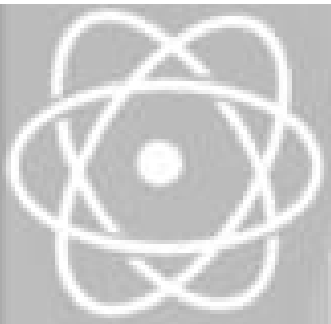


SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL4 No3
SEPTEMBER 2020

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 1-6 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

THE ANALYSIS OF THE DIFFERENCE OF 4G AND 5G SECURITIES.

4G და 5G უსაფრთხოების განსხვავებების ანალიზი

მ. იავიჩი. კავკასიის უნივერსიტეტი
M. Iavich. Caucasus University of Georgia
გ. იაშვილი. კავკასიის უნივერსიტეტი
G. Iashvili. Caucasus University of Georgia
ა. გაგნიძე. სამეცნიერო კიბერუსაფრთხოების ასოციაცია
A.gagnidze Scientific Cyber Security Association
ლ.ნაჭყებია. სამეცნიერო კიბერუსაფრთხოების ასოციაცია
L.Nachkebia Scientific Cyber Security Association
შ. ხუხაშვილი. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი
S. Khukhashvili. Ivane Javakhishvili Tbilisi State University

ABSTRACT: The paper analyzes the difference between 4G and 5G architectures. The difference between 4g and 5G security is also analyzed. We analyzed the new security features of 5G, the advantages and disadvantages are identified. Are analyzed the existing attacks on 5G, such as MNmap, MiTM and Battery drain attacks. The recommendation for securing 5g are provided.

აბსტრაქტი: აღნიშნული სტატია აანალიზებს განსხვავებებს 4G და 5G ქსელების არქიტექტურებს შორის. ასევე განხილულია 4G და 5G ქსელების უსაფრთხოება. აქ გავაანალიზეთ სიახლეები 5G-ს უსაფრთხოების სისტემაში, მათი დადებითი და უარყოფითი მხარეები. ასევე განხილულია არსებული შეტევები 5G-ზე: MNmap, MiTM და Battery drain(ბატარეის გამოფიტვის შეტევა). აგრეთვე მოყვანილია რეკომენდაციები სისტემისთვის უკეთესად დასაცავად.

საკვანძო სიტყვები: *4G და 5G, უსაფრთხოება, ფიჭური ქსელი*

Keywords: *4G vs 5G, security, cellular network*

შესავალი

5G არის მე-5 თაობის მობილური ქსელი, წინამორბედი 4G LTE ქსელის თვალსაჩინო გაუმჯობესება. 5G შექმნილია, რათა შეძლოს დიდ მონაცემებთან გამკლავება და შეესაბამებოდეს თანამედროვე საზოგადოების მოთხოვნებს, უზრუნველყოს მილიონობით IoT მოწყობილობის ჩართულობა და სამომავალი ინოვაციები. თავდაპირველად, 5G იმუშავებს არსებულ 4G ქსელთან ერთად, მომდევნო ეტაპზე კი - როგორც დამოუკიდებელი ქსელი.

5G-ს აქვს შემდეგი უპირატესობები: უფრო სწრაფი კავშირი და გაზრდილი მოცულობა, შეყოვნების პატარა დრო (სწრაფი უკუკავშირი).

ტექნოლოგია	შეყოვნება(მილიწამი)
3G	100მწ
4G	30მწ
5G	1მწ(თეორიულად)

1. გამოყენების შემთხვევები

- მასიური მანქანათაშორისი კომუნიკაცია, ანუ ინტერნეტით დაკავშირებული მოწყობილობები (IoT), რაც გულისხმობს მილიონობით ურთიერთდაკავშირებულ მოწყობილობას ადამიანური რესურსის ჩარევის გარეშე, ისეთ მასშტაბებზე რაც აქამდე ჯერ არ ყოფილა.
- დაბალი შეყოვნების მქონე კომუნიკაცია - უზრუნველყოფს მოწყობილობების მონიტორინგს რეალურ დროში, ინდუსტირულ რობოტებს და სატრანსპორტო საშუალებებს შორის კომუნიკაციას, ავტომობილების აუტონომიურ მართვას და უფრო უსაფრთხო სატრანსპორტო ქსელს. დაბალი შეყოვნების მქონე კომუნიკაცია გვაძლევს შესაძლებლობას ვისარგებლოთ დისტანციური სერვისებით, მაგალითად,ჯანდაცვის სფეროში.

- გაუმჯობესებული მობილური კავშირი - უზრუნველყოფს მნიშვნელოვნად გაზრდილ სიჩქარეს და გაზრდილ გამტარუნარიანობას, რათა მსოფლიო იყოს მუდმივ კავშირში.

ბიზნესისა და მრეწველობისათვის, 5G და IoT უზრუნველყოფს დიდი რაოდენობით მონაცემებს და მათი ანალიზის შედეგად ისეთ დასკვნებს, რაც აქამდე არ ყოფილა. ბიზნესი მიიღებს გადაწყვეტილებებეს, რომელიც უშუალოდ იქნება დაყრდნობილი მანამდე არსებულ მონაცემებზე, რაც ხელს შეუწყობს მაგ.: აგრარული სფეროს გაციფრულებას, მომხმარებელთან ურთიერთობის ხარისხის ამაღებას. ახალი ტექნოლოგიების დანერგვას, როგორებიცაა: ვირტუალური და აუგმენტირებული რეალობა რაც ყველასათვის იქნება ხელმისაწვდომი. რა თქმა უნდა, ეს გააჩენს აქამდე ჯერ არ არსებულ შესაძლებლობებს. 5G და ვირტუალური რეალობის ერთობლიობა შესაძლებლობას მოგვცემს ვირტუალურად ვიმოგზაუროთ სასურველ ქალაქში, ვუყუროთ ფეხვურთის მატჩს და განვიცადოთ იგივე შეგრძნებები რაც სტადიონზე ყოფნისას და მრავალი სხვა.

5G იქნება ძირეული კომპონენტი სამომავლოდ ,,ჭკვიანი ქალაქების“, ‘‘ჭკვიანი სახლების“, ,,ჭკვიანი სკოლების“ შესაქმნელად. რეალურს გახდის ისეთ შესაძლებლობებს, რისი წარმოდგენაც კი ძნელი შეიძლებოდა ყოფილიყო აქამდე.

2. **5G-ს მუშაობა 4G-თან ერთად**

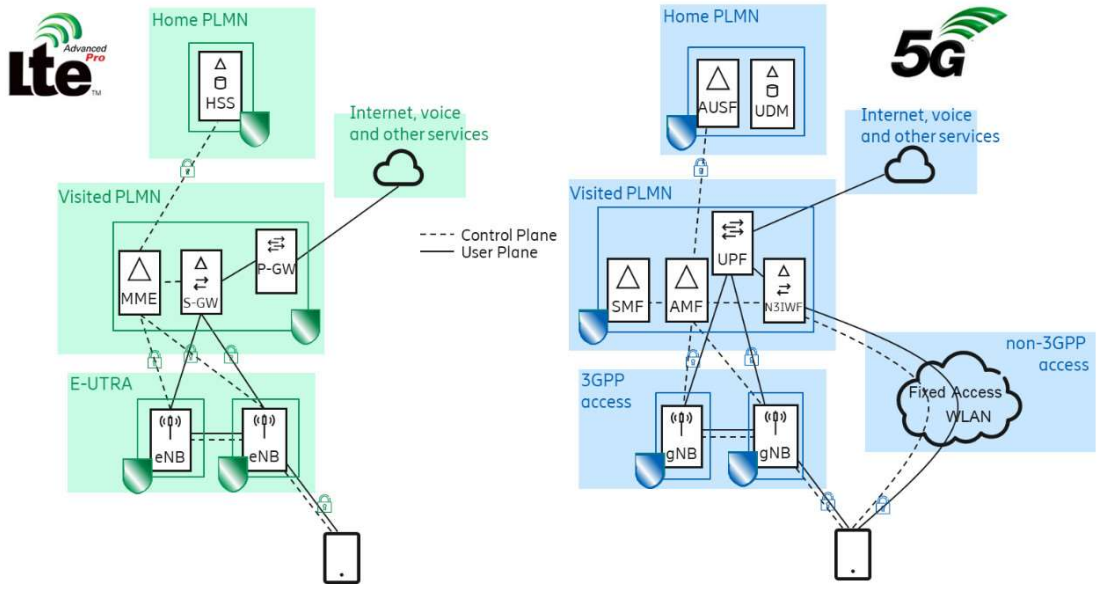
როდესაც 5G-სთან მიერთდება მოწყობილობა, ის მიუერთდება ასევე 4G ქსელსაც. ანუ პირველ ეტაპზე, სანამ 5G დამოუკიდებელ სისტემად ჩამოყალიბდება, არსებული 4G ქსელი 5G-სთან დაკავშირებისას მისი გამაძლიერებლის ფუნქციას შეასრულებს.

3. **4G vs 5G security**

5G და 4G ქსელების უსაფრთხოების არქიტექტურა მსგავსია. ორივე სისტემაში უსაფრთხოების მექანიზმები შეიძლება დაიყოს ორ ჯგუფად:

- პირველი ჯგუფი მოიცავს ქსელთან წვდომის დასამყარებლად საჭირო უსაფრთხოების მექანიზმებს. აქ არის უსაფრთხოების ისეთი კომპონენტები, რომლებიც უზრუნველყოფს მომხარებლის უსაფრთხოებას და იცავს შეტევებისაგან რომლებიც ხორციელდება მოწყობილობასა და მიმღებ ანტენას შორის

- მეორე ჯგუფი კი მოიცავს ქსელის დომეინის უსაფრთხოების მექანიზმებს. ეს მექანიზმები უწყობს ხელს ანტენებს შორის ინფორმაციის უსაფრთხოდ მიმოცვლას. მაგალითად მიმღებ რადიო ანტენასა და ძირითად ქსელს შორის.



უსაფრთხოების ძირითადი პროცედურა 3GPP ქსელებში არის აუტენთიფიკაცია, ცნობილი როგორც პირველადი აუტენთიფიკაცია 3GPP 5G უსაფრთხოების სტანდარტში. ეს პროცედურა სრულდება ყოველთვის როდესაც, მაგალითად, პირველად ირთვება მობილური ტელეფონი.

წარმატებული აუტენთიფიკაციის შემდეგ, იქმნება გასაღებები სესიისათვის. გასაღებები გამოიყენება მოწყობილობასა და ქსელს შორის კომუნიკაციის დასაცავად [1, 2]. აუტენთიფიკაციის პროცედურა 3GPP 5G უსაფრთხოების სისტემაში ისეა შემუშავებული, რომ

ჰქონდეს გაფართოებული აუტენთიფკაციის პროტოკოლის (EAP) მხარდაჭერა. აღნიშნული პროტოკოლი არის კარგად დამუშავებული და ფართოდ გამოიყენება IT გარემოში.

EAP იძლევა საშუალებას გამოვიყენოთ განსხვავებული ტიპის სენსიტიური მონაცემები, რომლებიც ინახება SIM ბარათზე: სერთიფიკატები, გასაღებები, მომხმარებლის სახელები/პაროლები. ამ აუტენთიფიკაციის მეთოდის მოქნილობის მთავარი მიზეზი არის ის, რომ ხელს უწყობს 5G-ს დანერგვას როგორც სატელეკომუნიკაციო ინდუსტრიაში, ასევე სხვა ინდუსტრიებში.

თავდაპირველი აუტენთიფიკაციისა და გასაღებების განაწილების პროცედურები ხელიმსაწვდომს ხდის აუტენთიფიკაციას მომხმარებელსა და ქსელს შორის და ასევე ქმნის არსებით კავშირებს მომხმარებელსა და ქსელს შორის უსაფრთხოების მომავალი პროედურებისათვის. ძირითადი პროდუქტი რაც ამ პროცედურების შემდეგ იქმნება არის „მთავარი გასაღები“ KSEAF, რომელსაც გადასცემს შიდა ქსელის AUSF ფუნქცია მომსახურე ქსელის SEAF ფუნქციას.

„მთავარი გასაღების“ კონცეფცია გვაძლევს საშუალებას ვაწარმოოთ გასაღებები უსაფრთხოების მრავალი განსვავებული მიზნისათვის ისე, რომ აუტენთიფიკაციის ხელახალი გავლა არ იქნება საჭირო. მაგალითად 3GPP ქსელში ავტორიზაციისას შექმნილი გასაღები, ასევე გამოიყენება მომხმარებელსა და Non-3GPP Interworking Function (N3IWF) შორის.

4. 5G უსაფრთხოების უპირატესობები

5G იყენებს ქსელის შრეებად დაყოფის კონცეფციას. ჩვენი კვლევის თანახმად ეს არის 5G-ს მთავარი უპირატესობა 4G LTE-სთან მიმართებაში. განსაზღვრების თანახმად, ქსელის ცალკეული შრე არის დამოუკიდებელი, ლოგიკური ქსელი, რომელიც მუშაობს გაზიარებულ ფიზიკურ ინფრასტრუქტურაზე, რომელსაც შეუძლია უზრუნველყოს სერვისის შესაბამისი ხარისხი. ეს კი ნიშნავს, რომ ჩვენ შეგვიძლია მთლიანი 5G დავყოთ თანაუკვეთ კომპონენტებად(ნაწილებად). ეს კონცეფცია ანალოგიურია VLAN-ის, რაც მოგვცემს საშუალებას, რომ დავყოთ და უსაფრთხოდ ვმართოთ სერვისები როგორიცაა:

- მობილური კავშირგაბმულობა: საკომუნიკაციო სისტემები, გართობა, ინტერნეტი
- მასიური IoT შრე: სამეწარმეო საქმიანობა, გადაზიდვები
- კრიტიკული IoT შრე: აუტონომიური სამედიცინო ინფრასტრუქტურა

აღნიშნული კონცეფცია სასარგებლოა უსაფრთხოების პერსპექტივიდანაც, რადგან სისტემა იქნება მეტად დაცული, სტრუქტურირებული და ადვილად სამართავი.

5. შეტევები 5G-ს უსაფრთხოებაზე

5G არქიტექტურაზე აღინიშნება წარმატებული შეტევები. ბოლო წლებში, მკვლევარებმა აღმოაჩინეს ხარვეზები 5G-ს უსაფრთხოების სისტემაში, რაც ხელს აძლევს ჰაკერებს სისტემაში ჩააშენონ მავნე კოდი და მიიღონ სასურველი შედეგები. აქ განვიხილავთ რამდენიმე მიზანმიმართულ შეტევას:

- **Mnmap**
  მკვლევართა გუნდმა მოიპოვა ინფორმაცია, რომელიც ქსელში გაგზავნილი იყო ღია ტექსტის სახით და ამის მეშვეობით მათ შექმნეს მოწყობილობების რუკა, რომლებიც დაკავშირებული იყო ამ ქსელთან. ასევე მათ შექმნეს ცრუ საბაზო სადგური და იმახსოვრებდნენ მიერთებული მოწყობილობების მონაცემებს. ამის შედეგად მათ შეეძლოთ დაედგინათ მოწყობილობის: მწარმოებელი, მოდელი, ოპერაციული სისტემა, მოწყობილობის ტიპი და ვერსია. ასევე შეეძლოთ დაედგინათ იყო თუ არა ეს მოწყობილობა ავტომობილი, როუტერი, USB თუ სხვა.

- **MiTM**
  ახლანდელი 5G შემტევს აძლვს საშუალებას განახორციელოს MiTM შეტევა. MiTM-ის იმპლემენტაციით შესაძლებელია ბატარეის გამოფიტვის შეტევის განხორციელება. შემტევს შეუძლია MIMO-დან (5G სიხშირეების მიმღები და გამცემი მოწყობილობა) ამოიღოს ფიზიკური ნაწილი, რომელიც უშულოდ პასუხისმგებელია მაღალ სიჩქარეზე. ამის შედეგად, სისტემა ექვივალენტური გახდება 2G/3G/4G ქსელების და შეეძლება იმ სისუსტეების გამოყენება რაც აღნიშნულ ქსელებს აქვთ.

