in (34), for a given $\varepsilon > 0$, we choose η such that the total variation of $F(x)$ in $[0,\eta]$ is less than $\varepsilon/4K_0$, where $K_0 = sup|K(x,y)|$. Then the first integral will be less than $\varepsilon/4$, and the next two can be represented as:

$$\int_{1+0}^{\eta} K(0,x)dF(x) - \int_{\delta}^{\eta} K(\delta,x)dF(x) +$$
$$+ \int_{\eta}^{1+0} \big(K(0,x) - K(\delta,x)\big)dF(x) = I_1 + I_2 + I_3. \tag{35}$$

It is obvious from (35) that all $|I_i| \le \varepsilon/4, i = 1,2,3$. Hence, this proves the validity of (31).

Let us first take the value $a = 0$. From $C_1(F,y) = 0$ for $a < y < 1$ it follows that $C_1(F,+0) = 0$. For $a > 0$, it should be $C_1(F,0) = 0$. It leads to a contradiction with (31), due to the expression $k(0) < 0$. On the other hand, for $\propto = 0$ we have the following expression

$$C_1(F,+0) = -\int_{0}^{1} k(0)f(x)dx = -k(0)\int_{0}^{1} f(x)dx = -k(0) > 0 \tag{36}$$

that, obviously, it is also impossible. If we take $\propto > 0$, then from $C_1(F,a) = 0$ and strict decrease of the function we obtain

$$C_1(F,y) = \propto k(0) - \int_{a}^{1} k\left(\frac{y}{x}\right) f(x)dx \tag{37}$$

on the interval $0 < y \le \propto$ we get $C_1(F,+0) > 0$. If $\propto > 0$ and $C_1(F,0) = 0$, then from expression (31) we obtain $C_1(F,+0) = \propto k(0) < 0$. This is a contradiction. Hence $\propto > 0$ and $\propto = 0$. In this case, expression (26) is equivalent to the expression $C_1(F,y) = 0$ on the interval $(\propto, 1)$ under the condition $C_1'(F,y) = 0$. From this expression, we obtain an integral equation for determining the density $f(x)$)

$$2k(1)f(y) = \int_a^y \frac{x}{y^2} k'\left(\frac{x}{y}\right) f(x)dx + \int_y^1 \frac{f(x)}{x} k'\left(\frac{y}{x}\right) dx\,, (a < y < 1). \quad (38)$$

In this case, the normalization condition must be satisfied

$$\int_a^1 f(x)dx = 1.$$

Remark 4.

For the case $k'(u) \leq 0$, it can be shown [28, 29] that optimal strategies are $F(x) = \propto I_0 + \beta I_1$. In addition, it is easy to check the validity of the following expressions

$$F(x) = \begin{cases} I_1(x) for\ k(0) < 0, \\ \propto I_0(x) + (1-\propto) I_1(x)\ \ for\ k(0) = 0\ (0 \leq \propto \leq 1), \\ I_0(x)\ for\ k(0) > 0. \end{cases}$$

The solution of the game $G(M, [0,1])$ with the payoff function $M(x, y), (0 \leq x, y \leq 1)$ is called a pair of distribution functions (strategies) F_1^* and F_2^* and a real number υ (value of the game) that satisfies the condition

$$\int_0^1 M(x, y) d\, F_2^*(y) \leq \upsilon \leq \int_0^1 M(x, y) d\, F_1^*(x), 0 \leq x, y \leq 1.$$

From this expression it follows that if player $G1$ uses the strategy F_1^*, then the average payoff is calculated by the following formula

$$F(F_1^*, F_2) = \iint_0^1 M(x, y) dF_1^*(x) dF_2^*(y).$$

This payoff cannot be less than the number υ, i.e. player $G1$, as it were, neutralizes the opponent's actions. And, conversely, if player $G2$ applies the strategy F_2^*, then his average loss $F(F_1, F_2^*)$ will always be greater than the number υ, regardless of the actions of player $G1$. Therefore, it is natural that each player should strive to choose such distribution functions F_1^* and F_2^*, which could neutralize the opponent's actions. Indeed, for the $G1$ player, the best strategy is a strategy that makes his average winnings as large as possible within reason, regardless of the opponent's actions. And, conversely, player $G2$ must choose a strategy that would provide him, within reasonable limits, the smallest possible loss, regardless of the actions of player $G1$. Naturally, if the game has an equilibrium position on the space of distribution functions, then only in this case the players can choose optimal strategies [30].

In general, the player $G1$ can guarantee himself a payoff of at least

$$\upsilon_1 = \max_{F_1} \min_y \int_0^1 C_1(F_1) d\, F_2(y) = \max_{F_1} \min_y C_1[F_1(y)]. \quad (39)$$

Here

$$C_1(F_1) = \int_0^1 M(x,y)dF_1(x).$$

Similarly, the player $G2$, by the appropriate choice of the distribution function $F_2(y)$, can guarantee himself a loss of no more than

$$\upsilon_2 = \min_{F_2} \max_{F_1} \int_0^1 C_2(F_2)d\,F_1(x) = \min_{F_2} \max_{x} C_2[F_2(x)]. \quad (40)$$

Here

$$C_2(F_2) = \int_0^1 M(x,y)dF_2(y).$$

From the equation (39) and the equation (40) we obtain

$$\begin{aligned} \upsilon_1 &\geq \min_{y} C_1(F_1) \\ \upsilon_2 &\leq \max_{x} C_2(F_2), \end{aligned} \quad (41)$$

Let player $G2$ choose the distribution function $F_{20}(y)$ as his strategy, and let player $G1$ know this choice. Naturally, assuming such an opportunity, the $G2$ player should strive to find a sustainable strategy. From (41) it becomes clear that if the value $C_2(F_2)$ has a maximum, then the player $G1$ will always get the best result, choosing a point χ_0 that corresponds to this maximum

$$\upsilon_0 \leq C_2\big(F_2(\chi_0)\big) = \max_{\chi} C_2(F_2(\chi)).$$

It would be beneficial for the player $G2$ to bring the value of $C_2(F_2(x))$ to a minimum, but this is not always possible. The player cannot influence the form of the payoff function and the choice of χ_0 by the player $G1$. Nevertheless, player $G2$ can in any case try to choose the strategy $F_{20}(y)$ so that the value of $C_2(F_2)$ does not have a single maximum, that is, so that its "curve" has a flat top.

Similarly, if player $G2$ has learned the strategy of player $G1$, then he will always choose the point y_0 at which the function $C_1(F_1(y))$ will take the minimum value. In this case, the task of the player $G1$ is to choose such a strategy $F_{10}(x)$ so that the function $C_1(F_1(y))$ does not have a single minimum.

We denote $\Omega_1 = \{x: C_2(F_2(x)) = \nu_1 = const\}$ and $\Omega_2 = \{y: C_1(F_1(y)) = \nu_2 = const\}$, where ν_1 and ν_2 are arbitrary numbers, and $\upsilon_1 \leq \nu_1 \leq \nu_2 \leq \upsilon_2$.

If there is such a pair of real numbers $(\nu_1 \leq \nu_2)$ and a pair of distribution functions (F_1, F_2), which simultaneously satisfies the following conditions

$$C_1(F_1(y))\begin{cases}= \nu_1 \; for \; y \in \Omega_2, \\ > \nu_1 \; for \; y \notin \Omega_2. \end{cases} \quad (42)$$

$$C_2(F_2(x))\begin{cases}= \nu_2 \; for \; x \in \Omega_1, \\ > \nu_2 \; for \; x \notin \Omega_1, \end{cases} \quad (43)$$

then the functions F_1 and F_2 will be called stable [27, 30] strategies.

The question of the existence of sustainable strategies for the payoff function $M(x, y)$ in most cases remains unsolved. The scheme itself finding sustainable strategies is always useful in many applications and, in particular, in the game theory with a choice of a moment in time. Such games do not require the definition of strategies that neutralize the enemy. It turns out [27, 30] that instead of them one can be content with partially stable strategies, i.e. strategies that provide the player with a stable position in a certain subinterval of the unit interval.

Conclusion

Widespread use of game theory in the analysis of attacks on information resources and countering them can significantly reduce errors and miscalculations that occur in the management of information security, which in turn minimizes the negative and adverse political, social and financial consequences for the subjects of information warfare.

Systematic studies of the behaviour for complex dynamic processes requires consideration of a large number of features and relationships, processes typical attacks on information and informational influences. The investigated features contradict one another; however, each of them cannot be neglected, since they give us a complete picture of the process that investigates or simulates. Some incorrectness of the tasks being solved, generated by the antagonistic goals of the subjects, is manifested in their multi-criteria setting, where the players' resources are the partial quality criteria.

REFERENCES

1. Pirchalava L.G., Khoroshko V.A., Khohlachjova Ju.E., Shelest M.E. Informacionnoe protivoborstvo v sovremennyh uslovijah. K: CP "Komprint", 2019. – 226 s. [in Russian].

2. Avinash K. Dixit, Susan Skeath, David McAdams. Games of Strategy. (Fifth Edition). W.W. Norton, 2020. – 768 p.

3. Kempe D., Kleinberg J., Tardos E. Maximizing the spread of influence through a social network. Proceeding KDD '03 Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, 2003, ACM New York, NY, USA, pp. 137–146.

4. Kempe D., Kleinberg J., Tardos E. Maximizing the spread of influence through a social network. Proceeding KDD '03 Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, 2003, ACM New York, NY, USA, pp. 137 – 146.

5. Domingos P., Richardson M. Mining the Network Value of Customers. Proceedings of the Seventh International Conference on Knowledge Discovery and Data Mining, 2002. Zhang D., Gatica-perez D., Bengio S., Roy D. Learning influence among interacting Markov chains. Advances in Neural Information Processing Systems, 2005, 18.

6. Leskovec J. Cost-effective outbreak detection in networks. Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), 2007, pp. 420 – 429.

7. Goyal A., Lu W., Lakshmanan L.V.S. CELF++: Optimizing the greedy algorithm for influence maximization in social networks, 2011.

8. Chen W., Yuan Y., Zhang L. Scalable influence maximization in social networks under the linear threshold model. ICDM, 2010.

9. Goyal A. SIMPATH: An Efficient Algorithm for Influence Maximization un-der the Linear Threshold Model. Proceeding ICDM '11 Proceedings of the 2011 IEEE 11th International Conference on Data Mining, 2011.

10. Mathioudakis M., Bonchi F., Castillo C., Gionis A., Ukkonen A. Sparsification of influence networks. KDD, 2011, pp. 529 – 537.

11. Jiang Q. Song G., Cong G., Wang Y., Si W., Xie K. Simulated Annealing Based Influence Maximization in Social Networks, AAAI, 2011.

12. He X., Song G., Chen W., Jiang Q. Influence blocking maximization in social networks under the competitive linear threshold model. Proceedings of the 12th SIAM International Conference on Data Mining (SDM'2012), 2012.

13. Chen W., Lu W., Zhang N. Time-critical influence maximization in social networks with time-delayed diffusion process. Proceedings of the 26th Conference on Artificial Intelligence (AAAI'2012), 2012.

14. Tang J. Social influence analysis in large-scale networks, KDD, 2009.

15. Jain M., Korzhyk D., Vanek O., Conitzer V., Pechoucek M., Tambe M. A double oracle algorithm for zero-sum security games on graphs. Proceeding AAMAS '11 The 10th International Conference on Autonomous Agents and Multiagent Systems, 2011, vol. 1.

16. Tsai J., Nguyen T. H., Tambe M. Security Games for Controlling Contagion, AAAI, 2012.

17. Lenkov S.V. Metody i sredstva zashhity informacii: v 2-h t / Lenkov S.V., Peregudov D.A., Khoroshko V.A. – K.: Arij, 2008. – 464 s. [In Russian].

18. Kobozeva A.A. Analiz informacionnoj bezopasnosti / Kobozeva A.A., KhoroshkoV.A.–K.: izd. GUIKT, 2009. – 251 s. [In Russian].

19. Differential Games: A Mathematical Theory with Applications to Warfare and Pursuit, Control and Optimization. Rufus Isaacs. Courier Corporation. – 1999 – p. 384.

20. Differential Games. Avner Friedman. Courier Corporation. 2013 – p. 368

21. Smol'jakov E.R.Teorija antagonizmov i differencial'nye igry / Smol'jakov E.R. – M.: Jeditorial URSS, 2000. – 160 s. [In Russian].

22. Vasylev V.V. Modelyrovanye zadach optymyzatsyy i dyfferentsyalnykh yhr / V.V. Vasylev, V.L. Baranov. – K.: Naukova dumka, 1989. – 286 s. [In Ukraininan].

23. Differential Games: A Mathematical Theory with Applications to Warfare and Pursuit, Control and Optimization. Rufus Isaacs. Courier Corporation. – 1999 – p. 384.

24. Petrosjan L.A. Teorija igr. / Petrosjan L.A., Zenkevich N.A., Shevkopljas E.V. SPb.: BXB-Peterburg, 2012 – 432 s. [In Russian].

25. A. V. Krushevskij. Teorija igr / A. V. Krushevskij – M.: Kniga po Trebovaniju, 2013. – 216 s. [In Russian].

26. M. Dresher. Games of Strategy: Theory and Applications. Prentice Hall. – 1961. – 186 p.

27. Karlin S. Matematicheskie metody v teorii igr, programmirovanii i jekonomike. / S. Karlin. – M.: Mir, 1964. – 835 s. [In Russian].

28. Wolfersdorf L. Eine Bemerkung zur Theorie der symmetrischen Zeltspide. "Elektron. Juf. – verarb und Kybernet", 1999, v.3, N5. – pp. 54 – 68.

29. Hryshchuk R.V. Teoretychni osnovy modeliuvannia protsesiv napadu na informatsiiu metodamy teorii dyferentsialnykh ihor ta dyferentsialnykh peretvoren. / R.V. Hryshchuk. – Zhytomyr. Ruta, 2010. - 280 s. [In Ukrainian].