- **Battery drain attack.**

  ეს შეტევა მიმართულია NB-IoT მოწყობილობებზე. ისინი გარკვეული დროის შუალედებით აგზავნიან ინფორმაციის მცირე პაკეტებს. ამ პაკეტებს შეუძლიათ გამოფიტონ ბატარეის ისეთი ზომის ენერგია, რაც 10 წელი ეყოფოდა ენერგიის შენახვის მდგომარეობაში(power saving mode). შემტევს შეუძლია ისეთი მოდიფიკაცია გაუკეთოს ამ მდგომარეობაში მყოფ მოწყობილობას, რომ მას ქონდეს უწყვეტი აქტივობა და მუდმივად ეძებდეს ქსელს დასაკავშირებლად. ამ შემთხვევაში, შემტევს შეუძლია დააკავშიროს მოწყობილობა სასურველ ქსელთან, შემდეგ კი განახორციელოს სასურველი ქმედებები, როგორც ქსელთან ასევე მოწყობილობასთან მიმართებაში.

6. დასკვნა

ჩვენს კვლევაზე დაყრდნობით შეგვიძლია ვთქვათ, რომ 5G-ს აქვს ახალი ფუნქციები, რომლებიც აუმჯობესებს უსაფრთხოებას. აღსანიშნავია, რომ 5G უახლესი ტექნოლოგიაა და მისი უსაფრთხოება სათანადოდ არაა გამოკვლეული ამ ეტაპისათვის. ამ სტატიაში მოვიყვანეთ არსებული შეტევები 5G-ზე, რაც თვალნათლივ გვანახებს 5G უსაფრთხოების

სისუსტეებს. აქედან ჩანს, რომ დიდი სამუშაოა გასაწევი და შესამუშავებელია უფრო მძლავრი უსაფრთხოების სისტემა 5G-ს ეფექტურად მუშაობისათვის.

შენიშვნა:

აღნიშნული სამუშაო შესრულებულია CARYS-19, PHDF-19-519 და კავკასიის უნივერსიტეტის მიერ დაფინანსებული გრანტის ფარგლებში.

The work was conducted as a part of PHDF-19-519, the grant financed by Caucasus University and CARYS 2019 [CARYS-19-121]

ლიტერატურა:

1. Gagnidze, A., Iavich, M, Iashvili, G. : Novel version of merkle cryptosystem. Bull. Georgian Natl. Acad. Sci. 11(4), 28–33 (2017)

2. Avtandil Gagnidze & Maksim Iavich & Giorgi Iashvili, 2017. "Some Aspects Of Post-Quantum Cryptosystems, " Eurasian Journal of Business and Management, Eurasian Publications, vol. 5(1), pages 16-20.

3. S. Zhang, "An Overview of Network Slicing for 5G, " in IEEE Wireless Communications, vol. 26, no. 3, pp. 111-117, June 2019, doi: 10. 1109/MWC. 2019. 1800234.

4. P. Popovski, K. F. Trillingsgaard, O. Simeone and G. Durisi, "5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A Communication-Theoretic View, " in IEEE Access, vol. 6, pp. 55765-55779, 2018, doi: 10. 1109/ACCESS. 2018. 2872781.

5. V. Sciancalepore, K. Samdanis, X. Costa-Perez, D. Bega, M. Gramaglia and A. Banchs, "Mobile traffic forecasting for maximizing 5G network slicing resource utilization, " IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, Atlanta, GA, 2017, pp. 1-9, doi: 10.1109/INFOCOM.2017.8057230.

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 7-10 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

PRETTY GOOD PRIVACY (PGP)- გამოყენებასთან დაკავშირებული გამოწვევები

CHALLENGES OF USING OF PRETTY GOOD PRIVACY (PGP)

ზაალ ჯანიკაშვილი, სამეცნიერო კიბერუსაფრთხოების ასოციაცია
Z. Janikashvili, Scientific Cyber Security Association
ირმა ჩინჩალაძე, სამეცნიერო კიბერუსაფრთხოების ასოციაცია
I.Chinchiladze, Scientific Cyber Security Association

აბსტრაქტი: სტატიაში განხილულია PGP-ის ადრეული ისტორია, მუშაობის პრინციპი, წამოჭრილია ის პრობლემები რასაც ვაწყდებით მისი გამოყენებისას.

ABSTRACT: It is discussed and examined earlier history and working principles of PGP in this article. Also, we discuss challenges and problems we are faced while using PGP

საკვანძო სიტყვები: *კრიპტოგრაფია, PGP;*

KEYWORDS: *cryptography, PGP*

პგპ-ს ადრეული ისტორია

PGP გახლავთ ყველასთვის კარგად ცნობილი კრიპტოგრაფიული პროტოკოლი რომლის ძირითად მიზანს წარმოადგენს მომხმარებელთა ძირითადი მასის კონფიდენციალურობის უზრუნველყოფა. მისი თავდაპირველი სქემა, შექმნილი ფილიპ რ. ციმერმანის(Philip R. Zimmermann) მიერ, პირველად ინტერნეტში გამოქვეყნდა 1991 წელს, რომელიც ემსახურებოდა ელექტრონული შეტყობინებების დაშიფვრას. იმის გათვალისწინებით, რომ ღია გასაღების დაშიფვრისა და ხელმოწერის შესაქმნელად დამოკიდებული იყო RSA-ს საფუძვლებზე, სწრაფადვე მიიპყრო იმ კომპანიის ყურადღება, რომელსაც დაპატენტებული ჰქონდა RSA-ის თავდაპირველი ალგორითმები, და უფრო მეტიც PGP-თი დაინტერესდა შეერთებული შტატების მთავრობაც, კერძოდ, ციმერმანს ბრალს სდებდნენ კრიპტოგრაფიასთან დაკავშირებული გაშიფვრის აკრძალვის დარღვევაზე, რაც განაპირობა PGP-ის საწყისი კოდი ის გასაჯაროვებამ.[1]

საინტერესოა, რისთვის დაგვჭირდა და რამ გამოიწვია PGP ის შექმნა. მოგეხსენებათ, ჯერ კიდევ წინა საუკუნიდან მოყოლებული რამდენად სწრაფად მიიწევს წინ ციფრული ტექნოლოგიების განვითარება, აღნიშნული ფაქტის შედეგად, ადამიანთა უმრავლესობამ უარი თქვა ერთ დროს ძალიან გავრცელებულ საქმიანობებზე, მაგალითად, როგორიცაა ქაღალდზე წერა, ფოსტით შეტყობინებიბს გაგზავნა და ა.შ. და გადავიდნენ უფრო მეტად მოხერხებულ, მოქნილ და დღესდღეობით ფართოდ გავრცელებულ ელექტრონული ფოსტის სისტემაზე.

აღნიშნული წინსვლა, ერთი მხრივ, მოხერხებულობას სთავაზობდა კაცობრიობას, თუმცა, მეორე მხრივ, შეიქმნა უსაფრთხოების პრობლემაც [2], მაგალითად, როდესაც კონვერტით ხდებოდა შეტყობინების გაგზვნა, ამ დროს მომხმარებელი ბევრად უფრო დაცული იყო, რომ მის მიერ გაგზავნილ კონვერტს არავინ გახსნიდა, რადგან გახსნის მცდელობის შემთხვევაშიც კი კონვერტი დაზიანდებოდა და დანაშაულებრივი ქმედება გამოაშკარავდებოდა.

რაც შეეხება ჩვენს თანამედროვე რეალობაში მიმდინარე მოვლენებს, ყოველი დღის განმავლობაში იგზავნება მილიონობით მეილი, იქნება ეს პირადი თუ ოფიციალური ხასიათის, და ყოველთვის, როდესაც გამოიყენება ელექტრონულ ფოსტა, ამ გზით გაგზავნილი ყოველი შეტყობინება ავტომატურად ხდება მოწყვლადი. შეტყობინებები ვისთვისაცაა მოწყვლადი, უმეტეს შემთხვევაში არიან უცნობი ადამიანები, სისტემის ადმინისტრატორები რომელთაც დრო არ აქვთ უცხო ადამიანების პირადი შეტყობინებების საკითხად. მაგრად რა მოხდება თუ შენ ხარ ვიღაც ადამიანის ან ადამიანთა ჯგუფის სამიზნე და შენ აგზავნი ბიზენს მეილს, მათ შეუძლიათ წაიკითხონ შეცვალონ ან გამოიყენონ ეს ინფორმაცია შენ საზიანოდ.

პგპ-ის მახასიათებლები

PGP დიდი უპირატესობა იმაში მდგომარეობს, რომ იგი უზრუნველყოფს უსაფრთხოების ოთხივე ასპექტს, კერძოდ: (1) კონფიდენციალურობას, (2) მთლიანობას, (3) აუთენთიფიკაციასა და (4) გაგზავნილი შეტყობინების ანულირებას.

ამასთანავე, იმისათვის, რომ PGP-ს ახასაითებდეს მთლიანობა, ავთენთიფიკაცია და ანულირება, იგი იყენებს ელექტრონული ხელმოწერის მეთოდს, უფრო კონკრეტულად, ჰეშ(hash) ფუნქციისა და ღია გასაღების(public key) დაშიფვრის მეთოდების კომბინაციას. რაც შეეხება კონფიდენციალურობის უზრუნველყოფას, ამისათვის პგპ-ის ფარგლებში სიმეტრიული (symmetric key) და ღია(public key) გასაღებების გაშიფვრის კომბინაცია.

როგორც უკვე ცნობილია, PGP-ის გამოყენება მეტად უსაფრთხოა, თუმცა ამასთანავე აღსანიშნია, რომ მისი მუშაობის სქემა საკმაოდ მარტივია. განვიხილოთ ნაბიჯები, რომლებიც მუშაობის პროცესში სრულდება:

თავდაპირველად გენერირდება საიდუმლო გასაღები(secret key) და ღია გასაღები(public key). საიდუმლო გასაღები არის შეტყობინების ადრესანტისთვის და ეს გასაღები უნდა ჰქონდეს მხოლოდ მას. ხოლო, რაც შეეხება, ღია გასაღებს, იგი არის ადრესატისთვის განკუთვნილი. ამის შემდეგ იწყება პირველი ბიჯი ხელის მოწერა. ადრესანტი აწერს ხელს მესიჯს თავისი საიდუმლო გასაღებით, იმის დასადასტურებლად, რომ ეს ნამდვილად მისი შეტყობინებაა.

(1) ხელმოწერა σ_m = SIGN(sk,m) სადაც sk არის საიდუმლო გასაღები(secret key).
(2) შემდეგ m იკუმშება ჰეშ(Hash) ფუნქციით და ხდება m`. ამ ბიჯშივე ხდება შეკუმშული შეტყჯობინება m`-ის კონკატენაცია მის ხელმოწერილ ვერსიასთან σ_m-თან.

მესამე ბიჯში გენერირდება ახალი სიმეტრიული გასაღები(symmetric key) k და შიფრავს მეორე ბიჯში მიღებულ შედეგს ანუ m`| σ_m.

(3) $c_m = E(k,m' |\sigma_m)$

მეოთხე ბიჯში ჩვენ ვშიფრავთ დაგენერირებულ სიმეტრიულ გასაღებს(symmetric key) ღია გასაღებით(public key).

(4) $c_k = E(pk, k)$.

საბოლოო ეტაპზე კი ჩვენი შიფრის დასრულებული ვერსია, წარმოდგენილია წინა ორ ეტაპზე მიღებული შიფრების კონკატენაციის შედეგად.

(5) $c = c_k \mid c_m$

სწორედ ამ სქემის გამო არის PGP ამ დროისთვის არსებული დაშიფვრის პროგრამებს შორის ყველაზე დაცული და უსაფრთხო. თუმცა, არსებობს მისი სხვა მხარეც, რის გამოც არ ვიყენებთ მას ყოველღიურად, მიუხედავად იმისა, რომ იგი ასეთ დაცულ სერვისს გვთავაზობს.

მინუსები და შეზღუდვები

სამწუხაროდ, PGP-ის აქვს როგორც ცალსახა მინუსები, ასევე შეზღუდვები, თუმცა ეს შეზღუდვები და მინუსები ერთმანეთთან მჭიდრო კავშირშია, ამიტომ განვიხილოთ ერთად, რომ მეტად გასაგები იყოს.

PGP-ზე საუბრისას, თავდაპირველად აუცილებლად უნდა აღინიშნოს, რომ ეს არაა მომხმარებელზე გათვლილი სისტემა. სისტემა ისეა შექმნილი და იმდენი ბიჯია შესასრულებელი შეტყობინების გასაგზავნად, რომ მომხარებელს ჭირდება საკმაოდ დიდი დრო და ცოდნა ამ ოპერაციის შესასრულებლად, თუმცა, თუ მომხმარებელს არ აქვს საკმარისი ცოდნა, უნარები და გამოცდილება, სავარაუდოა, რომ მან არათუ დიდი დრო მოანდომოს დაკისრებული დავალების შესრულებას, არამედ საერთოდაც ვერ გაართვას თავი. ამიტომაც მომხარებლების უმეტესობა ამჯობინებს გამოიყენოს ელექტრონული ფოსტის მარტივი სისტემა ყოველდღიური პირადი შეტყობინებებისთვის და ა.შ., მაგრამ როცა საქმე კომპანიების ოფიციალურ ბიზნეს მიმოწერას ეხება, აქ უკვე მომხმარებელს უწევს, გააკეთოს არჩევანი უსაფრთხოებასა და სისწრაფეს შორის და ბუნებრივია, აღარ არსებობს იმის ფუფუნება, რომ მოკლე დროში შესასრულებელი ოპერაცია იქცეს უპირატესად, ვიდრე უსაფრთხოება. ასეთ შემთხვევაში, საჭიროა დეველოპერთა ცალკეული ჯგუფის გამოყოფა, რომელიც შეძლებს და გააგზავნის შეტყობინებებს PGP -ს მეშვეობით. ეს გახლავთ ის ძირითადი ნაკლოვანება, რაც PGP-ის ახასიათებს.

ახლა კი განვიხილოთ მისი შეზღუდვები. მომხმარებელს რაგინდ დიდი სურვილი ჰქონდეს, რომ დაცული იყოს და იყენებდეს PGP-ის, მას საშუალება აქ გააგზავნოს შეტყობინება მხოლოდ მასთან, ვინც ასევე PGP-ის მომხარებელია. ამასთანავე, შეუძლებელია მომხმარებელმა გაიგოს, მისი შეტყობინება მივიდა თუ არა ადრესატამდე.

გარდა ამისა, PGP ის საიდუმლო გასაღები (secret key) უნდა იყოს დაცული და არახელმისაწვდომი. თუმცა მისი დაკარგვის შემდეგ თქვენ არ გაქვთ არანაირი ბერკეტი, რომ იქამდე გაუშიფრავი შეტყობინებები გაშიფროთ, ამის გამო შეიძლება ძალიან დაზარალდეთ, ამიტომ უნდა არსებობდეს, საიდუმლო გასაღების ასლი გაუთვალისწინებელი

შემთხვევებისთვის. აქვე თავს იჩენს ასლის შენახვის პრობლემა რადგან საიდუმლო გასაღები(secret key) უნდა იყოს დაცული.

ასევე, დიდი ორგანიზაციის შემთხვევაში საჭიროა, დიდი ფაილების დაშიფვრა ამაშიც აქვს PGP-ის შეზღუდვა. ამიტომ სხვა ხერხია მოსაფიქრებელი ამ დროს, მაგალითად ფაილის დაყოფა და ა.შ.

ამასთანავე, მომხარებელს არ შეუძლია შეამოწმოს, გახსნამდე მოსული შეტყობინება ხომ არ შეიცავს რაიმე მავნე ფაილს, ვირუსს. ამ პრობლემის გადაჭრის ერთ-ერთი საშუალებაა, შეტყობინება გაიხსნას ჯერ სატესტო გარემოში(ვირტუალური მანქანა,sandbox) და შემოწმების შემდეგ თუ ფაილი ან შეტყობინება დავირუსებული არაა, გადავიტანოთ რეალურ გარემოში. ეს პრობლემას არ წარმოადგენს კომპანიებისთვის, მათ ამისთვის საკმარისი შესაძლებლობა, უნარი და რესურსი გააჩნიათ, მაგრამ როცა ვლაპარაკობთ ერთეულ მომხმარებლებზე, მათთვის ეს მოუხერხებელი და არაპრაქტიკული მიდგომაა.

და ბოლოს, რასაც მინდა შევეხო, ესაა ანონიმურობა. ჩვეულებრივი ელექტრონული შეტყობინების გამოყენებისას თქვენ შეგიძლიათ გამოიყენოთ, VPN მაგალითად რომ დამალოთ თქვენი ადგილმდებარეობა. PGP -ის გამოყეენებისას კი ადრესატმა ზუსტად იცის ვისგან და შეუძლია დაადგინოს, საიდან მიიღო შეტყობინება.

რომ შევაჯამოთ, არსებობს უამრავი აპლიკაცია- სხვადასხვა სისტემისთვის ინდივიდუალური, არსებობს ელქტრონული შეტყობინებები, რომელთაც PGP ჩაშენებული აქვთ მაგალითად ProtonMail. თუმცა უამრავი აპლიკაციისა და სხვადასხვა ელექტრონული შეტყობინების არსებობის მიუხედავად, ჩვეულებრივ მომხარებელს უფრო მეტად აბნევს, უჭირს გადაწყვეტილების მიღება, რომელ აპლიკაციას ენდოს და რომელს- არა, იმის გათვალისწინებით, რომ არსებობს ამდენი შეზღუდვა. სწორედ ამ და სხვა მიზეზების გამო, არსებობს მრავალი საკითხი, რაზე მუშაობაც და გამოსწორებაც საჭიროა PGP-ს ფუნქციონირებისა და გამოყენებადობის დასახვეწად.

გამოყენებული ლიტერატურა

1. Harry Halpin, “SoK: Why Johnny Can’t Fix PGP Standardization”, *ACM, 2020.*
2. Garfinkel, Simson. *PGP: Pretty Good Privacy*. United States of America: O’Reilly & Associates, Inc., 1995

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 11-17 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

SECURE CLOUD COMPUTING INFORMATION SYSTEM FOR CRITICAL APPLICATIONS

Sergiy Gnatyuk, NAU Cybersecurity R&D Lab
National Aviation University, Kyiv, Ukraine
Vitaliy Kishchenko, NAU Cybersecurity R&D Lab
National Aviation University, Kyiv, Ukraine
Andriy Tolbatov, NAU Cybersecurity R&D Lab
National Aviation University, Kyiv, Ukraine
Yuliia Sotnichenko, NAU Cybersecurity R&D Lab
National Aviation University, Kyiv, Ukraine

ABSTRACT: The usage of cloud computing has gained a significant advantage due to the reduced cost of ownership of IT applications, extremely fast entry into the services market, as well as rapid increases in employee productivity. Everything can be implemented in the cloud service: from data storage to data analysis, applications of any scale or size. Employees also implement their own cloud applications for work, contributing to the development of their own cloud culture (BYOC). In addition, the use of cloud services is now available not only for large enterprises, but also for companies in medium and small businesses, which makes cloud technologies one of the main environments for the operation of their information systems. However, such an increase in the efficiency of working with cloud technologies has led to increased attention to the problems of cyber threats, the growth of which is inseperably linked with the growth of IT technologies. A cloud service user can deploy their own applications, build their infrastructure, or simply process data, but in any case, they trust their confidential data to the cloud service provider and want to be sure that their data is secure. Providing information security IS in a cloud environment is the responsibility of the provider, and therefore their systems must meet a number of requirements of both national and international law and international recommendations. Therefore, the main scientific and technical problem can be formulated as follows: data security may be compromised and there is a risk of mass data loss by many users due to the possibility of conducting cyber threats in cloud services. Because information is not only stored in the cloud, but is also processed, users must be confident in the security and availability of their data. The solution to this problem can be provided by using various methods of cyber threat detection, IDS / IPS systems, cyber incident response modules, etc.

KEYWORDS*: information technology, cloud computing, security, critical applications, cyber attack.*

INTRODUCTION

Cyber threat is any circumstance or event that may cause a breach of information security policy and / or damage to an automated system. The main purpose of cybersecurity is to prevent the implementation of existing cyber threats, ie to prevent the implementation of any cyber attacks, which are the sources of the following risks [1-4]:

– *Loss of intellectual property.* Analysis, conducted by the Skyhigh company, has found that more than 20 percent of the data stored in enterprises contains confidential information, including intellectual property. Most businesses now use multi-tier cloud services, where their data is stored on servers that are also used to provide similar services to other organizations. There are also several providers of cloud storage solutions that do not have modern data protection and security tools. Any security breaches encountered by the cloud service provider compromise confidential data.

– *Violation of compliance and regulations.* There are several regulatory requirements and compliance requirements for businesses in all markets and territories. This means that businesses have to make sure that their cloud storage and application providers take care of these regulations. Also, for businesses that promote the concept of Bring Your Own Device and Bring Your Own Cloud, make it difficult to comply with these standards. Any security breaches and data leaks can lead to severe penalties and loss of brand value.

– *Compromising credentials and authentication.* Poor certification and key management, weak passwords, and poor authentication are the causes of frequent data breaches in cloud applications: businesses struggle with authentication management issues because they reflect permissions and privileges for user roles; businesses very often do not delete or change user access when he / she resigns or changes role; the lack of multi-factor authentication is due to the compromise of 80 million customer records, and some cloud programs still do not have such authentication; Developers are often to blame for leaving cryptographic keys and credentials in the open source, making them free for analysis on portals such as GitHub.

– *API threats.* Most cloud solution providers offer their APIs for enterprise IT teams to help them with cloud services, management and monitoring. This makes the security and availability of cloud solutions dependent on the security of the API. Weak APIs expose cloud applications to the risks of accountability, confidentiality, integrity, and availability. For most businesses, such APIs remain the most vulnerable because they are fairly easily accessible directly through the Internet. Strict security-based intrusion testing and security checks are key elements in ensuring that these APIs are permanently protected from cyberattacks.

– *Hacking accounts.* Software exploits, phishing and fraud still are widespread occurrences. Cloud services are also susceptible to this kind of damaging cyber attacks, because cybercriminals have wider range of abilities to control user activities in public cloud services. In addition, there are two of the most effective measures for businesses cloud data and applications protection: to prevent users from accessing passwords and requisites of user accounts; ensure that multifactor authentication schemes are available where possible. Avoiding account data loss is the first step in protecting your cloud software from phishing and other breaches.

– *Improper usage of cloud services.* Cloud services can be misused, from using cloud resources to access encryption keys, to launch DDoS attacks on enterprise servers. The use of the enterprise's cloud resources for cybercrime has the following consequences: low availability of cloud systems; the impact of legal obligations in the form of lawsuits from influential parties; serious loss of reputation.

REVIEW OF RELATED PAPERS

As mentioned earlier, cloud computing has considerable advantages over conventional “physical” computing [5-6]. However, this advantage - only for the direct user, because no matter what the user does - deploys its own infrastructure, launches applications, or simply stores and processes data – for him it will all be on remote servers, i.e. in the “cloud”. However, for a cloud computing service provider, the entire process from system construction to direct service delivery and maintenance takes place at the physical and hardware levels [7-9]. Therefore, problems at the software level include failures at the hardware level. The task is complicated when IoT (Internet of Things) tools are used in real production, and traditional approaches to cybersecurity cease to work effectively. Solving these problems will help to create conditions for a new corporate culture and technology for automatic protection of data, operations and applications [10-12]. It is an indisputable fact that the number and sophistication of cyberattacks is growing every year. According to a report by Alert Logic and Crowd Research Partners, more than half of security professionals in large companies predict the possibility of at least one cyberattack on their company. So it is not surprising that the business budget for these needs has grown by an average of 21%. The same report, based on a survey of 350,000 experts and experts around the world, says that today most attention is paid to the security of cloud infrastructure (33% of costs), cloud applications (28%), another 23% of costs go to increase staff qualifications.

The process of cyberattack prevention can be divided into two streams - descending and ascending. The first involves building a mechanism for classifying corporate data and add-ons by security and prescribing levels for each security protocol. The second is responsible for the use of tools and technologies to detect hacking attempts. Vulnerabilities are usually there. It can be taken for granted that the company is not able to protect itself from hacking the most "persistent" hackers. This means that all resources must be thrown to deter attacks until they cause irreparable damage to the data. In any situation, effective work with cyberattacks depends on proper planning. There should be

an effective method for instant identification of the source of the threat and a plan for its isolation, prevention of further spread [13-14].

SECURE CLOUD COMPUTING INFORMATION SYSTEM

Cloud environment in which the method of detecting cyber threats will be introduced.

The technology architecture is based on the recommendations of Cisco, which has developed its own progression of evolution of "cloud" data centers:

1) consolidation and aggregation of data center assets;

2) abstraction, is a key phase, because the assets of the data center are abstracted from the services that are actually supplied;

3) automation, which is capitalized on consolidated and virtual aspects, fast backup services and automatic modeling;

4) the interaction of the corporate “cloud” with the public;

5) the final phase - "inter-cloud", which replaces the existing types of "clouds".

Before building the architecture of the “cloud” data center, it is necessary to identify the system of components of the data center blocks in the basis of "cloud" architectures.

10 Gigabit Ethernet. The data center is designed with a high density of virtual machines that are combined with a large number of processors. From a network perspective, the growth of virtual machines and the concentration of cores will facilitate the transition to 10 Gigabit Ethernet as a necessary mechanism for providing servers. Specific benefits of the transition include: real-time policy configuration; mobile security and network policy, which is replaced by the policy of the virtual machine during its mobility; continuous operation of management models that establish management and operation of the environment for virtual machines and physical servers.

Unified Fabric, which gives all servers (physical or virtual) access to the local network, storage network, and IPC network, allowing them to be more integrated into the customer's network to increase efficiency and cost savings.

Unified Computing. The unified structure allows you to fully virtualize a "cloud" data center with pools of computer, network, and storage resources using unified computing. Unified Computing covers silos in a classic data center, allowing more efficient use of infrastructure in a fully virtualized environment, and creates a single architecture using standard technologies that ensure compatibility and investment protection. The Unified Computing system combines computing and network capacity, storage system access and virtualization resources in a scalable modular design that is managed as a single energy-saving system. This system can be managed using the built-in control system, in the Unified Computing platform.

In Fig. 1 shows the technological architecture, which presents the “cloud” data center of the next generation. The diagram shows examples of component blocks for the data center. In general, the completed architecture contains not only components of the structure, but also is regulated by different types of service and regulatory requirements.

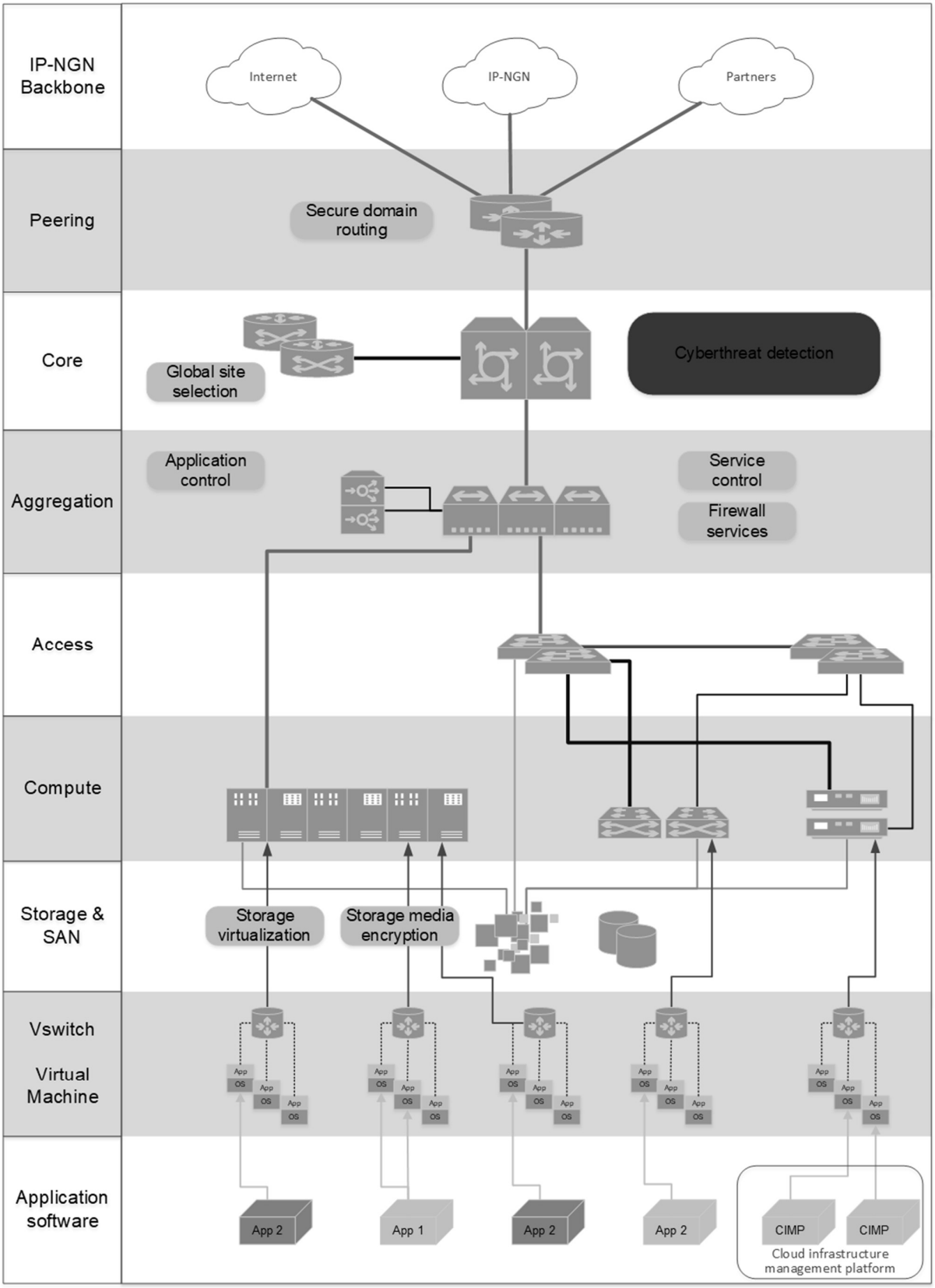


Fig. 1. Technological architecture of the data center based on Cloud Computing technology

The architectural model offers 9 tiers of the data center network:

- application software;
- virtual machine and distributed virtual switch (virtual machine, VSwitch);
- storage and storage networks (storage, SAN);
- calculation (compute);
- access;
- aggregation;
- core, where there is also a module for detecting cyber threats;
- peering;
- basics of the Internet (IP-NGN backbone).

Each subsequent level is connected to the previous one by a certain type of connection. From the application software tier to the Virtual machine & VSwitch tier, the App to HW / VM connection, then the virtual machine data, is fed to the distributed VSwitch virtual multilevel switches.

Data from the storage network (SAN) and application data from VSwitch are then transmitted to the computing tier using 4G FC (fiber chanel) and VSwitch to HW, respectively. The results of the calculations are sent to the access tier via 4G FC, 10G FCoE (Fiber Channel over Ethernet) and 1G Ethernet, and from this tier to the level of aggregation via 10G Ethernet. On this tier the control of applications and services is executed, and firewall services (IDS, SSL, anti-DDoS) are installed.

The next tier is the core, which also uses global location and cyber threat detection procedures. If a threat has been detected, the user and the system as a whole will be notified and appropriate action will be taken. At the peer-to-peer tier (the interconnection of individual networks to exchange traffic between users on each network), the domain is routed. The last tier is the Internet, using the 10G Ethernet connection type.

The downward movement of traffic and data occurs in the reverse order to that described above. Other key software components include: business applications for service tools; service management programs for service search, display and matching; SLA measurement, billing applications for reporting; web and business logic hosting applications. Key components of facilities: power supply and cooling of facilities; elements of the physical structure of data center components; racks and cable components.

Along with the technological component of the architecture of data centers, an important place is also occupied by the issue of trust in the infrastructure model of “cloud” computing. The key to gaining an advantage from the cloud is to establish a trust approach that begins with the establishment of such attributes in cloud architecture.