30. Khoroshko V. The use of Game Theory to Study Processes in the Informational Confrontation / V. Khoroshko, R. Hryshchuk, N. Brailovsky, T. Shcherbak // Scientific and Practical Cyber Security Journal (SPCSJ) 4(3). – pp. 45 – 51.

Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 35-39 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

USING OPEN SOURCE INTELLIGENCE (OSINT) AS ONE OF THE EFFECTIVE AND LEGITIMATE WAYS TO AVOID THREATS TO THE CORPORATION

Oleksii Kuchmai, Tetiana Shelest

Taras Shevchenko National University of Kyiv, 24 B. Gavrilishyna St., Faculty of Information Technology, Kiev, 02000, Ukraine

ABSTRACT: Open source intelligence (OSINT) is an intelligence discipline that includes the search, selection and collection of intelligence from publicly available sources, as well as its analysis. In the intelligence community, the term "open information source" refers to the public availability of a source (as opposed to secret and restricted sources), but it is not related to the notion of "just a source of information" (English open source information; OSIF), which means any information in the media space.

KEYWORDS: *Cyber Intelligence, OSINT, Cybercrime, Threats, Company, Security*

Introduction

The current OSINT regulatory framework is based on the Directive of the Director of National Intelligence (2006) ICD 301 "National Plan for Intelligence Based on Open Sources". It defines the following strategic objectives of ROII: - the principle of "first step" - OSINT should be the "first step" for all intelligence disciplines and precede intelligence and intelligence by technical means; - reliance on specially trained groups of experts in the field of ROII, training in methods of obtaining open information and implementation of ROII technologies in all intelligence processes; - global coverage of information sources; - a single architecture of means, forms and methods of ROII; - the use of the principle of skunkworks, ie the introduction to solve certain problems of "breakthrough", highly intelligent methods of obtaining information with a minimum of bureaucratic red tape and restrictions. air force "[1].

Regulatory framework

The law enforcement OSINT community applies open-source intelligence to crime prediction, prevention, investigation, and prosecution, including terrorism. Search through social media and DarkNet plays a significant role in their work, and so does connection analysis [2]. With the sheer volume of content traffic transiting across the internet through social media platforms, law enforcement would be remiss to ignore social media accounts as a resource for discovering evidence potentially relevant to a variety of criminal investigations.

Private corporate security services are also eager to apply OSINT tools. They conduct individual checks: their own employees, top-management, employees, executive officers and shareholders of their contractors. 'Know Your Customer' (KYC) mode is on here. Is this an off-shore company or not? Who is the real owner? Hasn`t it been into any dark business? Knowing this is crucial before execution of any major deal.[3]

To check affiliation of individuals or entities - this is the main goal, as it is expressed usually. Economic security services monitor internal deals for hidden interest. For instance, if a procurement manager enters into transactions with entities belonging to his or her family members. Transaction services department runs check-ups before each merger or acquisition: whether a firm acquired is run by criminals. Thus, major companies endeavor to minimize reputational risks for the company, as for the shareholders. Each serious firm usually has its own list of reliable and non-advisable counter agents. In any case, management always has to know, who stands behind this or that entity[4].

Interesting cases of application of OSINT in insurance business have already come into our knowledge. They correlate to a company's personal data analysis, as so as to business analytics. A huge federal company notices that in one separate region payments for one separate insurance product have increased significantly.

Affiliation checks through social media of the company's region branch employees has shown that one of the managers had been insuring his or her friends and family in order to register insured accidents and payments afterwards. Such knowledge is still not an evidence of the person's guilt, but it sure is a matter for internal investigation.

HR departments [8] employ OSINT for running check-ups of actual or possible employees of their companies. Do they post any negative data on the company in their social media? Or maybe they disclose confidential information? Sometimes it happens not out of malice but accidentally [5].

Some public organizations perform constant monitoring of threats, including terrorist threats. For example, one Jewish studies organization form the USA uses Social Links for this exact purpose. They fear attacks or incidents during their events, so they perform such monitoring in order to prevent them.

A whole other group of goals is reached through OSINT: risk assessment, when information is collected in order to make a decision [10]. Due diligence procedure can be performed by a bank or by a consulting company, when the main goal is to run a complex assessment of the asset value. In such cases reputation, connections and beneficiaries' financial position matter.

Such check-ups, as so as affiliation search between employees and contractors, have been performed as far as business goes [8]. The matter is - how fast and how efficient, and how precise they may be. Internet, especially social media, gives us huge volume of data for analysis, but collecting data by hand would be too difficult, too long and too inefficient.

The main bonus of the OSINT tools is possibility to find and check all the necessary information with software. For example, a Social Links product requires one hour to gather such an amount of data from open sources, which a skilled worker would collect by hand in a week.

With Social Links you can mine data from 50+ socials, databases and use 700+ search methods empowered with Face Recognition and search by Geo-coordinates [13]. You will get unique searches in 30+ DarkNet forums and marketplaces without authorization by Phrase, PGP Key, Alias, also, you can get analytics by Products and Locations (shipping from/to).

Small businesses also arguably have the most to lose from being hit with a damaging cyber-attack. A recent report revealed that businesses with less than 500 employees lose on average $2.5 million per attack. Losing this amount of money in a cyber breach is devastating to small businesses, and that's not to mention the reputational damage that comes from being hit by a cyber-attack.

For these reasons, small businesses need to be aware of the threats and how to stop them. This article will cover the top 5 security threats facing businesses, and how organizations can protect themselves against them.[14]

1) Phishing Attacks

The biggest, most damaging and most widespread threat facing small businesses are phishing attacks. Phishing accounts for 90% of all breaches that organizations face, they've grown 65% over the last year, and they account for over $12 billion in business losses. Phishing attacks occur when an attacker pretends to be a trusted contact, and entices a user to click a malicious link, download a malicious file, or give them access to sensitive information, account details or credentials.

2) Malware Attacks

Malware is the second big threat facing small businesses. It encompasses a variety of cyber threats such as trojans and viruses. It's a varied term for malicious code that hackers create to gain access to networks, steal data, or destroy data on computers. Malware usually comes from malicious website downloads, spam emails or from connecting to other infected machines or devices.[15]

3) Ransomware

Ransomware is one of the most common cyber-attacks, hitting thousands of businesses every year. They've grown more common recently, as they are one of the most lucrative forms of attacks. Ransomware involves encrypting company data so that it cannot be used or accessed, and then forcing the company to pay a ransom to unlock the data. This leaves businesses with a tough choice – to pay the ransom and potentially lose huge sums of money, or cripple their services with a loss of data [16].

4) Weak Passwords

Another big threat facing small businesses is employees using weak or easily guessed passwords. Many small businesses use multiple cloud based services, that require different accounts. These services often can contain sensitive data and financial information. Using easily guessed passwords, or using the same passwords for multiple accounts, can cause this data to become compromised.

5) Insider Threats

The final major threat facing small businesses is the insider threat. An insider threat is a risk to an organization that is caused by the actions of employees, former employees, business contractors or associates. These actors can access critical data about your company, and they can case harmful effects through greed or malice, or simply through ignorance and carelessness. A 2017 Verizon report found that 25% of breaches in 2017 were caused by insider threats. [17]

This is a growing problem and can put employees and customers at risk, or cause the company financial damage. Within small businesses, insider threats are growing as more employees have access to multiple accounts, that hold more data. Research has found that 62% of employees have reported having access to accounts that they probably didn't need to [18].

Conclusion

There are a range of threats facing small businesses at the moment. The best way for businesses to protect against these threats is to have a comprehensive set of security tools in place, and to utilize Security Awareness Training to ensure that users are aware of security threats and how to prevent them.

REFERENCES

1. McLaughlin, Michael (June 2012). "Using open source intelligence [https://www.usersearch.org software] for cybersecurity intelligence". ComputerWeekly.com. Archived from the original on 2018-06-29.
2. The US Intelligence Community. ASIN 0813349184.
3. Gagnidze, M. Iavich, G. Iashvili, Some Aspects of Post-Quantum Cryptosystems, Abstract book, EURO-ASIA FORUM IN POLITICS ECONOMICS AND BUSINESS – 2016, JULY 21-22, 2016, BELGRADE, SERBIA.
4. "Spy Agencies Turn to Newspapers, NPR, and Wikipedia for Information: The intelligence community is learning to value 'open-source' information". Archived from the original on 2012-04-07. Retrieved 2008-09-15.
5. "As defined in Sec. 931 of Public Law 109-163, entitled, "National Defense Authorization Act for Fiscal Year 2006."". Archived from the original on 2008-11-12.
6. Richelson, Jeffrey T (2015-07-14). The U.S. Intelligence Community. Avalon Publishing. ISBN 9780813349190. Retrieved 15 May 2017.
7. George, edited by Roger Z; Kline, Robert D; Lownethal, Mark M (2005). Intelligence and the national security strategist: enduring issues and challenges. Lanham: Rowman and Littlefield. ISBN 9780742540392.

8. Bornn, D Marshall (9 Jan 2013). "Service members, civilians learn to harness power of 'Open Source' information". www.army.mil. Archived from the original on 9 December 2017.
9. Lowenthal, Mark; Clark, Robert (2015). The Five Disciplines of Intelligence Collection. CQ Press. p. 18.
10. (The Commission on the Intelligence Capabilities). Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction
11. "Reexamining the Distinction Between Open Information and Secrets – Central Intelligence Agency". www.cia.gov. Archived from the original on 2018-06-08. Retrieved 2018-06-29.
12. Hudnall, Ken (2011). "Intelligence Failures". No Safe Haven: Homeland Insecurity. Grave Distractions Publications. ISBN 9781452493923.
13. Kozlenko, M., Lazarovych, I., Tkachuk, V., Vialkova, V. Software Demodulation of Weak Radio Signals using Convolutional Neural Network
    2020 IEEE 7th International Conference on Energy Smart Systems, ESS 2020 - Proceedings, 2020, pp. 339–342
14. Zhengbing Hu, Sergiy Gnatyuk, Tetiana Okhrimenko, Sakhybay Tynymbayev, Maksim Iavich, "High-Speed and Secure PRNG for Cryptographic Applications", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.3, pp.1-10, 2020. DOI: 10.5815/ijcnis.2020.03.01
15. Zh. Hu, V. Kinzeryavyy, M. Iavich et al., "High-Speed Privacy Amplification Method for Deterministic Quantum Cryptography Protocols Using Pairs of Entangled Qutrits", CEUR Workshop Proceedings, vol. 2393, pp. 810-821.
16. Hubskyi, O., Babenko, T., Myrutenko, L., Oksiiuk, O. Detection of sql injection attack using neural networks //Advances in Intelligent Systems and Computing, 2021, 1265 AISC, pp. 277–286
17. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019
18. Kovalova, Y., Babenko, T., Oksiiuk, O., Myrutenko, L. OPTIMIZATION OF LIFETIME IN WIRELESS MONITORING NETWORKS//International Journal of Computing, 2020, 19(2), pp. 267–272

Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 40-48 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

VIRTUAL ASSISTANTS & ARTIFICIAL INTELLIGENCE: TRANSFORMING DIGITAL CENSORSHIP

Yasir Nawaz Shaikh, Cybersecurity, Artificial Intelligence,Organization: PureVPN, Digital Content Producer, Karachi, Pakistan

ABSTRACT

Artificial Intelligence continues to break new barriers each day. Thanks to AI, it is not inconceivable to believe that we may rely even less on actual physical labor than we do now. One such example of virtual assistants such as Alexa, Siri, Google Assistant, Cortana, Bixby, and many more. While currently, they are glorified tools on our smartphones for voice commands, they are quickly being programmed to be the perfect assistant suited for our daily tasks. While that sounds great, it comes with a threat that may not be immediate, but it is only a matter of time until it does; censorship.

This study triangulates the opinion of renowned authors and researchers within the field of Artificial Intelligence to get an idea of what the future holds for censorship online in an era when artificial intelligence-backed assistants are the primary customers toggling through the visible search results, and humans rely on them for their effectiveness and efficiency. The results indicate a need for brands to rethink how they inform their customers, the importance of brand recognition and loyalty in the era ahead and a much better-informed public that does not solely rely on the search results provided to it via these assistants.

KEYWORDS: *Cybersecurity, Artificial Intelligence, Digital Censorship, Virtual Assistants*

Rubrics: Cyber hygiene, cybercrime, information warfare.

Introduction

"AI will overtake humans within the next 100 years. When that happens, we need to make sure the computers have goals aligned with ours" – Stephen Hawking (Matyszczyk, 2015)

Not only did Hawking's prediction come to fruition, but it came a lot sooner than even he may have anticipated. Machines and artificial Intelligence have begun substituting humans in areas that were previously considered impossible (Paulo, 2019). While some might point to the doom and gloom aspect of such wide-scale automation, there is an undeniably enormous amount of potential (Chui, et al., 2016). Nothing will be spared of the effects of Artificial Intelligence becoming more potent, that includes marketers (Talbot, 2019).

Arguably no other facet of modern technology represents AI in its most human-interactive form than virtual assistants. After all, it is an interface designed to "have all the perfections of human interactions and none

of the flaws" (Joshi, 2018). Allowing people to designate mundane tasks, receive timely updates on their billing information, crack a joke or two, and reorganizing the way it interacts based on learning patterns displayed by the users (Jurowiec, 2018).

The rising popularity of voice assistants such as Alexa, Cortana, and Google Assistant has made it easier for users to interact with the Internet (Cheyer et al., 2014). Simultaneously, it has managed to revolutionize the concept of multi-tasking. Forget "just a click away," now whatever you need is a "sentence away" (Guzman, 2019).