Trust in a "cloud" data center is based on several basic concepts:

1. Security: traditional data issues and resource access control, encryption and incident detection.

2. Control: the ability of the enterprise to directly manage the processes of deployment of applications.

3. Compliance and maintenance at the management level: compliance with general requirements.

4. Timely detection of cyber threats, prevention of intrusions, blocking cyberattacks.

Fig. 2 shows the structure of a protected data center based on Cloud Computing technology from the point of view of security, namely the models of threats and measures that need to be taken to minimize risks. The structure also reflects full control, compliance with requirements and agreements on the level of services.

The key idea of this model is that information security should not be secondary or simply part of the overall security, it should be disseminated and implemented at all levels of the architecture.

The threat profile (Threat profile) consists of such elements as:

- service disruption;
- data leakage;
- data disclosure;
- data modification;
- identity theft and fraud;

– intrusion.

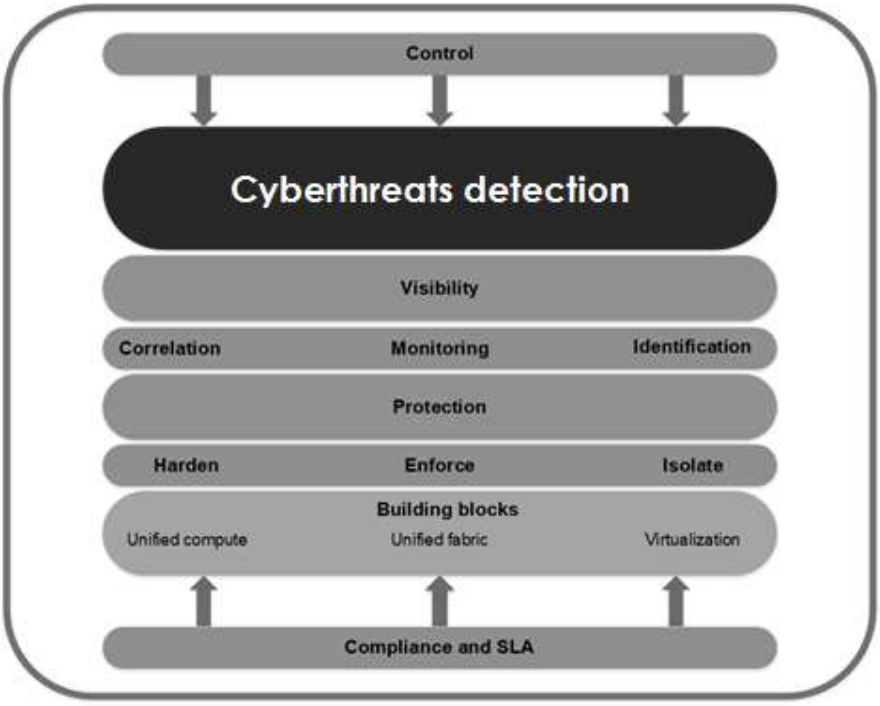


Fig. 2. The structure of a secure data center based on Cloud Computing technology

As can be seen from Fig. 2 detection of cyber threats is one of the most important tasks in the system of information security of cloud environments.

CONCLUSIONS

In this paper the analysis of the existing models, systems and methods of detecting cyber threats was conducted, which allowed to identify their main shortcomings, namely: lack of data on experimental research, the impossibility of its use in cloud services (for the most part), some MVCs do not implement real-time cyber threat detection.

A model of cloud service has been developed, which through the use of technological architecture, high-speed communication, unified structures and calculations allows to ensure the security of cloud service based on Cloud Computing technology and conduct appropriate simulations.

REFERENCES

1. R. Abidar, K. Moummadi, F. Moutaouakkil, H. Medromi, Intelligent and Pervasive Supervising Platform for Information System Security Based on Multi-Agent Systems, International review on computers and software. – 2015. – Vol. 10, Issue 1. – p. 44–51.

2. The 6 Major Cyber Security Risks to Cloud Computing [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://www.adotas.com/2017/08/the-6-major-cyber-security-risks-to-cloud-computing/

3. Google Security Whitepaper for Google Cloud Platform [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://habrahabr.ru/post/183168/

4. Data Mining for Network Intrusion Detection / P. Dokas, L. Ertoz, V.Kumarhttps // Recent Advances in Intrusion Detection. – 2014. – Vol. 15(78). – P. 21-30.

5. Ahmed P. An intrusion detection and prevention system in cloud computing:A systematic review / P. Ahmed // Journal of Network and Computer Applications. – 2016. – Vol. 11. – P. 1-18.

6. Anderson J.P. Computer Security Threat Monitoring and Surveillance / James P. Anderson // Technical Report Contract. – 1982. – Vol. 36. – P. 179-185.

7. Carl G, Kesidis G, Brooks RR, Rai S. Denial-of-service attack-detection techniques. Internet Computing, IEEE, 2006;10:82–9

8. How to build physical security into a data center [Електронний ресурс] / S.D. Scalet. – Режим доступу: World Wide Web. – URL: http://www.csoonline.com/article/2112402/physical-security/physical-security-19-ways-to-build-physical-security-into-a-data-center.html?page=3

9. Al-Mamory S, Zhang H. New data mining technique to enhance IDS alarms quality. Journal in Computer Virology 2010;6:43–55

10. Breaking down what's in your cloud SLA [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://searchcloudcomputing.techtarget.com/essentialguide/Breaking-down-whats-in-your-cloud-SLA

11. ISO/IEC 27035:2011 – Information technology – Security techniques – Information security incident management, 2011. – 69 p.

12. Antonopoulos N. Cloud Computing: Principles, Systems and Applications / N. Antonopoulos // Springer Science Business Media. –2010. – Vol. 13(6). – P. 26-38.

13. Byrski A, Carvalho M. In: Bubak M, van Albada G, Dongarra J, Sloot P, editors. Agent-Based Immunological Intrusion Detection System for Mobile Ad-Hoc Networks Computational Science—ICCS 2008, 5103. Berlin/Heidelberg: Springer; 2008. p. 584–93.

14. AWS Global Infrastructure [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://aws.amazon.com/about-aws/global-infrastructure/?nc1=h_ls

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 18-21 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

„PROMETEI“ - ახალი „ბოტნეტი“ კიბერდანაშაულისთვის”
“PROMETEI” – THE NEW “BOTNET” FOR CYBERCRIME”

ნათია ფილაშვილი _ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, IV კურსის სოციოლოგიის მიმართულების სტუდენტი.
Natia Pilashvili _ Ivane Javakhishvili Tbilisi State University, Sociology_Junior;
მარიამ კიკლიაშვილი _ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, IV კურსის სოციოლოგიის მიმართულების სტუდენტი.
Mariam Kikliashvili - Ivane Javakhishvili Tbilisi State University, Sociology_Junior;

ანოტაცია: XXI საუკუნეში, სწრაფი ტექნოლოგიური პროგრესის პარალელურად, გამოუვლენელი და გაუხსნელი დანაშაულების ყველაზე მზარდი ტენდენცია კიბერდანაშაულის კუთხით აღინიშნება, რომელსაც ხშირად „მომავლის დანაშაულსაც“ უწოდებენ. მავნე პროგრამები, რომლებიც კიბერდანაშაულის ერთ-ერთი მთავარი მექანიზმია, თითოეულ ჩვენგანს მათ მსხვერპლად ადვილად გვაქცევს. დღესდღეობით კრიპტოვალუტა ერთ-ერთი უდიდესი ინტერესის საგანია, ვინაიდან იგი სწრაფი ზრდადობით გამოირჩევა და უფრო და უფრო მეტ ქვეყანაში იმკვიდრებს ადგილს. სწორედ, „Prometei“ არის კრიპტოვალუტის მოსაპოვებლად გამოყენებული სრულიად ახალი კიბერდანაშაულის იარაღი, რომლის საშუალებითაც უამრავი ადამიანი ფინანსურად დაზარალდა.

ANNOTATION: In the 21st century, with the rapid advancement of technology, there is a growing trend of undetected and unsolved crimes in cybercrime, often referred to as the "crime of the future". Malware, which is one of the main mechanisms of cybercrime, makes it easy for each of us to fall victim to them. Cryptocurrency is one of the biggest topics of interest today, as it is growing rapidly and is gaining ground in more and more countries. „Prometei“ is a completely new cybercrime tool used to mine for cryptocurrency, and has already financially affected many people.

საკვანძო სიტყვები: *კიბერდანაშაული, მალვეარი, „ბოტნეტი“,„Prometei“, კრიპტოვალუტა.*

KEYWORDS: *cyber crime, malware, botnet "Prometei", crypto currency*

„ბოტნეტი“ წარმოადგენს ინტერნეტ ქსელში ჩართულ კომპიუტერთა ერთობლიობას, რომელთა თავდაცვის უნარი დარღვეულია. მათი მართვა მესამე პირის მიერ დისტანციურად ხდება. „ბოტი“(bot) - ასე უწოდებენ დაინფიცირებულ მოწყობილობას. მოწყობილობის დაინფიცირება ხდება კომპიუტერულ ქსელში მალვეარის შეჭრით, აგრეთვე იგი ცნობილია, როგორც მავნე პროგრამა. „ბოტნეტის“ მართვა მეტწილად IRC(Internet Relay Chat)-იდან ხდება, თუმცა მისი მართვა შესაძლებელია ვებგვერდიდანაც. საზიანო პროგრამების გამოყენების შემთხვევაში კომპიუტერები შესაძლოა, შეიტყუონ ბოტნეტში, მას შემდეგ, რაც მომხმარებელი ეწვევა დავირუსებულ საიტს და გადმოტვირთავს ამა თუ იმ ინფორმაციას. საზიანო ვირუსი შესაძლოა მიმაგრებული ფაილის სახითაც აღმოჩნდეს კომპიუტერში.

ტერმინ „ბოტნეტის“ გამოყენება შეგვიძლია კომპიუტერების ნებისმიერ ჯგუფზე, მაგალითად ასეთივეა IRC ბოტი. „ბოტ“-ის მფლობელს შეუძლია ჯგუფის დისტანციური კონტროლი, IRC-ის საშუალებით უმთავრესად კრიმინალური მიზნებისთვის. სერვერი ცნობილია (C&C) სერვერის სახელწოდებით. „ბოტის“ გაშვება ხდება მალულად, და გამოიყენება ფარული გზები (მაგ. ტვიტერი ან მესიჯი) კომუნიკაციის დასამყარებლად C&C სერვერთან. დამნაშავის ხელში გადადის რამდენიმე სისტემა სხვადსხვა ხელსაწყოს მეშვეობით. ახალი ”ბოტები” ავომატურად ასკანერებენ სისტემაში არსებულ მონაცემებს უადვილდებათ დანაშაულის ჩადენა, თუკი მომხმარებლის სისტემაში არასაიმედო პაროლები არსებობს.

რაც უფრო მეტი ინფორმაციის მოპოვებას შეძლებს ”ბოტი” სისტემიდან, მით უფრო ფასეული გახდება ”ბოტნეტის” მფლობელისთვის. კომპიუტერული სისტემიდან მონაცემების მოპარვას ”ბოტნეტში” ჩართვის შედეგად ასევე ეწოდება „Scrumping”-იც. „ბოტნეტს” უმთავრესად ჰყავს ერთი ან რამდენიმე მაკონტროლებელი პირი, რომელთაც არ გააჩნიათ ერთგვარი იერარქია, მათი ურთიერთობა დამყარებულია ინდივიდუალურ მეგობრულ კავშირებზე. 2006 წლის მონაცემებით მსგავსი ქსელის საშუალო ზომა შეადგენდა 20 000 კომპიუტერს, თუმცა ამჟამად ოპერირებენ უფრო ფართო ქსელებიც.

„ბოტნეტის“ შექმნის 4 საფეხური:

1. „ბოტნეტის“ მაკონტროლებელი პირი გზავნის ვირუსს/ვორმს და მათი საშუალებით აინფიცირებს მომხმარებელთა კომპიუტერებს.

2. „ბოტი“ შედის კონკრეტულად C&C სერვერზე.
3. სპამერი ოპერატორისგან იღებს „ბოტნეტის“ სერვისებს.
4. სპამერი ოპერატორს უგზავნის შეტყობინებას და გასცემს სპამ შეტყობინების გაგზავნის ბრძანებას.

„ბოტნეტის“ გამოყენება სხვადასხვა მიზნებისთვის ხდება, ასეთი შესაძლოა იყოს, პაროლების მოპოვება, საკრედიტო ბარათების ნომერთა ხელში ჩაგდება, აპლიკაციების მოპარვა და სახელმწიფო ქსელებზე კიბერ შეტევებიც კი.

Cisco Talos Intelligence Group არის მსოფლიოში ყველაზე მასშტაბური კომერციული საფრთხეების სადაზვერვო ჯგუფი, რომელიც შედგება მსოფლიო დონის მკვლევრების, ანალიტიკოსებისა და ინჟინრებისგან. სწორედ ამ სადაზვერვო ჯგუფმა აღმოაჩინა ახალი ბოტნეტი, სახელწოდებით - Prometei, რომელიც 2020 წლის მარტიდან განსაკუთრებით აქტიური გახდა და ძირითადად ორიენტირებულია კრიპტოვალუტის მოპოვებაზე.

კრიპტოვალუტა წარმოადგენს ელექტრონულ ფულს, რომლის საფუძველიცაა „ბლოკჩეინის სისტემა“ და იგი სახელმწიფოსა თუ ბანკებიდან დამოუკიდებლად ოპერირებს. თანამედროვე ტექნოლოგიების მეშვეობით მათი ღირებულება დღითიდღე იზრდება, შესაბამისად სხვადასხვა პლატფორმებზე მიმდინარეობს ვაჭრობა მათი საშუალებით. ამ ვალუტას ფიზიკური სახე არ გააჩნი, მასთან დაკავშირებული ნებისმიერი ოპერაცია ხორციელდება ინტერნეტის მეშვეობით.

Prometei-ს მსხვერპლი გახდნენ აშშ-ს, ბრაზილიის, პაკისტანის, ჩინეთის, მექსიკის და ჩილეს მოქალაქეები. ოთხი თვის შემდეგ „ბოტნეტის“ მაკონტროლებლებმა მოიპოვეს დაახლოებით 5000$, საშუალოდ 1,250 აშშ დოლარი თვეში.

საერთო ჯამში, მკვლევრებმა 15-ზე მეტი გავრცელების ტექნიკა დაითვალეს Prometei–ში. ყველა მათგანს აკონტროლებს მთავარი მოდული, რომელსაც შეუძლია გაშიფროს (RC4)მონაცემები იქამდე, ვიდრე იგი HTTP-ით გააგზავნის მართვის სერვერზე.

ბოტნეტი იპარავს პაროლებს Mimikatz-ის შეცვლილი ვერსიის საშუალებით, რის მერეც ეს პაროლები Spreader მოდულს გადაეგზავნება SMB-ს ანალიზისა და ავთენტიფიკაციისათვის. იმ

მშემთხვევაში თუ ეს გზა არ იმუშავებს, გამრავლებისთვის გამოიყენება EternalBlue-ს ექსპლოიტი.

ყოველი ახალი კიბერდანაშაულის შემთხვევა კარგად გვიჩვენებს, თუ როგორი საფრთხის წინაშე დგას თითოეული ჩვენგანი ციფრულ ტექნოლოგიასთან და სოციალურ ქსელებთან გადაჯაჭვული ცხოვრების გამო, რაც დღევანდელობის განუყოფელი ნაწილია. საჭირო და მნიშვნელოვანია ეს მაგალითი იყოს ჩვენთვის, იმისთვის, რომ გამოვიჩინოთ უფრო მეტი სიფრთხილე ინტერნეტ სივრცეში ყოფნის დროს, რათა არ გავხდეთ მავნე პროგრამების მორიგი მსხვერპლი.

ბიბლიოგრაფია

1. “Prometei botnet exploits Windows SMB to mine for cryptocurrency” By Charlie Osborne for Zero Day | July 22, 2020 www.zdnet. com https://www.zdnet.com/article/prometei-botnet-is-infecting-machines-to-mine-for-cryptocurrency/
2. “Botnets “ Published under Glossary www.enisa.europa.eu https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 22-28 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

TLS 1.3 ახალი პროტოკოლი ახალი შესაძლებლობებით
TLS 1.3 NEW PROTOCOL WITH NEW POSSIBILITIES

ლუკა ნაჭყებია, კიბერუსაფრთხოების მეცნიერთა ასოციაცია (SCSA)
L. Nachkebia Scientific Cyber Security Association(SCSA)
ნოდარ უგლავა, კიბერუსაფრთხოების მეცნიერთა ასოციაცია (SCSA)
N. Uglava Scientific Cyber Security Association(SCSA)
ქეთევან გრძელიძე, კიბერუსაფრთხოების მეცნიერთა ასოციაცია (SCSA)
Q.Grdzelidze, Scientific Cyber Security Association(SCSA)

აბსტრაქტი: დღესდღეობით TLS პროტოკოლები გამოიყენება თითქმის ყველა აპლიკაციაში. ის წარმოადგენს ვებ ბრაუზერს (კლიენტი) და ვებგვერდს (სერვერი) შორის მონაცემთა გადაცემის უსაფრთხოების უზრუნველყოფის ყველაზე ხშირად გამოყენებად მეთოდს. წინამდებარე სტატიაში განხილულია TLS 1.2-ის და TLS 1.3-ის ძლიერი და სუსტი მხარეები, მათი უსაფრთხოების სისუსტეები. სტატიის დასკვნითი ნაწილი შეეხება TLS 1.3-ის ნაკლოვანებების თავდამსხმელების მიერ გამოყენების შესაძლებლობებს.

ABSTRACT: Nowadays, TLS protocols are being used in almost every application. It is the most used method for ensuring secure communication and transfer of data between web-browser (client) and web-page (server). In the present paper the strentghs and weaknesses of TLS 1.2 and TLS 1.3 and their security concerns are discussed. The final part of the paper addresses the matter, how the hackers can use TLS 1.3 shortcomings for their advantage.

საკვანძო სიტყვები: *TLS 1.3, უსაფრთხოების პროტოკოლი, TLS 1.2, უსაფრთხო კომუნიკაცია*
KEYWORDS: *TLS 1.3 security protocol, TLS 1.2 secure communication*

Transport Layer Security (TLS) წარმოადგენს კრიპტოგრაფიულ პროტოკოლს, რომელიც შექმნილია ვებ-ბრაუზერებსა და სერვერებს შორის კომუნიკაციის უსაფრთხოების უზრუნველსაყოფად. დღესდღეობით TLS პროტოკოლები გამოიყენება თითქმის ყველა აპლიკაციაში. მეორეს მხრივ, SSL წარმოადგენს პროტოკოლს, რომელიც გამოიყენება ვებ-ბრაუზერებსა და სერვერებს შორის დაშიფრული კომუნიკაციის დასამყარებლად. SSL გადაცემული მონაცემების დასაშიფრად იყენებს.
ის წარმოადგენს ვებ ბრაუზერს (კლიენტი) და ვებგვერდს (სერვერი) შორის მონაცემთა გადაცემის უსაფრთხოების უზრუნველყოფის ყველაზე ხშირად გამოყენებად მეთოდს. ის უზრუნველყოფს რომ კომუნიკაციის ორივე მხარეს არსებული მხარეები იყვნენ ავთენტურები და ასევე, უზრუნველყოფს მონაცემთა მთლიანობას მათი დაშიფვრის გზით.

არსებობს TLS-ის 1.0, 1.1., 1.2 და 1.3 ვერსიები:

- TLS 1.0 გამოქვეყნდა 1999 წელს RFC 2246-ის სახელით.
- TLS 1.1 გამოქვეყნდა 2006 წელს RFC 4346-ის სახელით.
- TLS 1.2 გამოქვეყნდა 2008 წელს RFC 5246-ის სახელით[1].
- TLS 1.3 ოფიციალურად გამოქვეყნდა 2018 წელს RFC 8446-ის სახელით.
-

ცნობილია, რომ TLS 1.0 და TLS 1.1 წარმოადგნენ ადვილად მოწყვლად პროტოკოლებს, ამასთან 1.2 და 1.3 ითვლება ბევრად უსაფრთხო პროტოკოლებად და შესაბამისად,

[1] "TLS 1.2 vs TLS 1.1 - KeyCDN Support," October 4, 2018. https://www.keycdn.com/support/tls-1-2-vs-tls-1-1.

რეკომენდებულია მათი გამოყენება. მიუხედავად იმისა, რომ 1.2-ს გააჩნია უსაფრთხოების პრობლემები, მისი გავრცელებადობის და სისტემებთან თავსებადობის გათვალისწინებით, დღესდღეობით მას არსებულ პროტოკოლებს შორის ყველაზე მეტი მომხმარებელი ყავს.

ამასთანავე, უსაფრთხოების საკითხებიდან გამომდინარე, 2020 წლიდან Apple, Google, Microsoft და Mozilla-მ შეწყვიტეს TLS 1.0 და TLS 1.1-ის გამოყენება და მხარდაჭერა.

დღეს TLS 1.3-ის სრული და ნაწილობრივი გამოყენების მაჩვენებელი მსოფლიოში დაახლოებით 89.02%-ია[2], ხოლო TLS 1.2-ის მაჩვენებელი 97.91%-ს უტოლდება[3].

გრაფიკი 1. TLS 1.2 და TLS 1.3-ის გამოყენების შესახებ მონაცემები[4]

TLS 1.2

როგორც ზემოთ აღვნიშნეთ, TLS 1.2 დღესდღეობით წარმოადგენს ყველაზე გავრცელებულ პროტოკოლს. თუმცა, ეს არ ნიშნავს, რომ მას არ აქვს პრობლემები. TLS 1.2 კვლავაც აქვს შედარებით მოძველებული კრიპტოგრაფიული ალგორითმების მხარდაჭერა, რაც უფრო მოწყვლადს ხდის მას სხვადასხვა ტიპის თავდასხმებისათვის. მაგალითისთვის *Zombie POODLE attack.* ამ თავდასხმის დროს მეცნიერებმა გამოავლინეს ორი ახალი სისუსტე, რომელიც TLS 1.-2ზე POODLE-ს ტიპის განხორციელების საშუალებას. ამ შემთხვევაში, თავდამსხმელი იყენებს CBC-დაშიფვრის მეთოდის სისუსტეს, რომელიც იძლევა Man-in-the-middle თავდასხმის განხორციელების შესაძლებლობას იმ სისტემებზე, რომლებიც ჯერაც იყენებენ დაშიფვრის მოძველებულ მეთოდებს.

2 Can I use... Support tables for HTML5, CSS3, etc, September 24, 2020, https://caniuse.com/#feat=tls1-3
3 Can I use... Support tables for HTML5, CSS3, etc, September 24, 2020, https://caniuse.com/#search=1.2
4 Can I use... Support tables for HTML5, CSS3, etc, September 24, 2020, https://caniuse.com/#search=1.2, Can I use... Support tables for HTML5, CSS3, etc, September 24, 2020, https://caniuse.com/#feat=tls1-3

POODLE და სხვა ტიპის თავდასხმების შემდგომ, გარკვეულწილად მოხდა ამ ნაკლოვანებების აღმოფხვრა. თუმცა, მომხმარებელთა გარკვეული ნაწილს კვლავაც აქვს ძველი პროტოკოლების მხარდაჭერა, ვინაიდან ეს ხელს უწყობს ძველი ვებ-გვერდების შენარჩუნებასა და თავიდან ირიდებს ვებ-გვერდებიდან ძველი მომხმარებლების დაბლოკვას. ეს, თავის მხრივ, ნიშნავს, რომ პრობლემები და სისუსტეები კვლავას რჩება სისტემებში და შესაძლებელია მათი გამოყენება.[5]

გარდა კოდში არსებული პრობლემებისა, TLS 1.2 მის შემდგომ ვერსიასთან შედარებით არის უფრო ნელი. უმეტეს შემთხვევაში მონაცემთა დაშიფვრა გამოიყენებოდა კონკრეტულ სისტემაში ავტორიზაციის ან საკრედიტო ბარათის მონაცემების გადაგზავნისთვის. ამავდროულად, სხვა ტიპის მონაცემები რჩებოდა ღიად ხელმისაწვდომი. შესაბამისად, ბოლო პერიოდში უფრო აქტუალური გახდა ინტერნეტის ტრაფიკის სრულად HTTPS-ში გადატანა, რაც მოხმარებლებს მეტად იცავს ე.წ. „eavesdropper“-ების და ინექციური თავდასხმებისაგან, თუმცა, როგორც ზემოთ აღინიშნა, ამ პროტოკოლის და შესაბამისად განხორციელებული პროცესების მინუსს წარმოადგენს მისი სიჩქარე.

კერძოდ, იმისათვის, რომ ბრაუზერი და სერვერი შეთანხმდნენ დაშიფვრის გასაღებზე, მათ სჭირდებათ კრიპტოგრაფიული მონაცემების გაცვლა. გაცვლა, იგივე „ხელის ჩამორთმევა“ TLS-ში მცირედად არის შეცვლილი 1999 წლის შემდეგ (მას შემდეგ რაც მოხდა სტანდარტიზება). „ხელის ჩამორთმევისათვის“ საჭიროა ბრაუზერსა და სერვერს შორის ორი დამატებითი წრის გავლა, მანამ სანამ მოხდება დაშიფრული მონაცემების გადაგზავნა (ან სანამ გაგრძელდება წინა კომუნიკაცია). შესაბამისად, აღნიშნულიდან გამომდინარე HTTP-სთან შედარებით HTTPS არის უფრო ნელი. ამ შეფერხებამ კი შესაძლოა ნეგატიური გავლენა იქონიოს იმ აპლიკაციებზე, რომელთა ორიენტირსაც წარმოადგენს სისწრაფე.

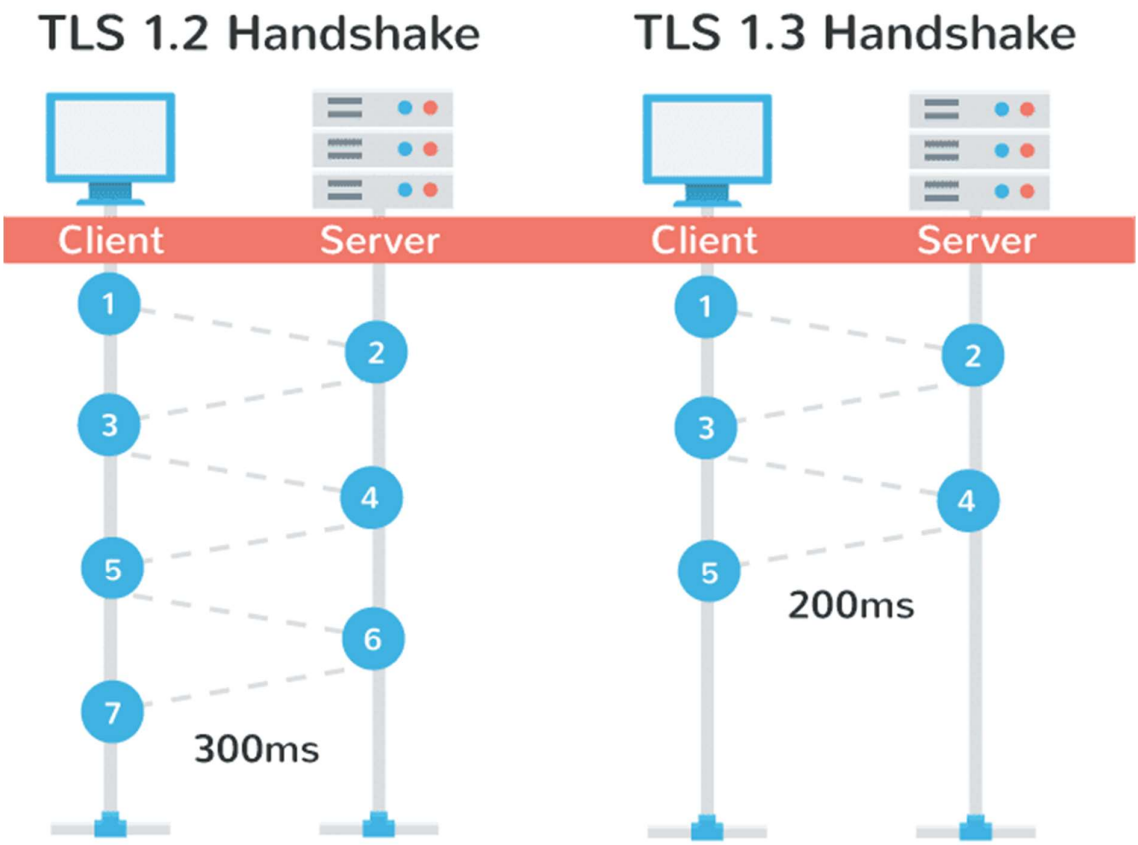
TLS 1.3-ს უპირატესობები TLS 1.2-თან შედარებით:

სისწრაფე

როგორც უკვე აღინიშნა, TLS 1.2 კავშირის დამყარებისას იყენებს უკვე მოძველებულ პროტოკოლს და არის შედარებით ნელი. მისგან განსხვავებით, TLS 1.3 პროტოკოლის მიხედვით, პირველადი კომუნიკაციის დამყარებისას საჭიროა მხოლოდ 1 წრის გავლა, რაც ბევრად ასწრაფებს და აადვილებს პროცესს. გარდა ამისა, TLS 1.3-ის პირობებში, თუ ვებ-გვერდი არის ახალი დახურული, ბევრად სწრაფად ხდება მასთან კავშირის გაგრძელება, რადგან აღარ არის საჭირო ხელახლა კომუნიკაციის დამყარება და „ხელის ჩამორთმევის“ პროცედურის გავლა, რადგან შესაძლებელია უკვე შეთანხმებული გასაღების გამოყენებით კომუნიკაციის გაგრძელება.

შესაბამისად, პროცესის გასაუმჯობესებლად TLS 1.3 კომუნიკაციიდან სრულად იღებს ხელის ჩამორთევის 1 წრეს. უმრავლეს შემთხვევაში, ახალი TLS 1.3 კავშირები მყარდება 1 წრის შემოვლით[6].

[5] Pollack Keren, “Leaving TLS 1.2 and Moving to TLS 1.3,” September 2, 2020, https://calcomsoftware.com/leaving-tls1-2-using-tls1-3/.
[6] “TLS 1.3,” EZ, accessed September 26, 2020, https://www.hcc-embedded.com/tls-1-3.



გრაფიკი 1: TLS 1.2 და TLS 1.3 პროტოკოლების „ხელის ჩამორთმევის“ პროცესი[7]

დაშიფვრის ახალი სქემა

მნიშვნელოვანია, რომ TLS 1.3 აღარ იყენებს იმ ალგორითმებს, რომლებიც TLS 1.2-ის პირობებში მიჩნეული იქნა თავდასხმებისადმი მოწყვლადად. შესაბამისად, გამოიყენება მხოლოდ ყველაზე უსაფრთხო ალგორითმები, როგორიცაა, მაგალითად ეფემერული დიფი-ჰელმანის (DHE) ალგორითმი.

გარდა ამისა, TLS 1.3-ის პირობებში 1.3-ის პირობებში „ხელის ჩამორთმევის“ მოლაპარაკების უფრო დიდი ნაწილი იშიფრება, რაც მონაცემთა გადაცემისათვის უფრო მეტ უსაფრთხოებას უზრუნველყოფს. ეს ხელს უწყობს კომუნიკაციის მონაწილე მხარეების საიდენტიფიკაციო მონაცემების დაცვას და ართულებს ტრაფიკის ანალიზის შესაძლებლობას.

Forward Secrecy არის ავტომატურად უზრუნველყოფილი. ეს გულისხმობს, რომ იმ შემთხვევაში, თუ TLS 1.3-ის პირობებში დაშიფრულ ინფორმაციას შეექმნება საფრთხე/მოხდება მისი განშიფვრა, შეუძლებელი იქნება ამ ინფორმაციის გამოყენებით გადაცემული მონაცემების/კომუნიკაციის განშიფვრა. ეს გულისხმობს, იმ შემთხვევაშიც კი,

[7] “Advantage of TLS 1.3 over TLS 1.2,” November 25, 2019, https://dev.to/https_india/advantage-of-tls-1-3-over-tls-1-2-6ig.