However, that has given rise to another question, frequently asked and discussed in both journalistic and academic circles, i.e., what intelligent AI designs mean for online censorship (Black & Fullerton, 2020). Of course, popular culture is filled with anecdotes and references to how an all-knowing AI could become self-aware and proceed to perceive humans as an enemy (Henry, 2020). Nevertheless, in more realistic terms, there is a surprising lack of research about the future iterations of Alexa and Google Assistant means for our access to information.

A more frequently touted scenario is what if humans were to become entirely dependent on these assistants for their daily news. Furthermore, under government regulations, what if these AIs were to omit certain pieces of information (Feldstein, 2019). In a genuinely Orwellian sense, we would not even know what we are not being told since we would not know there is something to miss out on. One might argue that this is an incredible stretch of the imagination, but one must also wonder, "Is it beyond plausible possibility?".

Simultaneously, it is considered inevitable that sooner or later, these virtual assistants will become the prima facto customers online as human activity online becomes increasingly automated (PwC, 2018). Human decisions might be eliminated, or at the very least, severely limited. The information available online will reflect that. We have already begun seeing such technology in its infancy on social media apps like Twitter and Facebook, where each news article is first vetted by bots and then presented to the viewer, with an accompanying fact-check message (Ding, 2018). As mentioned earlier, government regulations in the future could mean that this news vetting process could be taken to the next step. That next step could be draconian, considering the state of modern censorship practiced in modern dictatorships (Mchangama & Fiss, 2019).

Literature Review

Human-Machine Interaction

The prominence that virtual assistants have gained in the past few years falls in line with the guiding principles of AI innovation (Martinez-Lopez & Casillas, 2013). While companies have long foreseen the

looming reality that increased automation will present, there has been ambiguity in maximizing the potential opportunities it will present (Siau & Yang, 2017).

The primary reason for this has been the lack of foresight. That AI is the future has long been an accepted datum within the corporate world. The problem is, how does that future look like? As (Sterne, 2017) states, once technological innovations take a firm grip in terms of societal presence, it can take on a life of their own.

In other words, brands might have specific strategic objectives and tactics for virtual assistants in mind today based on how they exist today. Those strategies and tactics may become obsolete within a few years, depending on the direction virtual assistants take (Hoc, et al., 2013). These strategies and tactics might very well take on a more aggressive look once government agencies adopt them.

There is a flip side to the ease of inducing increased AI presence in our lives. Through various legislation, governments can create a back-channel in all these virtual assistants. There have been modern instances of mass-scale surveillance. Virtual assistants would make censorship far easier since there will be an active actor within our households that could be used. Such an act's legality would be debated, but one cannot remain optimistic if past examples are to go by.

Censorship in the Digital Age

New leaps in technology always promise a more effortless flow of information. The advent of the Internet meant that information could be communicated far easier and more accurately than ever. Subsequently, emails, multimedia options, and lastly, social media meant that information travels almost instantaneously. However, just because technology promises something does not always translate into practice. Governments, mainly, repressive ones have always held a penchant for stifling any such easy flow of information (Tenczer, et al., 2016).

They will undoubtedly welcome any tool that aids their efforts in restricting information they might be dangerous. These governments might welcome such developments since dissenters have begun evolving their methods (Shiwen & Mai, 2019). Unlike the past, where silencing journalists and provocateurs meant effective control of information, the digital age has transformed anyone with a smartphone into a conduit for information (Nadaf, 2020).

In such a scenario, a virtual assistant could be weaponized against the proliferation of such information deemed dangerous. We have seen how tech giants like Facebook and Google have had to bow down to demands by repressive governments worldwide (Coskuntuncel, 2018). Such past precedence begs the

question of how Orwellian virtual assistants in every house might be. In an age where virtual assistants are the primary source of information, if the assistants could be programmed to restrict their users' access to specific content, they might not even realize that they are being denied information (Qiang, 2019). 2+2 would become 5 since the user would not know how addition works. Hence, they would be unable to raise objections to the results being shown to them.

VPNs in the Age of Alexa

Virtual Private Networks (VPN) have been an essential asset available to dissenters by far when it comes to circumventing the restrictions imposed on them by repressive governments. (Peterescu & Krishen, 2020). Journalists, whistleblowers, and activists have relied on the tool to help them retain access to the Internet even when widespread restrictions have been imposed in their countries (Ververis, et al., 2019).

VPNs have retained their popularity since they are easy to set up and inexpensive. The paid ones provide better features and a far more secure sense of anonymity online, but the free services are good enough to unblock blocked content (Lilkov, 2020). However, that entire paradigm is likely to go a complete upheaval in the age of virtual assistants like Alexa (Perry & Roda, 2017). For instance, VPNs are already criminalized in several countries. However, no mechanism allows governments to restrict users from downloading the service (Khan, et al., 2018). Several VPNs usually set up mirror sites that allow users to easily download the service from within those countries even if the original website is banned (Hobbs & Roberts, 2018).

Enter the virtual assistant. Since the virtual assistants are the primary customer, governments could program them to ensure that users could not download the service via their internet connections (Wang, et al., 2020). Moreover, even if somehow users could install VPNs, these virtual assistants could alert the government agencies that such an app was detected on the user's device (Black & Fullerton, 2020). This might all be conjecture and speculation at this point, but since this study follows a secondary research model, past research indicates that governments have employed agents within populations to spy on their citizens' activities. There is no reason to believe that given the capability, governments would not, or at least would not attempt to carry out such protocols (Kaylee, 2020).

Research Question

How will VPNs adapt to the age of virtual assistants and ensure seamless accessibility to users in the most vulnerable countries?

Despite their obvious uses, will virtual assistants become government surveillance tools inside every house they are in?

Methodology

Since this study aims to study the potential effects of what the progress in virtual assistants and AI means for digital censorship, the primary source of data to be studied will be secondary. This means that this project will build on the work already done by researchers and past studies.

Initially, a thorough analysis of the secondary data available will be conducted. This would include a more exhaustive and extensive study of the literature that already exists on topics that lie on the fringes of the problems that this study hopes to address. The study of peer-reviewed literature will enable us to understand the academic discourse on the subject (Callaham, et al., 2002).

Since virtual assistants are a relatively new concept, it is necessary to understand the psychological motivations behind how government agencies could use them to censor information online.

In the end, data collected from up to 5-10 studies will be used to support arguments for what lies ahead in terms of censorship (Strauss, 1987). Since the purpose of this study is to triangulate the relationship between the rise in AI, its censorship potential in the hands of governments, and how VPNs will evolve in the light of those, the studies will be varied to cover all three subjects adequately (Maxwell, 2008).

Nature of Research

The nature of this research will be in interpretivist terms. Such an approach would allow the researcher to integrate the contrasting nature of the data gathered via different past studies and cases studied.

Findings

Since this paper follows a secondary form of research in an area that is still in its relative infancy, the ideas discussed continually undergo changes. However, all the resources used in this study illustrate a standard agreement on the one fundamental assertion; the relationship between humans and the Internet will change. This will undoubtedly be further exacerbated by the consistent improvement in how Artificial Intelligence, specifically virtual assistants, understand the Internet.

Aggravated Control:

It seems as if the writing is on the wall in terms of virtual assistants becoming increasingly popular. Like with invention in the internet age, virtual assistants will change the entire way humans interact. For instance, Stuard Russell and Peter Norvig state in Artificial Intelligence: A Modern Approach that these virtual assistants' sheer capabilities mean that humans will be unlikely to refuse to let them take over. If a human were to look over the Internet for a particular brand of shoes available at the lowest price, a virtual assistant could easily outperform and out search any human in a significantly less amount of time. Through the virtue

of pattern studies and previous search patterns, there may even come a time when these virtual assistants could easily predict exactly which criteria to use when searching for specific products.

Need To Reinvent

This is where ethical dilemmas truly start emerging. Alec Ross argues in his The Industries Of The Future that the very idea of privacy will come under attack in the age of virtual assistants. The book carefully investigates how, despite the ease of use they offer, it comes with several trade-offs. Moreover, we still do not know how severe or impactful these trade-offs can be in the long-run. For instance, in a future where virtual assistants are essentially the primary customers (Considering they are the ones that make the actual searches on Google through voice commands), it is the virtual assistant looking at the SERPs. At this point, the full potential of AI will come into place as these virtual assistants can easily comb through websites that use SEO black hat techniques to climb up the search results without offering the best product in return. If this is how it plays out, this essentially means two things. One, digital marketers will need to rethink their approach towards building their brand entirely. The current modus operandi of offering a value proposition often elicit an emotional response from the user. This will be absent entirely when it comes to AI-powered virtual assistants doing those searches for us.

Similarly, it gives most government agencies an unprecedented opportunity to control the way their citizens behave online. There is little or no government regulation directly dealing with these virtual assistants, but that is likely to change in the future. If, at any point, these were to be programmed to comply with government regulations, they could easily be used to filter out and censor search results a government does not want visible to its citizens. Furthermore, if humans are not the ones looking at the SERPs, they may not even know the results are being censored in the first place. Regarding VPNs, if a government were to ban VPNs, the virtual assistants would omit any relevant SERPs to them completely. A more infant form of similar censorship is already a staple of the Great Firewall of China, where most VPN providers are not allowed to operate and are entirely opaque to a significant part of the population. AI-powered censorship could multiply that manifolds.

Discussion

This paper deals with two essential questions: VPNs' future in an artificial intelligence-reliant world and whether it is headed towards obscurity in front of government regulation. Most of the current literature suggests that it is likely that governments are trying to pressurize VPNs to operate, with a catch, sharing complete activity logs. Complete bans have been enforced in the past, and they do remain in effect in several countries around the world. However, that does nothing to discourage users eager to use a VPN from simply

choosing the next available VPN service. By giving this small leeway, governments may end up gaining the amount of informational control since all VPNs will be required to provide logs. Considering how the general populace remains mostly unaware of how much data is being collected about them, it is not far-fetched to imagine them signing up for these services without reading the fine print.

This brings us back to the initial question; is that the future of VPNs? Government-mandated, in other words, government oversight. It does not have to be that way, but that would depend on more than one factor. Current research, as well as market incentive, lacks substantial study of such a scenario. However, the onus will fall on the developing end of these VPN providers to address these concerns. It would have to start with how they would deal with voice commands and voice searches in particular regions. Governments cannot control how a private business operates, but it can affect those options' visibility to potential customers. Since the projections indicate that most online searches will shift to voice searches, it will not be the humans making the best decision for themselves. Humans will probably not even be exposed to the SERPs. Hence, it would be worthwhile for VPN providers to start planning how to target and maximize their visibility to users through these voice assistants. More importantly, how they would evade restrictions by governments on these SERPs.

REFERENCES

1. Akgun, Ali Ekber, Ipek Kocoglu, and Salih Imamoglu. 2013. "An emerging consumer experience: Emotional branding." Procedia-Social and Behavioral Sciences 99: 503-508.
2. Ana, Canhoto Isabel, and Yuvraj Padmanabhan. 2015. "We (don't) know how you feel'– a comparative study of automated vs. manual analysis of social media conversations." Journal of Marketing Management 31 (9-10): 1141-1157.
3. Anand, Priya. 2018. The Reality Behind Voice Shopping Hype. Accessed October 11, 2019. https://www.theinformation.com/articles/the-reality-behind-voice-shopping-hype.
4. Barrett, Lisa Feldman, Ralph Adolphs, Stacy Marsella, Aleix Martinez, and Seth Pollak. 2019. "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements." Psychological Science in the Public Interest 20 (1): 1-68.
5. Basch, Charles. 1987. "Focus group interview: An underutilized research technique for improving theory and practice in health education." Health education quarterly 14 (4): 411-448.
6. Bazeley, Patricia, and Kristi Jackson. 2013. Qualitative data analysis with NVivo. Sage Publications Limited.
7. Biernacki, Patrick, and Dan Waldorf. 1981. "Snowball sampling: Problems and techniques of chain referral sampling." Sociological methods & research 141-163.
8. Biernacki, Patrick, and Dan Waldorf. 1981. "Snowball sampling: Problems and techniques of chain referral sampling." Sociological methods & research 10 (2): 141-163.

9. Black, Joanna, and Cody Fullerton. 2020. "Digital Deceit: Fake News, Artificial Intelligence, and Censorship in Educational Research." Open Journal of Social Sciences 8 (07): 71.
10. Black, Joanna, and Cody Fullerton. 2020. "Digital Deceit: Fake News, Artificial Intelligence, and Censorship in Educational Research." Open Journal of Social Sciences 8 (7): 71.
11. Bolls, Paul, and Darrel Muehling. 2007. "The effects of dual-task processing on consumers' responses to high-and low-imagery radio advertisements." Journal of Advertising 4 (36): 35-47.
12. Bonnington, Christina. 2018. What It Would Mean for Amazon to Bring Ads to Alexa. Accessed October 19, 2019. https://slate.com/technology/2018/01/amazon-echo-getting-ads-as-company-finds-promotional-partners-for-alexa.html.
13. Brooke, Sophia. 2019. Why AI for Logo Detection Is the Next Marketing Must-Have. Accessed September 22, 2019. https://blog.markgrowth.com/why-ai-for-logo-detection-is-the-next-marketing-must-have-e57a195a730a.
14. Brooks, Joanna, Serena McCluskey, Emma Turley, and Nigel King. 2015. "The utility of template analysis in qualitative psychology research." Qualitative Research in Psychology 2 (12): 202-222.
15. Buckley, Ralf. 2016. "Aww: The emotion of perceiving cuteness." Frontiers in psychology 7 (1740).
16. Calisir, Fethi, and Demet Karaali. 2008. "The impacts of banner location, banner content and navigation style on banner recognition." Computers in Human Behaviour 2 (24): 535-543.
17. Callaham, Michael, Robert L Wears, and Ellen Weber. 2002. "Journal prestige, publication bias, and other characteristics associated with citation of published studies in peer-reviewed journals." Jama 287 (21): 2847-2850.
18. Carrier, Mark, Nancy Cheever, Larry Rosen, Benitez Sandra, and Jennifer Chang. 2009. "Multitasking across generations: Multitasking choices and difficulty ratings in three generations of Americans." Computers in Human Behavior 2 (25): 483-489.
19. Chang, Yuhmiin, and Esther Thorson. 2004. "Television and web advertising synergies." Journal of Advertising 2 (33): 75-84.
20. Chowdhury, Rafi, Adam Finn, and Douglas Olsen. 2007. "Investigating the simultaneous presentation of advertising and television programming." Journal of Advertising 3 (36): 85-96.
21. Chui, Michael, James Manyika, and Mehdi Miremadi. 2016. Where machines could replace humans—and where they can't (yet). Accessed October 13, 2019. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/where-machines-could-replace-humans-and-where-they-cant-yet.
22. Clabiorne, Alejandro, Chris Stephenson, Craig Atkinson, Karine Courtemanche, Klint Finley, Malcolm Devoy, and Mark Holden. 2015. Sentience: The coming ai revolution and the implications for marketing.