თუ სამომავლო კომუნიკაციები არ იქნება უსაფრთხო, ეხლანდელ კომუნიკაციას მაინც არ ემუქრება საფრთხე.

TLS 1.3-ის შესაძლო საფრთხეები

სესიის სისწრაფე წარმოადგენს TLS 1.3-ის ერთ-ერთი ყველაზე დიდ მიღწევას, რადგან ის აუმჯობესებს მომხმარებლის გამოცდილებას. თუმცა, არსებობს 0-RTT-ს საშუალებით სესიის „გაგრძელებასთან“ დაკავშირებული უსაფრთხოების საკითხები - მაგალითად, ის რომ ეს შესაძლებელს ხდის „replay“ შეტევას. აღნიშნულიდან გამომდინარე, ბევრი კრიპტოგრაფი და ორგანიზაცია თვლის, რომ TLS 1.3-ის გაშვებისას/გამოყენებისას გათიშავს პროტოკოლის ამ ნაწილს[8].

TLS 1.3-ს აქვს ახალი ტიპის შიფრები, რომელიც იყენებს თანამედროვე AEAD ალგორითმებს, რომლებიც შეიქმნა სპეციალურად ამ პროტოკოლისთის. ეს არის დაშიფვრის იმგვარი ფორმა, რომელიც TLS-ის უსაფრთხოებისა და სანდოობის გაზრდის მიზნით ქმნის შემდეგ მახასიათებლებს:

- კონფიდენციალურობა: უზრუნველყოფს, რომ ვერავინ ვერ შეძლოს კლიენტსა და სერვერს შორის გაზიარებული მონაცემების დეშიფრაცია.
- ავტენთიფიკაცია: უზრუნველყოფს, რომ კლიენტი რეალურად ესაუბრებოდეს მხოლოდ რეალურ სერვერს. ასევე შესაძლებელია, რომ სერვერმა მოახდინოს კლიენტის ავტენთიფიკაცია, მაგრამ ეს არის იშვიათი შემთხვევა.
- მთლიანობა: უზრუნველყოფს რომ გაგზავნილი ინფორმაცია და კომუნიკაცია არ შეიცვალოს და არ მოხდეს მისი მთლიანობის დარღვევა[9'10].

რატომ გამოიყენება უფრო მეტად 1.2 ვიდრე 1.3

ვინაიდან, TLS და SSL არის ღია სტანდარტებზე დაფუძნებული, მათი ეფექტური განვითარებისთვის საჭიროა პროტოკოლის მასობრივი დანერგვა აღჭურვილობის მწარმოებლების, ვებ-ბრაუზერების, აპლიკაციების (მაგ: Facebook და მისი სერვერები), მხრიდან მათი დანერგვა და იმისი უზრუნველყოფა, რომ არ იყოს გარკვეული ტიპის ჩავარდნები.
აქედან გამომდინარე, მიუხედავად იმისა, რომ TLS 1.3 უკვე არსებობს 2018 წლიდან, დღემდე, როგორც ზემოთ აღინიშნა, TLS 1.2 არის უფრო ფართოდ გამოყენებადი, რადგან ეს უკვე არის დე ფაქტო დანერგილი და აპრობირებული სტანდარტი[11].

TLS 1.2-ს საფრთხის იდენტიფიცირების მიზნით გააჩნდა გარკვეული ხილვადობა, რომელიც ფართოდ იყო გავრცელებული. TLS 1.3-მა ამ ხილვადობის დიდი ნაწილი დაფარა. მისი მუშაობის და უსაფრთხოების უფრო მეტად უზრუნველსაყოფად განხორციელდა გარკვეული ცვლილებები, რამაც ასევე ხელი შეუწყო გარკვეული კომპლექსურობების და სიმარტივეების პროტოკოლიდან ამოღებას. თუმცა, ისეთი

8 Gigamon, “What Do You Mean TLS 1.3 Might Degrade My Security?,” Gigamon.com (Gigamon, 2020), https://www.gigamon.com/content/dam/gated/wp-what-do-you-mean-tls1.3-might-degrade-my-security.pdf.
9 Pecanek Michal, Improving web performance & security with TLS 1.3, September 24, 2018, https://blog.cdn77.com/latest-tls-improving-https/
10 Gigamon, “What Do You Mean TLS 1.3 Might Degrade My Security?,” Gigamon.com (Gigamon, 2020), https://www.gigamon.com/content/dam/gated/wp-what-do-you-mean-tls1.3-might-degrade-my-security.pdf.
11 Martin Rudd and April 6, “TLS 1.3: Slow Adoption of Stronger Web Encryption Is Empowering the Bad Guys,” April 5, 2020, https://www.helpnetsecurity.com/2020/04/06/tls-1-3-adoption/.

კორპორაციებისთვის, რომლებიც იყენებენ ქსელუს უსაფრთხოებაზე დაფუძნებულ გადაწყვეტებს, არსებობს შესაბამისობის, რისკების მართვისა და საფრთხეების მოკვლევისათვის გარკვეული მითითებები[12].

როგორ შეუძლიათ კიბერკრიმინალებს 1.3-ის დანერგვაში არსებული ხარვეზების/ნაკლოვანებების გამოყენება

ერთ-ერთი ტიპის თავდასხმა, რომელსაც ხშირად ახსენებენ არის „Bleichenbacher"-ის თავდასხმა. ის ძირითად სამიზნეს წარმოადგენს RSA განშიფვრის ალგორითმი. მანამ, სანამდე TLS-ის ავტორები ცხდილობდნენ რომ გაერთულებინათ RSA-ის განშიფვრის გასაღების ამოხსნა, Bleichenbacher-ის თითოეული ახალი ვერსია ამას ახერხებს. შესაბამისად, ნებისმიერი მოწყობილობა რომელიც იყენებს TLS-ზე დაფუძნებულ მახასიათებლებს არის მოწყვლადი. TLS 1.3 ზღუდავს RSA-ს გამოყენებას, მაგრამ კონკრეტული შემთხვევისთის მასზე უარის თქმა ნიშნავს TLS 1.2-ზე დაბრუნებას და მასზე თავდასხმები უკვე ხშირია.

არსებობს მოსაზრება, რომ DNS over HTTPS ხელს უწყობს კიბერუსაფრთხოების მხრივ გადადგმული ნაბიჯების შესუსტებას, რადგან უფრო მეტი ბოტნეტი იყენებს მისი დაშივრის შესაძლებლობას DNS-ის გვერდის ასავლელად. დაშიფრული მოთხოვნები ნიშნავს, რომ ისინი ხვდება ტიპიური ღონისძიებების სიაში და ხელს უშლის კორპორაციულ კიბერუსაფრთხოების საშუალებებს, რომლებიც დაფუძნებულია DNS სერვერებსა და DNS მონიტორინგზე, რომ დაბლოკონ კონკრეტულ მოთხოვნებზე წვდომა. შესაბამისად, ამას შეუძლია საშუალება მისცეს თანამშრომლებს რომ მოხვდნენ სახიფათო/დავირუსებულ საიტებზე[13].

გამოყენებული ლიტერატურა:

1. "Advantage of TLS 1.3 over TLS 1.2," November 25, 2019. https://dev.to/https_india/advantage-of-tls-1-3-over-tls-1-2-6ig.

2. Gigamon. "What Do You Mean TLS 1.3 Might Degrade My Security?" Gigamon.com. Gigamon, 2020. https://www.gigamon.com/content/dam/gated/wp-what-do-you-mean-tls1.3-might-degrade-my-security.pdf.

3. Keren, Pollack. "Leaving TLS 1.2 and Moving to TLS 1.3," September 2, 2020. https://calcomsoftware.com/leaving-tls1-2-using-tls1-3/.

4. Pecanek, Michal. "Improving Web Performance & Security with TLS 1.3: CDN77.Com." CDN77. CDN77, September 24, 2018. https://blog.cdn77.com/latest-tls-improving-https/.

5. Rudd, Martin, and April 6. "TLS 1.3: Slow Adoption of Stronger Web Encryption Is Empowering the Bad Guys," April 5, 2020. https://www.helpnetsecurity.com/2020/04/06/tls-1-3-adoption/.

12 Gigamon, "What Do You Mean TLS 1.3 Might Degrade My Security?," Gigamon.com (Gigamon, 2020), https://www.gigamon.com/content/dam/gated/wp-what-do-you-mean-tls1.3-might-degrade-my-security.pdf.
13 Martin Rudd and April 6, "TLS 1.3: Slow Adoption of Stronger Web Encryption Is Empowering the Bad Guys," April 5, 2020, https://www.helpnetsecurity.com/2020/04/06/tls-1-3-adoption/.

6. "TLS 1.2 vs TLS 1.1 - KeyCDN Support," October 4, 2018. https://www.keycdn.com/support/tls-1-2-vs-tls-1-1.

7. Can I use... Support tables for HTML5, CSS3, etc, September 24, 2020, https://caniuse.com/#search=1.2

8. TLS 1.3. Can I use... Support tables for HTML5, CSS3, etc, 25AD. https://caniuse.com/.

9. „TLS 1.3." EZ. Accessed September 26, 2020. https://www.hcc-embedded.com/tls-1-3.

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 29-36 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

THE IDEAS OF REDUCING THE SIGNATURE SIZE IN HASH-BASED DIGITAL SIGNATURES.

ჰეშზე დაფუძნებული ელექტრონული ხელმოწერის ზომის შემცირების იდეები

Giorgi Labadze, Georgian Technical University
გიორგი ლაბაძე, საქართველოს ტექნიკური უნივერსიტეტი
Irakli Pirtskhalava Scientific Cyber Security Association
ირაკლი ფირცხალავა სამეცნიერო კიბერუსაფრთხოების ასოციაცია

ABSTRACT: The data encryption has been the traditional way of ensuring the different types of sensitive data. It is expected the massive release of quantum computers in the near future. Quantum computers can break the classical crypto schemes. Therefore the classical encryption systems have become vulnerable to quantum computer-based attacks. This involves the research efforts that look for encryption schemes that are immune to quantum computers-based attacks. This paper describes one of the few digital signature schemes, which is essentially immune to quantum computers-based attacks. These schemes have the efficiency problems. The biggest problem of this scheme is the large size of the signature. The paper offers the idea and the methodology of reducing the size of the signature size.

აბსტრაქტი: მონაცემთა დაშიფვრას აქვს ტრადიციული გზა დაიცვას სხვადასხვა სახის სენსიტიური ინფორმაცია. ახლო მომავალში მოსალოდნელია კვანტური კომპიუტერების მასიური წარმოება. კვანტურ კომპიუტერს შეუძლია გატეხოს კლასიკური კრიფტო სქემები. აქედან გამომდინარე, კლასიკური დაშიფრის სქემები შესაძლებელია გარდაიქმნას გამოუსადეგარ სქემებად კვანტური კოპიუტერით შეტევების წინააღმდეგ. ეს მოითხოვს კვლევითი მიდგომების შემუშავებას. უნდა შემუშავდეს კრიფტო სისტემები, რომელთაც ექნებათ იმუნიტეტი კვანტური კომპიუტერით შეტევების წინააღმდეგ. ეს სტატია აღწერს რამდენიმე ხელმოწერის სქემას, რომელიც შესაძლებელია მოისაზრებოდეს კვანტური კომპიუტერით შეტევის წინააღმდეგ მდგრადად. თუმცა, სქემებს აქვთ ეფექტურობის პრობლემა. სქემების ყველაზე მნიშვნელოვანი პრობლემა გახლავთ ხელმოწერის გრძელი ზომა. სტატიაში შემოთავაზებულია ხელმოწერის ზომის შემცირების იდეა და მეთოდოლოგიები.

Keywords: *hash-based, digital signatures, signature size*

საკვანძო სიტყვები: *ჰეშზე დაფუძნებული, ელექტრონული ხელმოწერები, ხელმოწერის ზომა*

1. შესავალი

მსოფლიოს წამყვანი მეცნიერები და ექსპერტები აქტიურად მუშაობენ კვანტური კომპიუტერების შექმნაზე. ახლახანს გამოქვეყნდა სტატია იმის შესახებ, რომ კორპორაცია Google-მა, NASA-მ და კოსმოსური კვლევების უნივერსიტეტების ასოციაციამ (Universities Space Research Association — USRA) ხელი მოაწერეს თანამშრომლობაზე კვანტური D-Wave პროცესორების მწარმოებელთან.

კვანტურ კომპიუტერს ექნება შესაძლებლობა დაანგრიოს უმეტესი წილი ან აბსოლუტურად ყველა ტრადიციული კრიპტოსისტემა, რომელიც ფართოდ გამოყენებადია პრაქტიკაში და კონკრეტულად მთელი რიცხვების ფაქტორიზაციის ამოცანაზეა დაფუძნებული (მაგალითად RSA). ზოგიერთი კრიპტოგრაფიული სისტემა, როგორიც გახლავთ RSA - ოთხი ათას ბიტიანი გასაღებით, უსაფრთხოდ ითვლება დიდი კლასიკური კომპიუტერების თავდასხმებისგან, მაგრამ უძლურია დიდი კვანტური კომპიუტერების თავდასხმების საწინააღმდეგოდ. კრიპტოსისტემა RSA გამოიყენება სხვადასხვა პროდუქტებში, განსხვავებულ პლატფორმებზე მრავალ დარგში. დღესდღეობით RSA კრიპტოსისტემა ინერგება ბევრ კომერციულ პროდუქტში, რომელთა რაოდენობაც მუდმივად იზრდება. აგრეთვე იგი გამოიყენება Microsoft-ის, Apple-ის, Sun-ის და Novell-ის ოპერაციულ სისტემებში. აპარატულ შესრულებაში RSA ალგორითმი გამოიყენება დაცულ ტელეფონებში, Ethernet ქსელურ პლატებში, სმარტ ბარათებში, და ფართოდ გამოიყენება კრიპტოგრაფიულ აპარატულ უზრუნველყოფაში. ამასთან ერთად, ალგორითმი არის Internet დაცული კომუნიკაციების ძირითადი პროტოკოლების ნაწილი, მათ შორის S/MIME, SSL და S/WAN, და აგრეთვე გამოიყენება მრავალ დაწესებულებაში, მაგალითად სამთავრობო ორგანიზაციებში, ბანკებში, კორპორაციების უმრავლესობაში, სახელმწიფო ლაბორატორიებსა და უნივერსიტეტებში [1-4].

შემუშავებულია RSA-ს სხვადასხვა „კვანტური თავდასხმებისადმი მდგრადი“ ალტერნატივები. დღესდღეობით ამ სისტემებზე ფიქსირდება ეფექტური თავდასხმების მთელი რიგი.

აღსანიშნავია ეფექტურობის ასპექტის მნიშვნელობა. დღესდღეობით ექსპერტებმა კრიპტო ალგორითმების შესრულების სისწრაფეში საკმაოდ კარგ შედეგებს მიაღწიეს. კვლევის შედეგად ცნობილი ხდება, რომ შემოთავაზებული პოსტ-კვანტური კრიპტო სისტემები შედარებით ნაკლებ ეფექტურია, რადგან მათი რეალიზაციის ალგორითმები მოითხოვს ბევრად მეტ დროს შესრულების და ვერიფიკაციისთვის.

2. ციფრული ხელმოწერები

ციფრული ხელმოწერა გახდა მნშვნელოვანი ტექნოლოგია ინტერნეტისა და სხვა IT-ინფრასტრუქტურის უსაფრთხოებაში. ციფრული ხელმოწერა უზრუნველყოფს

ავთენტურობას, მთლიანობას და მონაცემის იდენთიფიცირებას. ციფრული ხელმოწერა ფართოდ გამოიყენება იდენთიფიცირების და ავთენთიფიკაციის პროტოკოლებში. ამგვარად, არსებული უსაფრთხო ციფრული ხელმოწერის ალგორითმს აქვს გადამწყვეტი მნიშვნელობა IT უსაფრთხოების მხარდაჭერისათვის.

ციფრული ხელმოწერის ალგორითმები, რომლებიც დღეს პრაქტიკაში გამოიყენება გახლავთ RSA, DSA, ECDSA. თუმცა ისინი არ არიან კვანტურად მდგრადები , რადგან მათი უსაფრთხოება დამყარებულია რთულ ფაქტორიზაციაზე, დიდ შედგენილ მთელ რიცხვებზე და დისკრეტული ლოგარითმების გამოთვლაზე.

ჰეშზე დამყარებული ციფრული ხელმოწერის სქემები, რომელსაც წარმოვადგენთ, გვთავაზობს ძალიან საინტერესო ალტერნატივებს . როგორც სხვა ციფრული ხელმოწერის სქემა, ასევე ჰეშზე დამყარებული ციფრული ხელოწერის სქემა იყენებს კრიფტოგრაფიულ ჰეშ ფუნქციას.

3. ერთჯერადი ხელმოწერის სქემები.

ლემპორტი-დიფფი ერთჯერადი ხელმოწერის სქემა (LD-OTS) წარმოადგენს:

დავუშვათ n არის დადებითი მთელი რიცხვი, უსაფრთხოების პარამეტრი

ლემპორტი-დიფფი ერთჯერადი ხელმოწერის სქემაში [5].

ლემპორტი-დიფფი ერთჯერადი ხელმოწერის სქემა იყენებს ცალმხირვ ფუნქციას.

$$f :\{0, 1\}n\rightarrow\{0, 1\}n,$$

და კრიფტოგრაფიული ჰეშ ფუნქციას.

$$g :\{0.1\}^{*}\rightarrow\{0,1\}n$$

LD-OTS გასაღებების წყვილების გენერაცია. ხელმოწერის გასაღებია X ლემპორტი-დიფფი ერთჯერადი ხელმოწერის სქემიდან შედგება 2n ბიტიანი n სიგრძის სტრიქონებისგან, რომელიც აირჩევა თანაბრად, შემთხვევითობის მეთოდით.

$$X = (x_{n-1}[0], x_{n-1}[1],\ldots,x_1[0], x_1[1], x_0[0], x_0[1]) \in R \{0,1\}(n.2n). \quad (1)$$

LD-OTS ვერიფიკაციის გასაღები Y

$$Y = (y_{n-1}[0], y_{n-1}[1],\ldots,y_1[0], y_1[1], y_0[0], y_0[1]) \in R \{0,1\}(n.2n). \quad (2)$$

სადაც

$$y_i[j]=f(x_i[j]),\quad 0\le i\le n-1,\ j=0,1 \qquad (3)$$

ანუ LD-OTS გასაღების გენერაცია მოითხოვს 2n შეფასებას F- იდან.

სტრიქონი და ვერიფიკაციის გასაღები არის 2n ბიტიანი n სიგრძის სტრიქონები.

LD-OTS ხელმოწერის გენერაცია. A დოკუმენტი $M \in \{0,1\}(n,n)$.

ხემოწერისთვის იყენებს ლემპორტი-დიფფი ერთჯერადი ხელმოწერის სქემას (LD-OTS) ხელმოწერის გასაღებით X, (1) გამოსახულების მნიშვნელობით.

დავუშვათ $g(M)=d = (d_{n-1},...,d_0)$ არის შეტყობინების წარმოდგენა M იდან. შემდეგ LD-OTS ხელმოწერა არის

$$\sigma = (x_{n-1}[d_{n-1}],\ldots,x_1[d_1]x_0[d_0] \in \{0,1\}(n,n) \qquad (4)$$

ეს ხელმოწერა წარმოადგენს n ბიტ სტრიქონების თანმიმდევრობას , რომელთაგან თითეულის სიგრძეა n. შემდეგ არჩეულია ფუნქცია, რომლის შეტყობინებასაც წარმოადგენს d-ს. ბიტური სტრიქონი ამ ხელმოწრაში არის x_i [0], თუ i ბიტ d ში ტოლია 0-ის, ხოლო ყველა სხვა შემთხვევაში არის x_i [1] . ხელმოწერა არ მოითხოვს შეფასებას f-იდან. ხელმოწერის სიგრძეა 2n.

LD-OTS ვერიფიკაცია. ხელმოწერის ვერიფიკაციისთვის $\sigma = (\sigma_{n-1},\ldots, \sigma_0)$. M დან, როგორც გამოსახულება (4) ში, ვერიფიკაცია ითვლის შეტყობინების წარდგენას $d= (d_{n-1},\ldots, d_0)$ შემდეგ ის ამოწმებს

$$(f(\sigma_{n-1}),\ldots, f(\sigma_0))=(y_{n-1}[d_{n-1}],\ldots, y_0[d_0]). \qquad (5)$$

ხელმოწერის ზომა გახლავთ n^2 .

მიუხედავად იმისა, რომ გასაღების და ხელმოწერის გენერაცია LD-OTS ეფექტურია, ხელმოწერის ზომა საკმაოდ დიდია. ვინტერნიცის ერთჯერადი ხელმოწერის სქემაში OTS (W-OTS) ხელმოწერის ზომა მნიშვნელოვნად პატარაა. იდეა მდგომარეობს იმაში, რომ გამოვიყენოთ ერთი სტრიქონი ერთჯერადი ხელმოწერის გასაღებში, რამდენიმე ბიტის ერთდროული ხელმოწერისთვის დაჰეშილ შეტყობინებაში. მეთოდი შემოთავაზებული იქნა მერკლეს მიერ 1979 წელს [6].

4 . მერკლეს ხის იდენთიფიკაციის სქემა

ერთჯერადი ხელმოწერის სქემები, შემოთავაზებული ბოლო ვერსიით, არ არიან გამოყენებადი პრაკტიკული სიტუაციების უმრავლესობისთვის, რადგან ყოველი გასაღების წყვილი გამოიყენება მხოლოდ ერთი ხელმოწერისთვის . 1979 წელს რალფ მერკლემ შემოგვთავაზა ამ პრობლემის გადაწყვეტა. მისი იდეა მდგომარეობს შემდეგში, რომ გამოვიყენოთ სრული ბინარული ჰეშ ხე,იმისათვის რომ შევამციროთ ვერიფიკაციის გასაღების რაოდენობა, ანუ შევცვალოთ კონკრეტული ფიქსირებული გასაღებების რაოდენობა ერთით, რომლსაც წარმოადგენს ხის ფესვი.

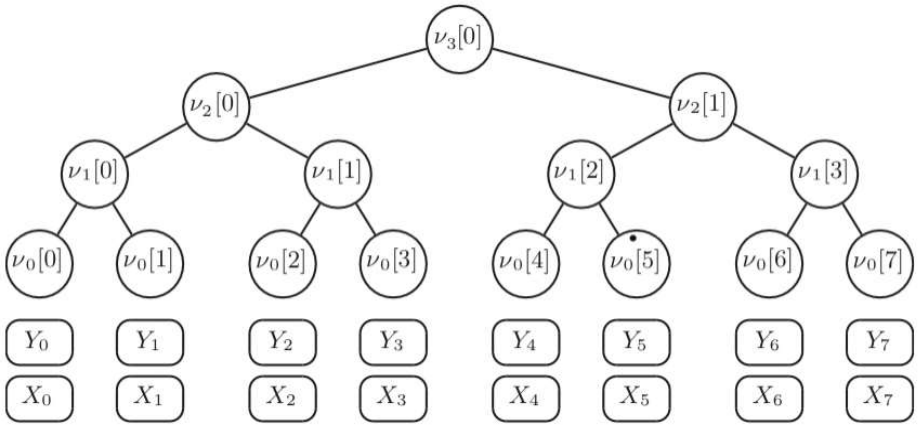
მერკლეს ხელმოწერის სქემა (MSS) მუშაობს ნებისმერ კრიპტოგრაფიულ ჰეშ ფუნქციასთან და ნებისმიერ ერთჯერად ხელმოწერის სქემასთან . განმარტებისთვის დავუშვათ $g: \{0,1\}^* \to \{0,1\}^n$ არის კრიპტოგრაფიული ჰეშ ფუნქცია. ჩვენ ასევე ვთვლით, რომ შეირჩა ერთჯერადი ხელმოწერის სქემა [7].

4.1. MSS გასაღებების წყვილის გენერაცია

ხელმომწერი ირჩევს $H \in N, H \geq 2$. შემდეგ დაგენერირებული გასაღებების წყვილი შეძლებს დოკუმენტების 2^H ხელმოწერა/ვერიფიკაციას. აღსანიშნავია, რომ არის მნიშვნელოვანი განსხვავება ისეთ ხელმოწერის სქემებთან, როგორიც არის RSA და ECDSA, სადაც პოტენციური, შემთხვევითი და ბევრი დოკუმენტები შეიძლება ხელმოწერილ/ ვერიფიცირებული იქნას ერთი წყვილი გასაღებით. თუმცა , ეს განსაზღვრული რიცხვი ასევე შეზღუდულია მოწყობილობით, რომელიც გენერირდება ხელმოწერით ან რაიმე პოლისით. ხელმომწერი აგენერირებს 2^H ერთჯერად გასაღებების წყვილს $(X_j, Y_i), 0 \leq j < 2^H$. ხის შიდა კვანძები მერკლეს ხეში გამოითვლება შემდეგი წესის მიხედვით: მშობელი კვანძი არის ჰეშ მნიშვნელობა, კონკატენცია მისი მარცხენა და მარჯვენა შვილების. MSS ღია გასაღების წყვილი არის მერკლეს ხის ფესვი. MSS საიდუმლო გასაღები წარმოადგენს 2^H ერთჯერადი გასაღებების მიმდევრობას. რომ ვიყოთ უფრო ზუსტი, მერკლეს ხეში აღვნიშნოთ კვანძები

$$\nu_h[j] = g(\nu_{h-1}[2j] || \nu_{h-1}[2j+1]), 1 \leq h \leq H, 0 \leq j < 2^{H-h}. \quad (6)$$

მაგალითი მოცემულია $H = 3$.



ნახაზი 1 მერკლეს ხე სიმაღლე $H = 3$

MSS გასაღებების წყვილების გენერაცია მოითხოვს გამოთვლებს 2^H ერთჯერადი გასაღებების წყვილიდან და $2^{H+1} - 1$ შედარების ჰეშ ფუნქციას.

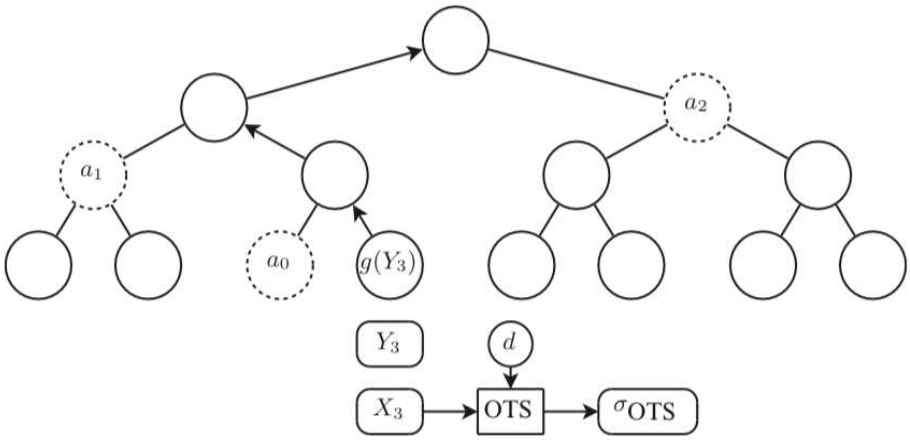
4.2 MSS ხელმოწერის გენერაცია

MSS თანმიმდევრულად იყენებს ერთჯერადი ხელმოწერის გასაღებს, რომ დააგენერიროს ხელმოწერა . შეტყობინება M-ის ხელმოსაწერად, ხელმომწერი პირი თავიდან ითვლის n-ბიტ ჰეშს, $d = g(M)$, შემდეგ აგენერირებს ჰეშ ერთჯერად ხელმოწერას σ_{OTS} , sth გამოყენებით , ერთჯერადი ხელმოწერის გასაღები არის $X_s, s \in \{0, \dots, 2^H - 1\}$. მერკლეს ხელმოწერა მოიცავს აღნიშნულ ერთჯერად ხელმოწერას და კორესპონდენციის ერთჯერად ვერიფიკაციას Y_s. რომ დავმტკიცოთ Y_s ვერიფიკაციის ავთენტურობა ,ხელმომწერი ასევე რთავს ინდექსს s , ასევე ავთენტიფიკაციის გზა ვერიფიკაციის გასაღები Y_s თვის. მერკლეს ხეში ბოლოების თანმიმდევრობაა $A_s = (a_0, \dots., a_{H-1})$. ეს ავთენთიფიკაციის ინდექსების გზა საშუალებას აძლევს ვერიფიკატორს აშენდეს უმოკლესი გზა ხის ბოლოდან მის ფესვამდე. ბოლო h აუთენთფიკაციის გზაში წარმოადგენს მშობელ დაბოლოებას. სიმაღლით h გზა მერკლეს ხეში ბოლოდან არის $g(Y_s)$ ფესვამდე :

$$a_h = \begin{cases} v_h\,[s/2^h - 1], if \lfloor s/2^h \rfloor \equiv 1\ mod\ 2 \\ v_h\,[s/2^h - 1], if \lfloor s/2^h \rfloor \equiv 0\ mod\ 2 \end{cases} \quad (7)$$

$$for\ h = 0, \dots H - 1.$$

$$\sigma_s = (s, \sigma_{OTS,} Y_s, (a_0, \dots., a_{H-1})) \quad (8)$$



ნახაზი №3 მერკლეს ხელმოწერის გენერაცია $s = 3$. მონიშული ბოლოები ასახავს ავთენთიფიკაციის გზას დაბოლოებამდე $g(Y_3)$. ისრები გვაჩვენებენ გზას ბოლოდან $g(Y_3)$ ფესვამდე .

4.3 MSS ხემოწერის ვერიფიკაცია

მერკლეს ხის ხელმოწერის ვერიფიკაცია მოიცავს ორ ეტაპს. პირველ ეტაპზე ვერიფიკატორი იყენებს ერთჯერად ვარიფიკაციის გასაღებს Y_s -ს და ერთჯერად ხელმოწერას σ_{OTS}-ს. ვერიფიკაციისთვის d-ს გამოთვლა ხდება შემოწმების ალგორითმის დახმარებით, რომელიც შესაბამისია ერთჯერადი ხელმოწერის სქემის. მეორე ეტაპზე ვერიფიკატორი ამოწმებს ვერიფიკაციის ერთჯერადი გასაღების შესაბამისობას Y_s -თან მარტივი გზით $(p_0, \dots, p_H)$, sth $g(Y_s)$ დაბოლოებიდან მერკლეს ხის ფესვამდე. ის იყენებს ინდექსს s აუთენთიფიკაციის გზისთვის $(a_0, \dots., a_{H-1})$ და გამოიყენება შემდეგი კონსრტუქცია.

$$p_h = \begin{cases} g(a_{h-1} \| p_{h-1}), if \lfloor s/2^h \rfloor \equiv 1 \ mod\ 2 \\ g(p_{h-1} \| a_{h-1}), if \lfloor s/2^h \rfloor \equiv 0 \ mod\ 2 \end{cases} \qquad (19)$$

$$for\ h = 1, \dots. H \qquad p_0 = g(Y_s).$$

ინდექსი s გამოიყენება იმისთვის, რომ დავადგინოთ თანრიგი და ავთენთიფიკაციის გზის კვანძები. კვანძები, რომლებიც ბოლოდან $g(Y_s)$ მერკლეს ფესვამდე უნდა გაერთიანდნენ. Y_s წარმატებულია, თუ p_H ტოლია ღია გასაღების.

5 ხელმოწერის შემცირების იდეა

როგორც (8) ფორმულაში აღინიშნა, მერკლეს სქემაში ხელმოწერა არის $\sigma_s = (s, \sigma_{OTS,} Y_s, (a_0, \dots., a_{H-1}))$. ეს ხელმოწერა შეიცავს $\sigma_{OTS,}$ - ერთჯერად ხელმოწერას. როგორც ვხედავთ, მერკლეს ხელმოწერაში, ხელმოწერის ზომა საკმაოდ მეტია, ვიდრე ერთჯერადი ხემოწერის დროს. ჩვენი მიზანია შევამციროთ ხელმოწერის ზომა.