23. Clark, Emily. 2019. Alexa, Are You Listening? How People Use Voice Assistants. Accessed October 26, 2019. https://clutch.co/app-developers/resources/alexa-listening-how-people-use-voice-assistants.
24. Coskuntuncel, Aras. 2018. "Privatization of governance, delegated censorship, and hegemony in the digital era: The case of Turkey." Journalism Studies 19 (5): 690-708.
25. Cüneyt, DIrican. 2015. "The impacts of robotics, artificial intelligence on business and economics." Procedia-Social and Behavioral Sciences 195: 564-573.
26. David, Stewart, and Prem Shamdasani. 2014. Focus groups: Theory and practice. Sage Publications.

Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 49-57 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

RESEARCH OF PROCESSES OCCURRING WITH INFORMATION COUNTER-FIGHTING IN MODERN CONDITIONS

ИССЛЕДОВАНИЕ ПРОЦЕССОВ ПРОИСХОДЯЩИХ ПРИ ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ В СОВРЕМЕННЫХ УСЛОВИЯХ

Volodymyr Khoroshko, National Aviation University, Doctor of Engineering Science, Full Professor, Kiev, Ukraine
Хорошко Владимир Алексеевич, доктор технических наук, профессор, профессор Национального авиационного университета (г. Киев).
Zhukov Anatoly, Zhitomir Military Institute (Zhitomir), Ukraine.
Жуков Анатолий Алексеевич, Житомирский военный институт (г. Житомир), Украина.
Latko Iryna, Zhitomir Military Institute (Zhitomir), Ukraine.
Латко Ирина Игоревна, Житомирский военный институт (г. Житомир), Украина.

ABSTRACT: The information sphere today has become a system-forming factor that has united all spheres of national security - economic, political, social, military, etc. As a result, through the information sphere, new threats to state security are being implemented. Therefore, the study of information security issues is inextricably linked with the study of the processes occurring in the course of information confrontation. Taking into account the antagonism of the interests of the opposing sides, the article proposes a well-known approach for solving the above problem, based on the basic provisions of game theory. In the course of the study, the optimal distribution of the means of defense and attack of the opposing sides was obtained, the basic theorems of information confrontation were formulated, and the gains and losses of each of the parties to the conflict were determined in an analytical form. The results obtained can serve as a mathematical basis for finding strategies for information countermeasures in an aggressive information environment.

АННОТАЦИЯ: Информационная сфера сегодня стала системообразующим фактором, объединившим все без исключения сферы национальной безопасности-экономическую, политическую, социальную, военную и др. Как следствие, через информационную сферу, реализуются новые угрозы безопасности государства. Поэтому изучение вопросов обеспечения информационной безопасности, неразрывно связано с исследованиями процессов происходящих в ходе информационного противоборства. Учитывая антагонизм интересов противоборствующих сторон в статье предложен известный подход для решения вышеизложенной задачи, основывающейся на базовых положениях теории игр. В ходе исследования получены оптимальные распределения средств защиты и нападения противоборствующих сторон, сформулирована базовые теоремы информационного противоборства, а также определены в аналитическом виде выигрыш и проигрыш каждой из сторон конфликта. Полученные результаты могут служить математическим базисом для нахождения стратегий информационного противодействия в условиях агрессивной информационной среды.

KEYWORDS*: cyberspace, cyber war, countering hybrid war, information space, analysis of the processes of attack and counteraction in the information space, game theory.*
КЛЮЧЕВЫЕ СЛОВА: *киберпространство, кибервойна, противодействия гибридной войне, информационное пространство, анализа процессов нападения и противодействия в информационном пространстве, теория игр.*

ВВЕДЕНИЕ

Информационная сфера стала сегодня базой для развития всех других сфер: экономической, политической, военной, дипломатической и т.д.

В информационной сфере Украины происходят различные события и явления, изучение и анализ которых становятся жизненно необходимыми для любого субъекта [1, 2].

Информационное противоборство не является детищем сегодняшнего дня. Многие его приемы возникли тысячи лет назад вместе с появлением информационных систем. История обучения человечества – это и есть своего рода противоборство.

Очень точно суть информационного противоборства и войны выражены в наставлениях древнекитайского военного деятеля Сунь Цзы [3, 4].

Следует отметить, что по интенсивности, масштабам и средствам, которые используются, необходимо выделить следующие его виды (формы) [4]: информационная экспансия, информационная агрессия и информационная война.

Таким образом, арсенал информационного противодействия совершенствовался на протяжении веков и на начало XXI века состоит из средств и приемов информационной борьбы, более результативных, чем у обычной войны, т.е. вооруженного конфликта. Информационные технологии и современные условия играют роль информационного оружия при реализации стратегии соперничества – информационного противоборства.

Специалистами информационное противоборство рассматривается как самое эффективное средство для достижения и обеспечения различных целей и интересов [5]. В отличие от других форм и способов противоборства, информационная борьба ведется постоянно как в мирное, так и в военное время и воздействует почти на все жизненно важные сферы деятельности страны-противника, а также на мировое информационное пространство [6].

Теоретической основой исследования информационного противоборства или конфликтных ситуаций может стать теория игр [7], широкому распространению которой в последнее время способствует как применение средств вычислительной техники, так и создание аналитического аппарата, позволяющего находить формульные решения для поставленных задач [8].

Для того, чтобы дать формальное математическое определение игры (противостояния) [9], необходимо учесть следующие четыре фактора.

Во-первых, важно понимать то, что в конфликте участвуют те или иные стороны, которые являются субъектами, принимающими решения. Эти стороны называются коалициями и обозначаются *J*.

Во-вторых, необходимо учесть возможности участников конфликта, т.е. указать, какие именно решения может принять каждая из коалиций действия $i \epsilon I$. Эти решения называются стратегиями коалиций i. Множество всех стратегий коалиций действия и будем обозначать через X_i. Между стратегиями различных коалиций действия может иметь место та или иная связь. Результат выбора всех таких связей и ограничений называется ситуацией. Таким образом, множество всех ситуаций можно понимать как некоторое заданное подмножество Z декартового произведения

$$\prod_{i \epsilon I} X_{i.}$$

В-третьих, необходимо определить стороны, отстаивающие некоторые интересы.

Их называют коалициями интересов. Как и коалиции действий, коалиции интересов являются в общем случае коллективами. Различные коалиции интересов могут пересекаться, и, более того, один такой коллектив может содержаться в другом. Множество всех коалиций интересов обозначается через U.

В-четвертых, необходимо описать интересы (т.е. цели) участников конфликта. Это значит, что для каждой коалиции интересов $j \epsilon U$ на множество ситуаций Z должны быть указано бинарное отношение предпочтения $> j$.

Таким образом, сказанное позволяет сформулировать общее определение игры на математической модели конфликта.

То есть игрой (противостоянием) называется система

$$G = \langle J, \{X_i\} i \epsilon j, Z, U, \{>_j\} i \epsilon j \rangle, \quad (1)$$

где $J, X_i, (i \epsilon j)$ и $U-$ произвольные множества,

$$Z \subset \prod_{i \epsilon J} X_i$$

а $>_j$ $(i \epsilon j)$ –произвольные бинарные отношения на Z.

Стоящая в правой части (1) система, определяющая противостояние G, является формальным обозначением того, что обычно принято называть условиями противостояния (игры).

В дальнейшем, считая $J = U$, бинарное отношение предпочтения $>_j$ определим следующим образом. Введем для каждого $j \epsilon U$ на множестве всех ситуаций Z принимающую вещественные значения функцию $M_j(z)$. Эта функция служит показателем успеха коалиции интересов j в ситуации z∈Z и называется функцией выигрыша (победы) коалиции интересов j. Поэтому будем считать, что $z' >_j Z''$ для $j \epsilon U$,
если $M_j(z') > M_j(z'')$.

ЦЕЛЬ СТАТЬИ

Целью статьи является применение теории игр для исследования и решения задач в информационной сфере, возникающих в результате информационного противоборства.

ОСНОВНОЙ РЕЗУЛЬТАТ

Основной теоремой теории игр является теорема о равенстве максимина и минимакса, впервые сформулированная и введенная Джоном фон Нейманом [4]. Она устанавливает условия существования оптимальных стратегий и цены игры или противодействия.

Для прямоугольных игр вопрос существования решения игры представлен следующей теоремой [4].

Теорема 1. Пусть

$$A = \begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{\mathrm{n}m} \end{Vmatrix}$$

– платежная матрица; $X = \|x_1, x_2, \dots, x_n\|$ и $Y = \|y_1, y_2, \dots, y_m\|$– смешанные стратегии игроков или сторон $C1$ и $C2$. Соответственно, математическое определение выигрыша игрока или стороны $C1$ определено следующим образом:

$$C(X,Y) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij}\, x_i x_j,$$

тогда величины $\max\limits_{X \epsilon S_n} \min\limits_{Y \epsilon S_m} C(X,Y)$ и $\max\limits_{Y \epsilon S_m} \min\limits_{X \epsilon S_n} C(X,Y)$ существуют и равны между собой.

Для непрерывных игр это теорема формулируется следующими образом [4, 5].

Теорема 2. Если M(x,y) есть непрерывной функцией двух переменных в замкнутом единичном квадрате, то величины

$$\max_{F \epsilon D} \min_{G \epsilon D} \int_0^1 \int_0^1 M(x,y)\, dF(x)\, dG(y), \tag{2}$$

$$\min_{G\in D}\ \max_{F\in D}\int_0^1\int_0^1 M(x,y)dF(x)dG(y) \tag{3}$$

существуют и равны между собой.

Доказательству этой теоремы при различных предположениях относительно функции выигрыша и пространств стратегий игроков были посвящены многие работы [4– 6].

Несмотря на то, что теорема фон Неймана и другие обобщающие ее теоремы убеждают в существовании цены и оптимальных стратегий для некоторых классов игр, они не дают никакого метода для нахождения решений любой конкретной игры. Ценность этих теорем заключается в том, что они устанавливают классы функций выигрыша, для которых решения игр существуют.

Типичной задачей исследования поведения противоборствующих сторон является оптимальное распределение средств нападения и защиты. Некоторые простейшие случаи были рассмотрены в [7], а более общие ситуации – в работах [4, 5, 8, 9].

Пусть имеются две стороны с антагонистическими интересами: сторона *C*1 стремится разрушить государственную систему и захватить сторону *C*2 с помощью имеющихся у неё сил и средств, а сторона *C*2 обороняется. Атакующие средства стороны *C*1 состоят из *S*1 типов, причем в некоторых условных единицах количество средств m-го типа равно a_m, так что суммарный поступательный потенциал стороны *C*1 составляет величину

$$\sum_{m=1}^{S_1} a_m = M_1.$$

.

Аналогично оборонительные средства стороны *C*2 подразделяются на *S*2 типов, причем количество средств *j*-го типа в условных единицах равно, а суммарный оборонительный потенциал стороны *C*2 составляет величину $\sum_{j=1}^{S^2} dj = M^2$.

Сторона *C*2 имеет *n* жизненно важных объектов (население, промышленность, экономику и т.д.) B_1, B_2, …, B_n причем объект B_1 оценивается некоторой условной величиной γ_i. Пусть также объекты B_1, B_2, …, B_n упорядочены по их ценности, т.е. $\gamma_{1\geq}\gamma_{2\geq}\gamma_{3\geq}\ldots\ {}_{\geq}\gamma_n$.

Предположим, что каждый незащищенный объект $B_{i(i=1,2,\ldots,n)}$ в результате атаки на него одной наступательной единицы *m*-го типа подвергнут разрушению или воздействиюе, ущерб от которых для *C*2 оценивается величиной $\gamma_i\,\varepsilon_m$. Величину воздействий при наличии наступательных и оборонительных средств будем считать пропорциональной разности их суммарных количеств, если эта разность положительна или равна нулю в противном случае.

Поведение сторон *C*1 и *C*2 определяется распределениями средств нападения и защиты.

Пусть сторона *C*1 для атак на объекты B_1 выделяет σ_{im} наступательных средств *m*-го типа, а сторона *C*2 для защиты и противодействие атаке на этом объекте выделяется μ_{ij} оборонительных средств *j*-го типа. При этом в отражении наступательных средств *m*-го типа принимает участие лишь λ_{mj} часть защитных средств *j*-го типа. Следовательно, распределение средств обороны можно описать матрицей

$$\bigwedge = \|\lambda_{\mathrm{mj}}\|,$$

где $0\leq \lambda_{mj} \leq 1$ $(1 \leq j \leq S_2, 1 \leq m \leq S_1)$, $\sum_{m=1}^{S_1}\lambda_{mj} = 1$.

Принимая величину результатов атаки на сторону *C*2, производимых воздействий наступательными средствами стороной *C*1, в качестве основной характеристики конфликта, получаем следующие выражения для суммарных потерь стороной *C*2:

$$M(\sigma,\mu) = \sum_{i=1}^{n}\gamma_i \max\left\{0, \sum_{m=1}^{S_1}\varepsilon_m\left(\sigma_{im} - \sum_{j=1}^{S_2}\lambda_{mj}\,\mu_{ij}\right)\right\}. \tag{4}$$

Сторона *C*2 своим поведением стремиться уменьшить величину суммарных воздействий, производимых наступательными средствами системы *C*1. Цель системы *C*1 противоположна. Поэтому функция (4) может быть принята в качестве платежа системы С2 системе *C*1, таким образом, получаем антагонистическую игру с функцией победы (выигрыша) (4). Функция (4) выпукла по μ при любом фиксированном σ.

Теорема3. Пусть *M*(*x,y*) – непрерывная по двум переменным функция победы (выигрыша) антагонистической игры, строго выпуклая по *y* для каждого *x* и имеющая в единичном интервале конечную первую производную по *y*. Тогда имеется единственная оптимальная стратегия для стороны *C*2, являющаяся ступенчатой функцией $I_{y_0}(y)$, причем константа y_0 – единственное решение уравнения

$$\max_{0\le x\le 1} M(x, y_0) = \upsilon,$$

а цена игры υ определяется формулой

$$\upsilon = \min_{0\le y\le 1} \max_{0\le x\le 1} M(x, y).$$

То есть с учетом теоремы 3 получаем замечание 1.

Замечание 1. В теореме 2 требования, положенные на функцию *M(x,y*) можно несколько ослабить.

1. Можно опустить условие существования производных. Но в этом случае нужно предполагать, что функция *M (x,y)* имеет обе односторонние производные в каждой точке интервала определения функции, за исключением, быть может, конечного числа точек. Тогда условия, наложенные на $M'x(x_{0,}y_1)$, $M'x(x_{0,}y_2)$, $M'y(x_{1,}y_0)$ и $M'y(x_{2,}y_0)$,соответствует условиям для односторонних производных в указанных точках.

2. Условие строгой выпуклости или строгой выгнутости функции выигрыша можно ослабить, заменив тем, что она, соответственно, просто выпукла или выгнута. Но в этом случае оптимальная стратегия для второй и первой стороны вообще не является единственной.

Следовательно, на основании теоремы 2 и с учетом замечания 1 сторона *C*2 имеет чистую оптимальную стратегию μ_0, определяемую условием

$$\inf_{\mu} \sup_{\sigma} M(\sigma, \mu) = \sup_{\sigma} M_{i'}(\sigma, \mu) = \Gamma,$$

а сторона *C*1 имеет смешанную оптимальную стратегию *F*(σ)*, представляющую собой определенную выпуклую комбинацию конечного числа чистых стратегий.

Введем обозначения:

$$X_i = \|\sigma_{i1}, \sigma_{i2}, \dots, \sigma_{iS_1}\|,$$
$$Y_i = \|\mu_{i1}, \mu_{i1}, \dots, \mu_{iS_1}\|,$$
$$I_i = \|\gamma_i\varepsilon_1, \gamma_i\varepsilon_2, \dots, \gamma_i\varepsilon_{S_1}\|.$$

Тогда функция (1) может быть записана в матричной форме:

$$\mathrm{M}(\sigma, \mu) = \sum_{l=1}^{n} max\,[0, I'\left(X_i - \bigwedge Y_i\right)], \tag{5}$$

где штрих означает транспортирование.

Там же функция (4) выпуклая по σ при любом фиксированном μ, то при построении оптимальной стратегии стороны *C*1 достаточно использовать рандомизацию лишь среди тех чистых стратегий, которые являются вершинами симплекса:

$$\sigma = \left\{\sigma: \sigma = \sum_{l=1}^{S_1} \delta_i\, a_i, \qquad \delta_i \ge 0, \sum_{i=1}^{S_1} \delta_i = 1\right\}.$$

Если взять во внимания, что функция *M(σ,μ)* выпукла, то σ при любом μ_1 получаем

$$M(\sigma,\mu) = M\left(\sum_{i=1}^{S_1} \delta_i\, a_i\right) \le \sum_{i=1}^{S_1} \delta_i\, M(a_i,\mu).$$

Обозначим через Γ_m часть цены борьбы (игры) Γ, которая может быть получена стороной $C1$ за счет применения атакующих средств m-го типа:

$$\left(\sum_{m=1}^{S_1} \Gamma_m = \Gamma\right), \text{ и } \theta = \left\|a_1, a_2, \dots, a_{S_1}\right\|.$$

Тогда, следуя теореме 2, для определения оптимальной стратегии стороны $C2$ получаем уравнение

$$\bigwedge Y_i - \theta = \Gamma_i, (i = 1,2, \dots, n) \tag{6}$$

Для решения этого матричного уравнения используем обобщенную обратную матрицу, введенную в работе [9]. Обобщенная обратная матрица A^+определяется для любой прямоугольной матрицы А следующими условиями:

$$AA+A=A,$$

$$A+AA^+=A^+,$$

$$(AA^+)^*=AA^+,$$

$$(A+A)^*=A+A$$

где A^* означает сопряженную транспортированную матрицу к матрице A.

В частности, для неособенной квадратной матрицы А таким образом определенная матрица A^+совпадает с обычной обратной матрицей A^{-1}. Из (6) получаем

$$Y_i = \bigwedge^{+} (\theta - \Gamma_i), (1 \le i \le n) \tag{7}$$

где $\bigwedge^+ = \left\|\beta_{ij}\right\|$ – обобщенная обратная матрица для матрицы $\bigwedge$.

Выражение (7) с учетом принятых выше обозначений принимает следующий вид:

$$\mu_{ij} = \sum \left(a_m - \frac{\Gamma_m}{\gamma_i \varepsilon_m}\right) \beta_{jm}\,, \tag{8}$$

где ($1 \le j \le S_2; 1 \le i \le n$).

Предположим, что сторона $C2$ использует свои оборонительные средства j-го типа среди $t(j)$ наиболее важных объектов, т.е.

$$\mu_{t(j)} + 1, j = \mu_{t(j)} + 2, \text{j} = \cdots = \mu_{nj} = 0. \tag{9}$$

Суммируя величины (8) по всем обьектам стороны С2 и учитывая (9), получаем

$$\sum_{i=1}^{t(j)} \mu_{ij} = t(j) \sum_{m=1}^{S_1} a_m\, \beta_{jm} - L_{t(j)} \sum_{m=1}^{S_1} \frac{\Gamma_m}{\varepsilon_m} \beta_{jm}, \tag{10}$$

где $L_{t(j)} = \sum_{i=1}^{t(j)} \frac{1}{\gamma_i}$.

Так как $\sum_{i=1}^{t(j)} \mu_{ij} = d_j$ по предположению, то из (10) имеем

$$\sum_{m=1}^{S_1} \frac{\Gamma_m}{\varepsilon_m} \beta_{jm} = \frac{1}{L_{t(j)}} \left[t(j) \sum_{m=1}^{S_1} a_m \beta_{jm} - d_j \right] \tag{11}$$

Обозначим

$$W = \left\| \frac{\Gamma_1}{\varepsilon_1}, \frac{\Gamma_2}{\varepsilon_2}, \dots, \frac{\Gamma_{S_1}}{\varepsilon_{S_1}} \right\|, R = \left\| \frac{d_1}{t_{(1)}}, \frac{d_2}{t_{(2)}}, \dots, \frac{d_{S_2}}{t_{(S_2)}} \right\|,$$

$$S = \left\| \begin{matrix} \frac{t_1}{L_{t(1)}}, 0, \dots, 0 \\ 0, \frac{t_2}{L_{t(2)}}, \dots, 0 \\ \dots, \dots, \dots, \\ 0, 0, \dots, \frac{t_{(S_2)}}{L_{t(S_2)}} \end{matrix} \right\|.$$

Тогда уравнение (11) можно записать в матричной форме:

$$\bigwedge^{+} W = S\left(\bigwedge^{+} \theta - R \right). \tag{12}$$

Умножив выражение (12) справа на матрицу $\bigwedge$ получаем,

$$\bigwedge \bigwedge^{+} W = W = \bigwedge S \left(\bigwedge^{+} \theta - R \right).$$

Отсюда следует

$$\Gamma_l = \varepsilon_l \sum_{j=1}^{S_2} \frac{\lambda_{\ell j}}{L_{t(j)}} \left[t_{(j)} \sum_{m=1}^{S_1} a_m \beta_{jm} - d_j \right], \tag{13}$$

где ($1 \le \ell \le S_1$).

Сторона $C1$ очевидно поступит оптимально, если будет нападать всеми силами с некоторыми вероятностями ρ_i на $t = \max t^*_{(j)}$ первых наиболее важных объектов системы $C2$, где $t^*_{(j)}$ соответствует максимальному значению цены противоборства:

$$\Gamma = \sum_{\ell=1}^{S_1} \Gamma_\ell = \sum_{\ell=1}^{S_1} \sum_{j=1}^{S_2} \frac{\varepsilon_\ell \lambda_{\ell j}}{L_{t(j)}} \left[t_{(j)} \sum_{m=1}^{S_1} a_m \beta_{jm} - d_j \right]. \tag{14}$$

При этом естественно считать, что математическое определение выигрыша от нападения всеми средствами на каждый из первых t объектов стороны $C2$ не должно зависеть от номера объекта, т.е. $\rho_i \gamma_i$=const.

Учитывая, что $\sum_{l=1}^{t} \rho_i = 1$, получаем

$$\rho_i = \begin{cases} \frac{c}{\gamma_i}, & 1 \le i \le t, \\ 0, & i > t, \end{cases} \tag{15}$$

где $C= \left(\sum_{i=1}^{t} \frac{1}{\gamma_i}\right)^{-1} = \frac{1}{L_t}$.

Таким образом, оптимальные стратегии стороны *C*1 и *C*2 определяются соответственно формулами (8) и (15). Однако при их выводе были допущены некоторые субъективные предположения, исходящие из здравого смысла. Поэтому убедимся в ходе непосредственной проверки, что найденные стратегии действительно являются оптимальными.

Итак, при любой стратегии стороны *C*1 стратегия (8) стороны С2 обеспечивает проигрыш не более величины

$$\gamma_i \sum_{\ell=1}^{S_1} \varepsilon_l \left\{ \sigma_{il} - \sum_{j=1}^{S_2} \left[\sum_{m=1}^{S_1} \left(a_m - \frac{\Gamma_m}{\gamma_i \varepsilon_m} \right) \beta_{jm} \right] \right\} \le$$

$$\le \left\{ \sum_{\ell=1}^{S_1} \varepsilon_l \left[a_l \sum_{j=1}^{S_2} \sum_{m=1}^{S_1} a_m \lambda_{\ell j} \beta_{jm} + \sum_{j=1}^{S_2} \sum_{m=1}^{S_1} \frac{\Gamma_m}{\gamma_i \varepsilon_m} \lambda_{\ell j} \beta_{jm} \right] \right\} =$$

$$= \gamma_i \left\{ \sum_{\ell=1}^{S_1} \varepsilon_l \, a_l - \sum_{\ell=1}^{S_1} \varepsilon_l \, a_l + \sum_{\ell=1}^{S_1} \frac{\Gamma_\ell}{\gamma_i} \right\} = \Gamma.$$

Наоборот, при любой стратегии стороны *C*2 стратегия (15) стороны *C*1 гарантирует ей выигрыш не менее

$$C_1 = \sum_{i=1}^{t} \frac{1}{\gamma_i L_t} \sum_{\ell=1}^{S_1} \varepsilon_{\ell \left[a_l - \sum_{j=1}^{S_2} \lambda_{\ell j} \mu_{ij} \right]} = \frac{t}{L_t} \sum_{\ell=1}^{S_1} \varepsilon_\ell \left[\sum_{j=1}^{S_2} \sum_{m=1}^{S_1} a_m \lambda_{ij} \beta_{jm} \right] -$$

$$- \sum_{i=1}^{t} \frac{1}{L_t} \sum_{\ell=1}^{S_1} \varepsilon_\ell \sum_{j=1}^{S_2} \varepsilon_{\ell j} \, \mu_{ij} \ge$$

$$\ge \sum_{\ell=1}^{S_1} \varepsilon_\ell \sum_{j=1}^{S_2} \left[t(j) \sum_{m=1}^{S_1} a_m \ \lambda_{\ell j} \beta_{jm} \right] \frac{t}{L_{t(j)}} -$$

$$\sum_{\ell=1}^{S_1} \varepsilon_\ell \sum_{j=1}^{S_2} \frac{\lambda_{\ell j} d_j}{L_{t(j)}} = \sum_{\ell=1}^{S_1} \varepsilon_\ell \sum_{j=1}^{S_2} \frac{\lambda_{\ell j}}{L_{t(j)}} * \left[t(j) \sum_{m=1}^{S_1} a_m \beta_{jm} - d_j \right] = \Gamma.$$

Из этих соотношений следует, что справедливы, все вышеуказанные ранее утверждения.

ВЫВОДЫ

Проведенные исследования показали, что применение теории игр позволяет довольно точно оценить сложившуюся конфликтную ситуацию при информационном противоборстве.

Полученные выражения позволяют оценить возможности как нападающей, так и защищающейся сторон в зависимости от выбранной оптимальной стратегии, т.е. предсказать результат осуществляемого информационного противоборства.

СПИСОК ЛИТЕРАТУРЫ

1. Грищук Р. В. Технологічні аспекти інформаційного протиборства на сучасному етапі / Р. В. Грищук, І. О. Канкін, В. В. Охрімчук // Захист інформації. – 2015. – Том 17. – № 1 – С. 80–86.
2. Грищук, Р.В. Проблемні питання створення та використання єдиного інформаційного простору для протистояння зовнішній інформаційній агресії / Р. В. Грищук, І. О. Канкін, Ю. І. Міхєєв // Інформаційна безпека. – 2017. – № 1 (25). – С. 5–9.
3. Сунь Цзы. Трактаты о военном искусстве. –Москва: ООО “Изд-во АСТ”; Санкт-Петербург: Terra fantastica, 2002. 558с.
4. Пирцхалава Л. Г., Хорошко В. А., Хохлачева Ю. Е., Шелест М. Е. Информационное противоборство в современных условиях –Киев: ЦП “Компринт”, 2019. 226с.
5. Грабар І.Г. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир : ЖНАЕУ, 2019. – 280 с.
6 Hryshchuk R. Methodological foundation of State’s information security In social networking services In conditions of hybrid war / R. Hryshchuk, K. Molodetska-Hrynhchuk // Information & Security: An International Journal – 2018. – Vol. 41. – С. 55–73.
7. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Грищук. – Житомир : РУТА, 2010. – 280 с.
8. Хорошко В. Применение теории игр для исследования процессов в информационном противоборстве / В. Хорошко, Р. Грищук, Н. Браиловский, Т. Щербак // Scientific and Practical Cyber Security Journal. – 2020. – № 4 (3). – С. 45–51.
9. Петросян Л. А. , Зенкевич Н. А., Семина Е. А Теория Игр – Москва:Высшая школа, Книжный дом “Университет”, 1998. 304 с.
10. Блекуэлл Д., Гиршин М. Теория игр и статических решений. –Москва:Изд-во “Иностранная лит-ра”, 2008. 360 с.
11. Карлин С. Математические методы в теории игр, программирование и экономика. –Москва: Изд-во “Мир”, 2000. 364с.
12. Воробьев Н. Н., Врублевская И. Н. Позиционные игры. –Москва: Изд-во “Наука”, 1967, 482 с.
13. Дрешер М. Стратегические игры. Теория и приложения –Москва: Изд-во “Советское радио”, 2004. 304 с.
14. Brodheim E., Herzer I., Russ L. A general dynamic model for air defence. url:https://pubsonline.informs.org/doi/abs/10.1287/opre.15.5.779. (дата обращения 10.02.2021).
15. Cohen N.D. An attack-defense game with matrix strategies. url:https://onlinelibrary.wiley.com/doi/abs/10.1002/nav.3800130403.(дата обращения 10.02.2021).

Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 58-66 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

სახელმწიფოს ეკონომიკური პოლიტიკის როლი ეროვნული უსაფრთხოების უზრუნველყოფაში

THE ROLE OF STATE ECONOMIC POLICY IN ENSURING NATIONAL SECURITY

ილია ხუციშვილი, „ნიუ ვიჟენ“ უნივერსიტეტი - სამართლის სკოლის დოქტორანტი

Ilia Khutsishvili, LEPL - Academy Of The Ministry Of Internal Affairs Of Georgia- Master's Academic Degree of Law, New Vision University - The Ph.D Programme in Law, Doctoral Student

ანოტაცია*

საბჭოთა კავშირის დაშლის შემდგომ განვლილ პერიოდში მიმდინარე სიღრმისეული გარდაქმნები საჭიროებენ ადეკვატური მეცნიერული კვლევების გაძლიერებას. ერთ-ერთ მნიშვნელოვან სფეროს ეკონომიკური უსაფრთხოების პრობლემების შესწავლა წარმოადგენს.

ეკონომიკის უსაფრთხო განვითარება სახელმწიფოს ეროვნული უსაფრთხოების უზრუნველყოფის ერთ-ერთი მნიშვნელოვანი წინაპირობაა. ეკონომიკურ უსაფრთხოებას სახელმწიფოთა განვითარების ყველა ეტაპზე ყოველთვის დიდი მნიშვნელობა ჰქონდა და ცივილიზაციის განვითარების სხვადასხვა ეტაპზე სხვადასხვა დატვირთვას იღებდა. ზოგჯერ იგი დაკავ-შირებული იყო ქვეყნის სამხედრო ძლიერებასთან, განვითარებასთან, მოსახლეობის კეთილდღეობასთან, თუმცა მისი მთავარი მიზანი ყოველთვის იქნება სახელმწიფოს ეროვნული უსაფრთხოების უზრუნველყოფა.

სახელმწიფოს წარმატება წარმოუდგენელია სუსტი ეკონომიკის ფონზე. სწორედ აღნიშნული საკითხების განხილვა და გაანალიზებაა საინტერესო, ვინაიდან სადაზვერვო-ოპერაციული ქმედებებით შესაძლებელია ქვეყანის ეკონომიკაზე ზემოქმედება სხვადასხვა ბერკეტით, რაშიც უდიდესი წვლილი სპეცსამსახურების საქმიანობას მიუძღვის.

კვლევის მიზანია, მოხდეს ეკონომიკურ უსაფრთხოებაზე მოქმედი სხვადასხვა დამაზიანებელი საქმიანობის შესწავლა, ანალიზი და კრიტერიუმების დადგენა, თუ რა ინდიკატორები არსებობს რითაც დგინდება სახელმწიფოს ეკონომიკურ უსაფრთხოებაზე დამაზიანებელი ზემოქმედების საფრთხე, რომელიც თავისთავად ხელყოფს სახელმწიფოს ეროვნულ უსაფრთხოებას, ამას შემდგომ მოჰყვება პოლიტიკური დამოუკიდებლობის დაკარგვა და მძიმე შემთხვევაში - ტერიტორიული მთლიანობის დარღვევაც კი.

ABSTRACT

The profound transformations that have taken place since the collapse of the Soviet Union illustrate the need to strengthen adequate scientific research. One of the most important areas is the study of problems of economic security.

*ნაშრომში გამოთქმული მოსაზრებები და დასკვნები ეკუთვნის ავტორს და არ გამოხატავს რომელიმე ორგანიზაციის ან უწყების ოფიციალურ პოზიციას.

Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 58-66 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

The safe development of the economy is one of the most important preconditions for ensuring the national security of the state. Economic security has always been of great importance at all stages of the development of States and has assumed various burdens at different stages of the development of civilization. At times, it was associated with the military power, development, and population welfare, but its main goal will always be to ensure the national security of the state.

A state cannot succeed against the background of a weak economy. It is interesting to discuss and analyze these issues, since intelligence and operational activities can affect the country's economy using various levers, to which the activities of the special services make the greatest contribution.

The purpose of the research is to study, analyze and define criteria for various harmful activities affecting economic security, to identify indicators for determining the threat of adverse impact on the economic security of the state, which in itself undermines the national security of the state resulting in loss of political independence and, in severe cases, even territorial integrity.

KEYWORDS: *safe development,* national security

სახელმწიფოს ეროვნული უსაფრთხოების შემადგენელი ერთ-ერთი სეგმენტი ეკონომიკური უსაფრთხოებაა. მისი უზრუნველყოფა სახელმწიფოსათვის განსაკუთრებულ საზრუნავს წარმოადგენს, ვინაიდან ეკონომიკური უსაფრთხოების სისტემის რღვევა სახელმწიფოში იწვევს სოციალურ-ეკონომიკურ პრობლემებს, რასაც შედეგად მოჰყვება ოპერატიული ვითარების გაუარესება მთელი ქვეყნისა თუ ცალკეული რეგიონების მასშტაბით. აღნიშნული ვითარება კი უცხო ქვეყნის სპეცსამსახურების თავისუფლად მოქმედების ხელსაყრელი გარემოებაა. ამდენად, ეკონომიკურ უსაფრთხოებასთან დაკავშირებული პრობლემების შესწავლაც უდიდესი თეორიული და პრაქტიკული მნიშვნელობისაა.

აღნიშნულიდან გამომდინარე, მეტად აქტუალური ხდება სახელმწიფოს ეკონომიკური უსაფრთხოების უზრუნველყოფის ფაქტორების გამოკვლევა.

სახელმწიფოს არსი, მისი ისტორიული როლი, ამოცანა და დანიშნულება ერთ-ერთი ცენტრალური საკითხია სახელმწიფოს თეორიაში. მისი რაობის გარკვევას ცდილობდნენ ანტიკური პერიოდიდან მოყოლებული, დღემდე. სახელმწიფო ხშირად წარმოადგენს ქვეყნის სინონიმს. სახელმწიფო არის ადამიანების ჯგუფი, რომლებიც მუდმივად ცხოვრობენ ერთ კონკრეტულ ტერიტორიაზე, აქვთ საერთო კანონები, ადათ-წესები, ჰყავთ მთავრობა და შესწევთ უნარი წარმართონ საერთაშორისო ურთიერთობები.

არისტოტელეს განმარტებით, ნებისმიერი სახელმწიფო ერთგვარ კავშირს წარმოადგენს. სახელმწიფო არის ოჯახებისა და გვარების გაერთიანება, შექმნილი იმისათვის, რომ ჰქონდეთ ბედნიერი, სრულყოფილი და თავისუფალი ცხოვრება. არისტოტელე გადამწყვეტ მნიშვნელობას ანიჭებდა პილიტიკურ დამოუკიდებლობას, რომლის გარეშეც სახელმწიფო უბრალოდ ვერ იარსებებს და გაურკვეველ წარმონაქმნად გადაიქცევა.

ცნობილი გერმანელი იურისტის - ჰუფენდორფის განმარტებით კი სახელმწიფო არის რთული მორალური პიროვნება, რომელიც წარმოადგენს თითოეულ პიროვნებას. ეს ყველაფერი წარმოიშობა ხელშეკრულების საფუძველზე, რომლის თანახმადაც, უზრუნველყოფილი უნდა იყოს ადამიანთა თავისუფლება და უსაფრთხოება. სახელმწიფოსა და ადამიანის უფლებების წარმოშობის საფუ-ძვლად იგი მიიჩნევს: საზოგადოებრივ ხელშეკრულებას (pactum) და დამორ-ჩილების შესახებ ხელშეკრულებას (decretum).

პირველი ხელშეკრულებით, ადამიანები ერთიანდებიან დიდ ჯგუფებად საზოგადოების სახით და შემდეგ დებენ მეორე ხელშეკრულებას, რომ იქნებიან მათ მიერ არჩეული ხელისუფლების მორჩილი, ადგენენ პირობებსა და განსაზღვრავენ თითოეულის უფლების ფარგლებს[1]. როგორც ჩანს, სახელმწიფოს ცნების განსაზღვრისას, ყველა ავტორი ასახელებს სახელმწიფოს ძირითად ნიშნად ტერიტორიასა და მოსახლეობას; ეს ბუნებრივიცაა, რადგან სახელმწიფო თავისთავად ვერ იარსებებს აბსტრაქტულად, ტერიტორიისა და მოსახლეობის გარეშე.

ამრიგად, სახელმწიფოს არსებობის ძირითადი ნიშნებია:

- განსაზღვრული ტერიტორიის არსებობა, რომელიც დასახლებულია მოსახლეობით;
- საჯარო ხელისუფლების არსებობა, რომელიც პასუხისმგებელია ქვეყნის მართვაზე;
- სახელმწიფოში გადასახადების სისტემა, რომელიც ხშირ შემთხვევაში მძიმე ტვირთად აწევს მოსახლეობას, თუმცა ყოველთვის აუცილებელია სახელმწიფოს არსებობისათვის.[2]

სახელმწიფო წარმოუდგენელია მოსახლეობის გარეშე, რომელიც აღქმული უნდა იყოს, როგორც სახელმწიფოს ქვაკუთხედი და მისი არარსებობობა მიწის კონკრეტულ ტერიტორიას აქცევდა ყოველგვარი სახელმწიფოებრივი ფორმისა და წარმონაქმნის გარეშე აუთვისებელ ადგილად.

თითოეული ინდივიდი დაკავშირებულია სახლმწიფოსთან სხვადასხვა ფორმით, ესენი არიან ქვეყნის მოქალაქეები, მოქალაქეობის არმქონე თუ სხვა პირები, რომლებიც სახლობენ ერთი რომელიმე კონკრეტული ქვეყნის ტერიტორიაზე და იმყოფებიან ამ სახელმწიფოს სამართლებრივ სივრცეში. სწორედ ინდივიდთა ერთობაა საზოგადოება სახელმწიფოში, ხოლო საზოგადოებას, ე.ი. ერთ დიდ ჯგუფად ნებაყოფლობით გაერთიანებულ ინდივიდებს აქვთ საერთო ინტერესები და ღირებულებები. ისინი ერთმანეთთან სხვადასხვა ფორმით (საერთო შეხედულებები, ღირებულებები, კულტურა, ადათ-წესები, ტრადიციები თუ სხვ.) არიან დაკავშირებული, მათთვის საერთო ნიშანს ერთ სამართლებრივ სივრცეში მოღვაწეობა წარმოადგენს.

არსებობის თვალსაზრისით, საზოგადოება განაპირობებს სახელმწიფოს, რადგან სწორედ საზოგადოებას შეუძლია, დადებითი ან უარყოფითი კუთხით ზემოქმედება მოახდინოს სახელმწიფო განვითარებაზე. უცხო სახელმწიფოთა სპეცსამსახურების მნიშვნელოვანი დაინტერესებისა და ზემოქმედების მიმართულებას ზემოქმედების ობიექტი სწორედ სახელმწიფოს საზოგადოება და მასში არსებული განწყობები წარმოადგენს, რადგან საზოგადოებრივი აზრით მანიპულირება (წინასწარ გათვლილი შედეგის მისაღწევად გარკვეული მოქმედებების განხორციელება რასაც საბოლოოდ მოჰყვება დაგეგმილი შედეგის დადგომა) ერთ-ერთი მძლავრი ბერკეტია სპეცსამსახურების წარმატებული სამოქმედო არეალის შესაქმნელად, რომლის ძირითად მიზანს ძალაუფლების მოპოვება ან უკვე არსებულის შენარჩუნება წარმოადგენს, ამ მიზნით უძველესი დროიდან აქტუალურია საზოგადოებრივი აზრით მანიპულირების მეთოდები.

სოციალურ-პოლიტიკურ ლექსიკონში არსებული განმარტების თანახმად, საზოგადოებრივი აზრი - ესაა, ქვეყნის მოსახლეობის დიდი ნაწილის დამოკიდებულება საზოგადოებრივი ცხოვრების პრობლემებისადმი, რაც გამოიხატება მათ შეფასებებში,

---

[1] „სახელმწიფო“, საქართველოს პარლამენტის ეროვნული ბიბლიოთეკა, http://www.nplg.gov.ge/gwdict/index.php?a=term&d=5&t=4393;

[2] გ. ინწკირველი. „სახელმწიფოსა და სამართლის ზოგადი თეორია.“ თბილისი, თბილისის უნივერსიტეტის გამომცემლობა, 2003 წ. გვ. 39-45;

მსჯელობასა და განწყობაში. საზოგადოებრივი აზრი არის იდეოლოგიურ-ფსიქოლოგიური დამოკიდებულება ქვეყენაში არსებული წესრი-გისადმი, მას შეუძლია შეცვალოს, მხარი დაუჭიროს ან უარყოს გარკვეული საკითხები, რომლებიც ეხება ქვეყნის საზოგადოებრივი ცხოვრების სხვადასხვა სფეროს.[3]

მ.ჭაბაშვილის განმარტებით, საზოგადოებრივი აზრით მანიპულირების ერთ-ერთი მიზანია ის, რომ დადგეს წინასწარ გათვლილი შედეგი[4], რომელიც სასურველი იქნებოდა კონკრეტული დაინტერესებული სახელმწიფოსათვის ან ამ სახელმწიფოს პოლიტიკის გამტარებელი ხელისუფალისთვის.[5]

აღნიშნულიდან გამომდინარე, სადაზვერვო ზემოქმედების პირობებში არსებობს მაღალი ალბათობა საზოგადოებრივი აზრის არარეალურზე მისამხრობად, რაც საზოგადოების სახელმწიფოს წინააღმდეგ მოქმედების მაპროვოცირებელი გარემოება შეიძლება გახდეს.

ნებისმიერი სახელმწიფოს სწორი ეკონომიკური პოლიტიკა უმნიშვნელოვანეს როლს ასრულებს ქვეყნის სუვერენიტეტის განმტკიცებაში, სოცალური პრობლემების მოგვარებასა და ზოგადად, სახელმწიფოს მოკლე ან გრძელვადიანი პერსპექტივების განსაზღვრაში.

მსოფლიოში ძნელად მოიძებნება თუნდაც ერთი ეკონომიკურად ძლიერი სახელმწიფო, რომელსაც თავისთავად პოლიტიკური ძალაუფლება არ გააჩნია, მაგრამ მრავლად არიან ისეთი სახელმწიფოები, რომლებსაც პოლიტიკურად გარკვეული ძალაუფლება გააჩნიათ, თუმცა ეკონომიკა სუსტ ან ძალიან რთულ მდგომარეობაში აქვთ.

ძლიერი ეკონომიკა განსაზღვრავს ქვეყნის სტრატეგიას რეგიონსა და საერთაშორისო ასპარეზზე. სწორედ ეკონომიკის განვითარებაზეა დამოკიდებული სახელმწიფოთა სამხედრო პოტენციალი, მოსახლეობის განათლება, დემოგრაფიული მდგომარეობა და სახელმწიფოთა განვითარების უამრავი სხვა ფაქტორი.

დღემდე მსოფლიოში წამყვან როლს ასრულებდნენ მძლავრი მილიტარისტული სახელმწიფოები, თუმცა დღეს მსოფლიო გლობალიზაციის პროცესების დაწყების შემდეგ განსაკუთრებული მნიშვნელობა ენიჭება ქვეყნის ეკონომიკური მდგომარეობის დროულ, სრულყოფილ და ობიექტურ შეფასებას.

ქვეყანაში სუსტი ეკონომიკის არსებობა, პირველ რიგში, ზიანს აყენებს ქვეყნის მოსახლეობას (საზოგადოებას), უარესდება მოსახლეობის სოციალური მდგომარეობა, რაც განაპირობებს მოსახლეობის უკმაყოფილებას ხელისუფლების მიმართ, ამით კი საფრთხე ექმნება სახელმწიფოს პოლიტიკურ, სოციალურ და სამართლებრივ სტაბილურობას. იმ შემთხვევაში, თუ ვერ ან არ მოხერხდება ქვეყანაში სოციალური მდგომარეობის გამოსწორება, მაშინ შესაძლოა სახელმწიფომ თავიდან ვერ აიცილოს სახელმწიფო (მათ შორის ეკონომიკურ) უსაფრთხოებაზე დამაზიანებლად მოქმედი ისეთი ქმედებები, როგორიცაა: მასობრივ არეულობა, სამოქალაქო ომი, ეკონომიკური დივერსიები და ა.შ.

შეიძლება ითქვას, რომ სახელმწიფოთა შენარჩუნება-განვითარების მნიშვნელოვანი წინაპირობა არის სახელმწიფოში დადებითი ეკონომიკური მაჩვენებლების უზრუნველყოფა.

---

[3] სოციალურ და პოლიტიკურ ტერმინთა ლექსიკონი-ცნობარი, თბილისი, გამომცემლობა „ლოგოს პრესი,“ 2004 წ. გვ. 258;

[4] მიხეილ ჭაბაშვილი, უცხო სიტყვათა ლექსიკონი, გამომცემლობა „განათლება,“ თბილისი 1973, გვ. 231;

[5] „საზოგადოებრივი აზრი“, საქართველოს პარლამენტის ეროვნული ბიბლიოთეკა, განმარტებითი ლექსიონი, www.nplg.gov.ge/gwdict/index.php?a=term&d=6&t=6359;

ამ მიმართებით უძველესი პერიოდიდან დღემდე ერთ-ერთ მნიშვნელოვან პირობას წარმოადგენს სახელმწიფოში ზომიერი საგადასახადო სისტემის ჩამოყალიბება.

ისტორიაში არაერთი მაგალითია იმისა, თუ რა შედეგი შეიძლება მოჰყვეს სახელმწიფოში დიდ და შეუსაბამო გადასახადებსა და არასწორი ეკონომიკური სისტემის დანერგვას, ასე, მაგალითად:

ძვ.წ აღ. 241 წელს კართაგენში მოქირავნეების, მონებისა და ადგილობრივი თავისუფალი მოსახლეობის აჯანყება (აჯანყებულთა რიცხვი: 4000 კაცი)[6] აუტენელი გადასახადების გამო მოხდა, რადგან სოციალურ-ეკონომიკური მდგომარეობის სიმძიმის გამო კართაგენის მოსახლეობა პრაქტიკულად გადახდისუუნარო იყო. აჯანყებამ ორი წელს გასტანა ძვ.წ აღ. 241-238 წწ. რასაც შედეგად მისი ჩახშობა, ე.ი. არსებული ხელისუფლების უკმაყოფილო პირთა წრის გაზრდა მოჰყვა, ამას თან დაერთო, კონტოლირებადი ტერიტორიების (კორსიკისა და სარდინიის) დაკარგვა და რომის იმპერიის კონტროლქვეშ გადასვლა.

აქედან გამომდინარე, კართაგენში აჯანყება მოსახლეობის სოციალურ-ეკონომიკური მდგომარეობის შესახებ ოპერატიული მონაცემების არ არსებობით, ან არსებობით, თუმცა მისი გაუთვალისწინებლობის გამო მოხდა. აჯანყების ჩახშობის ფონზე მიღწეული იქნა სადაზვერვო მიზანი კონტროლს დაქვემდებარებული ტერიტორიების დაკარგვის კუთხით. ყოველივე ეკონომიკური დაზვერვის ნიშნებს შეიცავს.

532 წელს ბიზანტიასა და ირანს შორის დაზავების შემდეგ, ბიზანტიის იმპერატორმა ეგრისში ვაჭრობის მონოპოლია დააწესა, რამაც ადგილობრივი მოსახლეობის ცხოვრების პირობების გაუარესება და მათი უკმაყოფილება გამოიწვია. 541 წელს უკმაყოფილო მოსახლეობამ დაიწყო აჯანყება ბიზანტიის მმართველობის წინააღმდეგ, მათ დასახმარებლად მიმართეს ირანს, რომელმაც ეგრისში შემოიყვანა თავისი ლაშქარი. ეგრისში გავლენის მოსაპოვებლად დაიწყო ომი ბიზანტიასა და ირანს შორის, რომელიც 20 წელს გაგრძელდა[7].

მყარ სადაზვერვო კონტროლს დაქვემდებარებულ ტერიტორიაზე რეალური სოციალურ-ეკონომიკური ვითარების გაუთვალისწინებლობით შეუსაბამო გადასახადების დაწესებამ, მოსახლეობის მასობრივი უკმაყოფილების, პროტესტის ფონზე დაზვერვას დაქვემდებარებულმა სახელმწიფომ არჩია სხვა სახელმწიფოს აქტიური სადაზვერვო ზეგავლენის ქვეშ ყოფნა, რამაც მზვერავ სახელწიფოებს შორის ხანგრძლივი საომარი კონფლიქტის ინსპირირება გამოიწვია. ყოველივე ეს ეკონომიკური დაზვერვის ნიშნებს შეიცავს.

ქართლში სპარსელთა ბატონობის წინააღმდეგ 1742-1745 წლებში, აჯანყების მიზეზი მოსახლეობის სოციალურ-ეკონომიკური პირობების შეუსაბამო, დიდი გადასახადების ხარკის სახით დაწესება გახდა, იმ პირობებში, როდესაც საქართველოს მოსახლეობას მძიმე

---

[6] ალექსანდრე წერეთელი, „ძველი რომის ისტორია“, თავი VI, „ბრძოლა რომსა და კართაგოს შორის“, თბილისი, თბილ. უნ-ტის გამ-ბა. ტ. II. 1961 წ. გვ. 75-86;

[7] მარიამ ლორთქიფანიძე. დავით მუსხელიშვილი, როინ მეტრეველი, „საქართველოს ისტორია“, „საქართველო VI-VII ს-ის დასაწყისში“, თბილისი, გამომცემლობა „პალიტრა L“, ტომი II, 2012 წ. გვ. 79-81;

ტვირთად აწვა ჯარის სავალდებულო შენახვისათვის დაწესებული ყიზილბაშური ხარკი „მალუჯათი“ და სპარსული ჯარისთვის სურსათის გადასახადი „ნუქერი“[8].

აჯანყების ორგანიზაციის ერთ-ერთი მნიშვნელოვანი კვანძი ქვეყნის გარეთ-ასტრახანში იყო, სადაც თავი ჰქონდა შეფარებული სამეფო ტახტზე ასვლისათვის მებრძოლ ვახტანგ VI-ის ძეს ბაქარს. აჯანყების მუხტის შესამცირებლად სპარსელთა მხრიდან სისტემატური ხასიათი მიიღო ქართველთა ერთიანობის გამორიცხვის მიზნით, თავადების მოსყიდვით გადაბირებამ, რამაც თავადებს შორის კონფლიქტის გაღვივება გამოიწვია. შეიქმნა ნოყიერი ნიადაგი საქართველოსადმი მტრულად განწყობილი ორი დიდი იმპერიის-ოსმალეთისა და ირანის დაპირისპირების ტერიტორიად ქცეულიყო საქართველო, რაც ქვეყნის დასუსტებისა და დაქუცმაცების მნიშვნელოვან პირობს წარმოადგენდა.

ამ შემთხვევაშიც არ განხორციელდა რეალური სოციალურ-ეკონომიკური ვითარების შესახებ ინფორმაციის სწორი ანალიზი. აჯანყების მიზანმიმართულ ორგანიზებას ქართლზე სადაზვერვო კონტროლის განმხორციელებელ სეგმენტში მესამე ქვეყნის (რუსეთი) მაღალი დონის სადაზვერვო შეღწევადობა განაპირობებდა, მიუხედავად იმისა, რომ სპარსეთს ქართლში გააჩნდა მყარი აგენტურული აპარატი ქართველი თავადების სახით. შეიძლება ითქვას, რომ სახეზეა ეკონომიკური ხასიათის სადაზვერვო ქმედებები პოლიტიკური მიზნების მისაღწევად.

1865 წელს თბილისში ამქართა აჯანყების (მონაწილეები: ათი ათასამდე მუშა, ხელოსანი, მეეტლე, მემწვანილე და ქალაქის ღარიბი მოსახლეობა)[9] გამომწვევი ერთ-ერთი ძირითადი მიზეზი ქალაქის თავის - შერმაზან ვარ-თანოვის განკარგულება იყო დამატებითი გადასახადების დაწესების თაობაზე. აჯანყების განვითარების ქრონოლოგია ასე გამოიყურებოდა: მღელვარების და ხელისუფლებისადმი მშვიდობიანი პროტესტის მასობრივ პროტესტსა და არეულობებში გადაზრდა, რომელიც პოლიციის განყოფილების, ქალაქის თავის საცხოვრებელი სახლის დარბევით, გადასახადის ამკრეფის სიკვდილით, ხოლო ხელისუფლების მხრიდან აჯანყებულთა დარბევის შედეგად რამდენიმე ადამიანის სიკვდილით დასრულდა.

აქედან გამომდინარე, სახეზეა ეკონომიკური ხასიათის კონტრსადაზვერვო ინფორმაციის არქონა ან არსებობა და მის გამოუყენებლობას, რითაც მიღწეულ იქნა საქართველოზე კონტრსადაზვერვო კონტროლის მქონე რუსეთის იმპერიის სადაზვერვო მიზნები.

ეგვიპტის 2011 წლის რევოლუციის ძირითად მაინსპირირებელ გარემოებებს მრავალი ათეული წლის განმავლობაში სახელმწიფოს მმართველი სამოქალაქო და სამხედრო სექტორის წევრების კორუფციულ პროცესებში მასშტაბური მონაწილეობა წარმოადგენდა, რაც დამანგრევლად მოქმედებდა სახელმწიფოს ეკონომიკურ პროცესებზე და მდიდარი რესურსების პირობებში მოსახლეობა საკმარის სარგებელს ვერ ნახულობდა. ამ შემთხვევაში მასობრივი პროტესტი მასობრივ არეულობაში გადაიზარდა, რასაც თან დაერთო ქვეყნის პრეზიდენტის იძულებითი გადაყენების პროცესი; [10]

---

[8] მარიამ ლორთქიფანიძე, დავით მუსხელიშვილი, როინ მეტრეველი, „საქართველოს ისტორია“, „ქვეყნის სოციალურ-ეკონომიკური განვითარების ხასიათი XVIII საუკუნეში“, თბილისი, გამომცემლობა „პალიტრა L“, ტომი III, 2012 წ, გვ. 393-394;

[9] ნ. ნიკოლაძე, „ივნისის დღეები თბილისში“, თბილისი, თბილ. უნივერსიტეტისტის გამომცემლობა. თხზ. ტომი 1, 1962 წ. გვ. 300-301;

[10] Al Jazeera, „Egypt's revolution, A chronicle of the revolution that ended the three-decade-long presidency of Hosni Mubarak“, http://www.aljazeera.com/news/middleeast/2011/01/201112515334871490.html;

2011 წლის 15 თებერვალს, კორუფციის მაღალი დონით და მოსახლეობის ცუდი საცხოვრებელი პირობებით უკმაყოფილო ხალხმა ანალოგიური სცენარით განავითარა მოვლენები ჩრდილო-აფრიკულ სახელმწიფო ლიბიაში.[11] ამ შემთხვევაში სახელმწიფოსათვის უფრო მძიმე შედეგები დადგა, რადგან მასიური არეულობა სამხედრო-შეიარაღებულ დაპირისპირებასა და სამოქალაქო ომში გადაიზარდა და საბოლოოდ ქვეყნის პრეზიდენტის - მუამარ კადაფის რეჟიმის ძალადობრივი დამხობით დასრულდა.

ეგვიპტისა და ლიბიის მაგალითებზე დაყრდნობით შეიძლება ითქვას, რომ აღნიშნულ სახელმწიფოს მმართველობით (მათ შორის ეკონომიკურ) სექტორში იყო უცხო ქვეყნის სპეცსამსახურების მაღალი დონის სადაზვერვო შეღწევადობა, რაც ქვეყნის განვითარების პროცესების შემზღუდველი გარემოებაა და რითაც მიღწეულ იქნა არასასურველი ხელისუფალის თანამდებობიდან იძულებითი ჩამოშორების პროცესი სასურველი ხელისუფალის ჩანაცვლების უზრუნველსაყოფად.

2014 წლის ოქტომბერ-ნოემბერში უნგრეთში მოსახლეობის მხრიდან მასშტაბური ანტისამთავრობო გამოსვლების ორგანიზების ხელშემწყობი მთავრობის მიერ ინიცირებული კანონპროექტი (ინტერნეტის პროვაიდერებისთვის გადასახადის გაზრდა) გახდა, რომლის შედეგადაც მოსახლეობას ინტერნეტმომსახურეობაზე გადასახადი უძვირდებოდა; ეს მათ სოციალურ-ეკონომიკური მდგომარეობის გაუარესებას გამოიწვევდა. ამ შემთხვევაშიც მშვიდობიანი საპროტესტო აქცია, რომელშიც 100 000 ადამიანი მონაწილეობდა, მასობრივ არეულობაში გადაიზარდა, რასაც მმართველი პარტიის ოფისების დარბევა-დაზიანება მოჰყვა.[12]

აღნიშნული ფაქტი ადასტურებს, რომ ხელისუფლებას არ გააჩნდა ან გააჩნდა და არ გაითვალისწინა მოსახლეობის სოციალურ-ეკონომიკური ვითარება. შესაბამისად ვერ იქნა გათვალისწინებული კონკრეტული ეკონომიკური ხასიათის გადაწყვეტილების შემთხვევაში მოსახლეობის დამოკიდებულება და მოსალოდნელი მავნე შედეგები სახელმწიფოსათვის.

2019 წლის ნოემბერში, ირანის დედაქალაქ თეირანში გამოვიდა ასიათასობით ირანის მოქალაქე, რომლებმაც გააპროტესტეს ირანში ნავთობის ფასის 50%-იანი ზრდა, რაც გამოიწვეულ იქნა აშშ-ის მიერ ირანისათვის სანქციების დაწესებით. აქციებმა მიიღო მასშტაბური ხასიათი, რაც საბოლოოდ ძალოვან ორგანიებთან დაპირისპირებითა და მსხვერპლით დასრულდა.[13] აღნიშნული ფაქტის გაანალიზებით, შეიძლება თქვას, რომ უცხო სახელმწიფოს სპეცსამსახურები ცდილობენ მოწინააღმდეგე სახელმწიფოზე კონტროლის დაწესებას, მათ შორის ეკონომიკურ სექტორზე, რაც აძლევს მათ საშუალებას მოახდინონ ზემოქმედება მოწინააღმდეგე სახელმწიფოს ხელისუფლებაზე გადაწყვეტილების მიღებისას ამათუ იმ საკითხში.

უნდა აღინიშნოს, რომ ხელისუფლებისადმი მოსახლეობის მასობრივი უკმაყოფილება, დაინტერესებულ უცხო სახელმწიფოთა სპეცსამსახურების ინტერესებში შედის, რომლებიც, რიგ შემთხვევაში მიზანმიმართულად ხელს უწყობენ, როგორც ასეთი განწყობების ინსპირირებას, ისე მათ მასობრივ საპროტესტო აქციებში, მასობრივ

---

11 Varun Vira and Anthony H. Cordesman Arleigh A. Burke Chair in Strategy,Center For Strategic & International Studies, „The Libyan Uprising“, 20 June 2011, http://csis.org/files/publication/110620_libya.pdf;

12, Pablo Gorondi, „Thousands in Hungary march against Internet tax“, Phys.org, http://phys.org/news/2014-10-thousands-hungary-internet-tax.html;

13 Hannah Brown, Why economic hardships finally sparked Iranian protests, Updated Dec 2, 2019, https://www.vox.com/world/2019/11/25/20980775/iran-protests-gas-prices;

არეულობებში, სამოქალაქო დაპირისპირებაში გადაზრდის ორგანიზებას. ყოველივე აღნიშნული კი ეკონომიკური დაზვერვის ერთ-ერთი მნიშვნელოვანი მიმართულებაა.

მოყვანილი ფაქტების განხილვისა და გაანალიზების შედეგად, შეიძლება გამოიკვეთოს სახელმწიფოს ეკონომიკურ უსაფრთხოებაზე და მათ შორის, ეროვნულ უსაფრთხოებაზე ზემოქმედების ინდიკატორები:

- სახელმწიფოს ძლიერება ქვეყანაში სტაბილური და გამართული ეკონიმიკური სისტემის ჩამოყალიბების, დაცვა-განვითარების პროცესების ორგანიზებითაა შესაძლებელი, რომლის მიღწევა სახელმწიფოს სპეცსამსახურების მიერ წარმატებული სადაზვერვო და კონტრსადაზვერვო საქმიანობის განხორციელებით არის შესაძლებელი;
- ძლიერი ეკონომიკის მქონე ქვეყანებს აქვთ უდიდესი შესაძლებლობები განახორციელონ მასშტაბური სადაზვერვო საქმიანობა საკუთარი ინტერესების გასატარებლად და ეროვნული უსაფრთხოების განმტკიცების მიზნით;
- ეკონომიკური დაზვერვის მნიშვნელოვან ინტერესს მოწინააღმდეგე სახელმწიფოში ეკონომიკური სექტორის დაზიანება ან/და ეკონომიკური ექსპანსია წარმოადგენს, რომლითაც შესაძლებელია მიღწეულ იქნას ეკონომიკური არასტაბილურობა, სოციალურ-ეკონომიკური და პოლიტიკური ვითარების დაძაბვა, რაც შემდგომში გამოხატულებას ჰპოვებს მასობრივ პროტესტებში, რა დროსაც არსებობს საფრთხე მისი მასობრივ არეულობასა და სამოქალაქო ომში გადაზრდისა და კონსტიტუციური წყობილების ძალადობრივი რღვევის;
- მასობრივი არეულობის გამომწვევია ისეთი სახის გადასახადების დაწესება, რომლებიც მასშტაბურად განაპირობებს მოსახლეობის უარყოფით განწყობას, ამ კუთხით აღსანიშნავია სახელმწიფოს მოსახლეობის უმეტესი ნაწილის მძიმე სოციალურ-ეკონომიკურ პირობებში ცხოვრება;
- ეკონომიკური დაზვერვისათვის ხელსაყრელი პირობები იქმნება როდესაც სახელმწიფოს (მათ შორის კონტრდაზვერვითი უზრუნველყოფის სპეცსამსახურებს) არ გააჩნიათ ოპერატიული მონაცემები სოციალურ-ეკონომიკური ვითარების შესახებ ან გააჩნიათ და არ იყენებენ მათ მიზანმიმართულად;
- სახელმწიფოს ეკონომიკურ სეგმენტზე კონტრსადაზვერვო ინფორმაციის არ არსებობა, ან არსებობა და მისი გაუთვალისწინებლობა ეკონომიკური და ეროვნული უსაფრთხოების რღვევის მაინსპირირებელი მნიშვნელოვანი წინაპირობაა;
- ეკონომიკური დაზვერვის ინტერესებიდან გამომდინარე, მსოფლიო ისტორიაში არსებობს არაერთი პრაქტიკა მოწინააღმეგე სახელმწიფოს არასასურველი ხელისუფლება ჩანაცვლებულ იქნას უცხო სახელმწიფოს სასურველი ხელისუფლებით, ფარული სადაზვერვო ხასიათის ოპერაციული ღონისძიებების განხორციელებით.[*]

[*] ამ კუთხით აღსანიშნავია 1954 წელს, ამერიკის შეერთებული შტატების ცენტრალური სადაზვერვო სააგენტოს მიერ ჩატარებული ფარული სადაზვერვო ოპერაცია სახელწოდებით „PBSUCCESS“ გვატემალაში, რომელსაც კანონიერი პრეზიდენტის ხაკობო არბენზის გადაყენება და ოპერაციის ორგანიზატორი სახელმწიფოს ინტერესების გამტარებელი მმართველის კარლოს კასტილიო არმასის სამხედრო რეჟიმის დამყარება მოჰყვა.

ბიბლიოგრაფია

1. „სახელმწიფო“, საქართველოს პარლამენტის ეროვნული ბიბლიოთეკა, http://www.nplg.gov.ge/gwdict/index.php?a=term&d=5&t=4393;
2. გ. ინწკირველი. „სახელმწიფოსა და სამართლის ზოგადი თეორია.“ თბილისი, თბილისის უნივერსიტეტის გამომცემლობა, 2003 წ. გვ. 39-45;
3. სოციალურ და პოლიტიკურ ტერმინთა ლექსიკონი-ცნობარი, თბილისი, გამომცემლობა „ლოგოს პრესი,“ 2004 წ. გვ. 258;
4. მიხეილ ჭაბაშვილი, უცხო სიტყვათა ლექსიკონი, გამომცემლობა „განათლება,“ თბილისი 1973, გვ. 231;
5. „საზოგადოებრივი აზრი“, საქართველოს პარლამენტის ეროვნული ბიბლიოთეკა, განმარტებითი ლექსიონი, www.nplg.gov.ge/gwdict/index.php?a=term&d=6&t=6359;
6. ალექსანდრე წერეთელი, „ძველი რომის ისტორია“, თავი VI, „ბრძოლა რომსა და კართაგოს შორის“, თბილისი, თბილ. უნ-ტის გამ-ბა. ტ. II. 1961 წ. გვ. 75-86;
7. მარიამ ლორთქიფანიძე. დავით მუსხელიშვილი, როინ მეტრეველი, „საქართველოს ისტორია“, „საქართველო VI-VII ს-ის დასაწყისში“, თბილისი, გამომცემლობა „პალიტრა L“, ტომი II, 2012 წ. გვ. 79-81;
8. მარიამ ლორთქიფანიძე, დავით მუსხელიშვილი, როინ მეტრეველი, „საქართველოს ისტორია“, „ქვეყნის სოციალურ-ეკონომიკური განვითარების ხასიათი XVIII საუკუნეში“, თბილისი, გამომცემლობა „პალიტრა L“, ტომი III, 2012 წ, გვ. 393-394;
9. ნ. ნიკოლაძე, „ივნისის დღეები თბილისში“, თბილისი, თბილ. უნ-ტის გამ-ბა. თხზ. ტომი 1, 1962 წ. გვ. 300-301;
10. Al Jazeera, „Egypt's revolution, A chronicle of the revolution that ended the three-decade-long presidency of Hosni Mubarak“, http://www.aljazeera.com/news/middleeast/2011/01/201112515334871490.html;
11. Varun Vira and Anthony H. Cordesman Arleigh A. Burke Chair in Strategy,Center For Strategic & International Studies, „The Libyan Uprising“, 20 June 2011, http://csis.org/files/publication/110620_libya.pdf;
12. Pablo Gorondi, „Thousands in Hungary march against Internet tax“, Phys.org, http://phys.org/news/2014-10-thousands-hungary-internet-tax.html;
13. Hannah Brown, Why economic hardships finally sparked Iranian protests, Updated Dec 2, 2019, https://www.vox.com/world/2019/11/25/20980775/iran-protests-gas-prices;