აღსანიშნავია, რომ ბოლოს შემოთავაზებული ერთჯერადი ხელმოწერის სქემა არ არის გამოყენებადი პრაკტიკული სიტუაციების უმრავლესობისთვის, რადგან ყოველი გასაღების წყვილი გამოიყენება მხოლოდ ერთი ხელმოწერისთვის. უნიკალური გასაღების გადაცემა თითოეული ხელმოწერისთვის დღევანდელ პირობებში არარეალურია. კვანტური კომპიუტერები კი მოგვცემენ საშუალებას გადავცეთ გასაღებები ეფექტურად და უსაფრთხოდ [8]. შესაბამისად, მიზანშეწონილია კვანტური გასაღების პროტოკოლის

ინტეგრაცია ერთჯერად ხელმოწერის სქემაში და მისი ოპტიმიზაცია. აღსანიშნავია, რომ ვინტერნიცის მიერ შემოთავაზებულ ხელმოწერის სქემაში, ხელმოწერის ზომა ნაკლებია ვიდრე ლამპორტის სქემაში. საინტერესო იქნებოდა ამ სქემაში ზემოთ აღნიშნული პროტოკოლის ინტეგრაცია.

ბიბლიოგრაფია

1. Gagnidze A., Iavich M., Iashvili G., (2017) Analysis of post quantum cryptography use in practice. Bulletin of the Georgian National Academy of Sciences, 2, 12: 29-36
2. Gagnidze, A., Iavich, M., Iashvili, G., Novel version of merkle cryptosystem, Bulletin of the Georgian National Academy of Sciences, 2017
3. Iavich, M., Gagnidze, A., Iashvili, G., Hash based digital signature scheme with integrated TRNG, CEUR Workshop Proceedings, 2018
4. Paquin C., Stebila D., Tamvada G. (2020) Benchmarking Post-quantum Cryptography in TLS. In: Ding J., Tillich JP. (eds) Post-Quantum Cryptography. PQCrypto 2020. Lecture Notes in Computer Science, vol 12100. Springer, Cham. https://doi.org/10.1007/978-3-030-44223-1_5
5. Ajtai, M. (1986) Generating hard instances of lattice problems. In Complexity of computations and proofs, volume 13 of Quad. Mat., pp. 1-32. Dept. Math., Seconda Univ. Napoli, Caserta (2004). Preliminary version in STOC 1996. 8. Babai, L.: On Lovász lattice reduction and the nearest lattice point problem. Combinatorica, 6:1*13
6. Buchmann J., Dahmen E., Ereth S., Hülsing A., Rückert M. (2011) On the Security of the Winternitz One-Time Signature Scheme In: Nitaj A., Pointcheval D. (eds) Progress in Cryptology – AFRICACRYPT 2011. Lecture Notes in Computer Science, vol 6737. Springer, Berlin, Heidelberg
7. R. Merkle. (1979) Secrecy, authentication and public key systems / A certified digital signature Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University.
8. Hu Z., Gnatyuk S., Okhrimenko T., Tynymbayev S. and Iavich M. High-speed and secure PRNG for cryptographic applications, International Journal of Computer Network and Information Security, Issue 12 (3), pp. 1-10, 2020

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 37-44 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

საარჩევნო კიბერდანაშაული: არსი და ძირითადი ფორმები

ELECTORAL CYBERCRIME : ESSENCE AND BASIC FORMS

ნინო ბოჭოიძე - ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი (პოლიტიკის მეცნიერების ბაკალავრის მე-3 კურსის სტუდენტი)
Nino Bochoidze- Ivane Javakhishvili Tbilisi State University (Bachelor in Political Science – Junior)

ანოტაცია: 21-ე საუკუნეში განსაკუთრებით დიდი აქტუალურობითა და გლობალურობით გამოირჩევა საერთაშორისო ტერორიზმის საკითხი. პრობლემას არ აქვს საზღვრები და ის მთელი მსოფლიოსთვის მთავარი გამოწვევაა,რომლის წინააღმდეგ ბრძოლა მხოლოდ ერთიანი ძალისხმევითაა შესაძლებელი. ტერორიზმის ერთ-ერთ სახედ შეიძლება ჩაითვალოს „ტექნოლოგიური ერის“ ახალი პრობლემა- კიბერდანაშაული.

ინტერნეტი დღეს არის ყველაზე სწრაფად მზარდი ტექნოლოგია და ამავდროულად ერთ-ერთი ყველაზე საფრთხის შემცველი გამოგონება,რომელიც კაცობრიობას გააჩნია. რთულია ზუსტად განსაზღვრო კიბერდანაშაულის დეფინიცია, გამომიდნარე მისი კომპლექსური სტრუქტურისა და მრავალფეროვანი ფორმების. ფართოდ რომ განვმარტოთ,კიბერდანაშაული,ეს არის ყველა სახის სისხლისსამართლებრივი დანაშაული ,რომელიც ჩადენილია საკომუნიკაციო ან საინფორმაციო ტექნოლოგიების გამოყენებით,ან მათ მიმართ. კიბერდანაშაულის საკმაოდ ფართო სპექტრია ჩვენს ირგვლივ გაშლილი და ყოველდღიურად ადამიანები ვხდებით ძალიან ხშირი ინტერნეტ თავდასხმის მსხვერპლი,რაც თანამედროვე „ციფრული საზოგადოებისთვის“ მნიშვნელოვანი პრობლემაა.

კიბერდანაშაულის ერთ-ერთი ქვესახეობაა, შეიძლება ასეც ითქვას, საარჩევნო კიბერდანაშაული. ჩემ მიერ შერჩეული საკვლევი თემა, კიდევ უფრო დიდი გამოწვევაა მსოფლიოსთვის. ცალკეული სახელმწიფოები აქტიური პოლიტიკით ებრძვიან ინტერნეტ-დანაშაულს,რომლის რადიკალური ფორმაა საარჩევნო კიბერდანაშაული. ძირითადად სიტყვის ეტიმოლოგიური გაგებიდან, ცხადია, მისი დეფინიცია თავსატეხს არ წარმოადგენს,თუმცა საარჩევნო კიბერდანაშაული და მის ფორმებთან ეფექტური ბრძოლა,ნამდვილად რთულია. ისეთი ქვეყნებისთვის,როგორებიცაა ამერიკის შეერთებული შტატები, დიდი ბრიტანეთი, ევროპის მოწინავე სახელწმიფოები- მათთვის კიბერუსაფრთხოების პრობლემა ბევრად უფრო ადრე დადგა,ვიდრე საქართველოსნაირ განვითრებად ქვეყნებში. საარჩევნო კიბერდანაშაული ხელს უშლის დემოკრატიულ განვითარებას, თავისუფალ და თანასწორ არჩევნებს და ზიანს აყენებს სახლემწიფო უსაფრთხოებას. ის,რომ საარჩევნო კიბერდანაშაული დღეს ძალიან გავრცელებული ფორმაა, დასტურდება როგორც უცხოეთის (აშშ-ს ელექტრონული არჩევნები),ასევე საქართელოს მაგალითით.

საკვაძო სიტყვები: *საარჩევნო კიბერდანაშაული, არჩევნები,ეროვნული უსაფრთხოება, პოლიტიკა, კიბერ თავდასხმები.*

ABSTRACT: The issue of international terrorism is especially relevant in the 21st century. The problem has no borders and it is a major challenge for the whole world, which can be fought only through joint efforts. One of the forms of terrorism can be considered a new problem of the "technological nation" - cybercrime.

Nowadays, The Internet is the fastest growing technology and at the same time one of the most dangerous inventions that mankind has. It is difficult to define the definition of cybercrime precisely, given its complex structure and variety of forms. To put it broadly, cybercrime is all types of criminal offenses committed

using, or in relation to, communication or information technology. There is a wide range of cybercrime around us and every day we become victims of very frequent internet attacks, which is a significant problem for the modern "digital society".

One of the sub-types of cybercrime is electoral cybercrime. The research topic I have chosen is an even bigger challenge for the world than it seems. Individual states are actively pursuing and fighting against cyber and internet crime- the radical form of which is electoral cybercrime. Basically from the etymological understanding of the word, it is clear that its definition is not a puzzle, although electoral cybercrime and its effective fight against its forms are really difficult. For countries such as the United States, the United Kingdom, and advanced European states, the problem of cybersecurity has arisen much earlier than in developing countries like Georgia. Electoral cybercrime hinders democratic development, free and fair elections, and undermines national security. The fact that electoral cybercrime is a very common form today is evidenced by the example of both foreign (US e-elections) and Georgia.

KEYWORDS: *Electoral Cybercrime, Elections, National Security, Politics, Cyber-attacks*.

კვლევის მიზანი,ამოცანა,პრობლემა,კითხვა:

ჩემი მცირე **კვლევის მიზანია** განვსაზღვრო რა არის საარჩევნო კიბერდანაშაული და როგორია მისი ძირითადი ფორმები. ვნახავთ თუ რამდენად ეფექტურია საარჩევნო კიბერდანაშაულის წინააღმდეგ ბრძოლის პრევენციული ღონისძიებები. არანაკლებ მნიშვნელოვანია საზოგადოების ცნობიერების დონე საარჩევნო კიბერდანაშაულთან მიმართებით,აქ ჩვენ შევეხებით ინდივიდების დამოკიდებულებას საარჩევნო სისტემების მიმართ და უსაფრთხოების ნორმების დაცვას. ამგვარად, ვნახავთ როგორ ხდება საარჩევნო კიბერთავდასხმის მომზადება,განხორციელება, აღმოფხვრა და მისთვის თავის არიდება.

კვლევის ამოცანაა საარჩევნო კიბერდანაშაულის შესახებ კვლევებისა და სტატიების გაცნობა თუ როგორ ხორციელდება საარჩევნო კიბერთავდასხმა (მომზადება), გავაანალიზებთ საზოგადოების ცნობიერების დონეს (საარჩევნო კიბერდანაშაულის შესახებ) და აღმოვაჩენთ რა ბერკეტებს ფლობს სახელწმიფო საარჩევნო კიბერდანაშაულის აღმოსაფხვრელად.

კვლევის მთავარი პრობლემა არის 21-ე საუკუნეში საარჩევნო კიბერდანაშაულთან ბრძოლის გზების სიმწირე და საზოგადოების ცნობიერების დონე,რაც გამოიხატება არაინფორმულობაში. ბევრი ადამიანისთვის უცნობია თუ რატომ უნდა იყოს მათი პირადი მონაცემები დაცული,ვისგან და რა სარგებელი შეიძლება მიიღოს დამნაშავემ ინფორმაციის მოპარვით. პრობლემის არსი ღრმაა,ვინაიდან საარჩევნო კიბერდანაშაული შედის იმ სისხლის სამართლებრივ დანაშაულთა რიცხვში,რომელიც რთულად გამოსაძიებელი და საკმაოდ მზარდი პრობლემაა.

საკვლევი კითხვა: რა არის საარჩევნო კიბერდანაშაული, როგორია მისი ძირითდი ფორმები და რამდენად ეფექტურია საარჩევნო კიბერდანაშაულის წინააღმდეგ პრევენციული ღონისძიებები?

ჰიპოთეზა:

საარჩევნო კიბერდანაშაული თავისი არსითა და ფორმით არის მნიშვნელოვანი გამოწვევა და კომპლექსური სტრუქტურის მქონე პრობლემა. ის თავისი ხასიათითა და მასშტაბურობით ზიანს

აყენებს ცალკეული ქვეყნის ეროვნულ და საერთშორისო უსაფრთხოებასა. საარჩევნო კიბერდანაშაული არის რთულად კონტროლირებადი დანაშაული,რომლის წინააღმდეგ ბრძოლაც მოითხოვს ერთობას და ს საერთშორისო საზოგადოების ურთიერთთანამშრომლობას.

კვლევის მეთოდოლოგია:

ჩემს კვლევაში ვიყენებ თვისობრივი კვლევის მეთოდს,ვინაიდან ჩემი საკვლევი თემა თეორიულია და მოითხოვს ემპირიულ მასალაზე დაყრდნობით კონცეპტუალური დასკვნების გაკეთბას. კვლევას საფუძვლად უდევს სხვადასხვა ექსპერტის კვლევის, სტატიების, პოლიტიკის სტრატეგიული გეგმების კონტენტ ანალიზი. პირველ ეტაპზე მოძიებულ იქნა საერთაშორისო კვლევითი დოკუმენტები საკვლევ თემასთან დაკავშირებით,მოხდა მათი სიღრმისეული შესწავლა და საბოლოოდ კვლევის დასასრულს,გაანალიზებული კონტენტის საფუძველზე დასკვნის გაკეთბა.

თემის მიმოხილვა:

სარჩევნო კიბერდანაშაულის არსი და რისკები

საარჩევნო კიბერდანაშაული თავისი ხასიათითა და გავრცელების არეალით საკმაოდ ხშირი და მრავლისმომცველია. მისი არსია სწორედ თავდასხმის განხორციელება პოლიტიკურად ყველაზე მნიშვნელოვან მოვლენაზე-არჩევნებზე. კიბერთავდასხმის მიზანია მოიპოვოს ფარულად ინფორმაცია, გამოიყენოს ის ბოროტოად და მიაყენოს ზიანი კონკრეტული ქვეყნის ეროვნულ უსაფრთხოებას, პარტიას,პოლიტიკურ ფიგურას ან ყველაზე რადიკალური ფორმით, გამოიწვიოს ქვეყნების დაპირისპირება. როგორც წესი მთავარი მიზანი საარჩევნო კიბერდანაშაულისთვის არის არა კიბერსივრცის ხელყოფა,არამედ მოსახლეობის დაშინება ან ზემოქმედება ხელისუფლების ორგანოზე. რა თქმა უნდა, თავდასხმის რისკები ყოველდღიურად იზრდება,თუმცა საერთაშორისო საზოგადოება თანხმდება,რომ ჯერ კიდევ არ დგას გლობალიზებულ ერაში ის მომენტი,როდესაც ქვეყნები ციფრულად დაიწყებენ კომუნიკაციას, შესაბამისად ეს კიდევ უფრო გაზრდის თავდასხმების რაოდენობას და შესაძლოა ქსელური კავშირებით ერთი სახელწმიფო შეიჭრას მეორე სახლემწიფოს სუვერენიტეტში, მოიპოვოს საჭირო ინფორმაცია და „გაქრეს“ კიბერსივრცეში ისე,რომ მისი კვალის მიგნებას ვერავინ შეძლებს. თითქოს წარმოუდგენელია როგორ ხდება ჩვენს რეალობაში ამგვარი რთული დანაშაულის ჩადენა და შემდეგ მისი იდენთიფიკაცია,თუმცა ყველაფერი დამოკიდებული არის რისკებზე და მათ სწორად გათვლაზე. დემოკრატიას ყველაზე დიდ ზიანს არალეგიტიმურად ჩატარებული არჩევნები აყენებს. საარჩევნო კიბერთავდასხმა სწორედ იმიტომაა კომპლექსური დანაშაული, რომ ქმედების განხორციელებისას გათვლილია ყველა მოსალოდნელი რისკი. სამწუხაროდ დღეს მსოფლიოს უმრავლეს ქვეყანაში ჯერ კიდევ არ დგას საკითხი კიბერუსაფრთხოების გაძლიერების პოლიტიკის კუთხით,რაც თავის მხრივ ზრდის საფრთხეებს,რომლებთან ბრძოლაც დიდ ძალისმხევას მოითხოვს. პირველ რიგში, საარჩევნო კიბერთვდასხმისას მთავარი სამიზნე ყოველთვის არის საარჩევნო სისტემები. ვირტუალური მმართველობა კიდევ უფრო ზრდის რისკებს მოსალოდნელი თავდასხმებისას. აღსანიშნავია ის კიბერ-რისკები,რომლებიც უკავშირდება მატერიალურ ზიანს, ორგანიზაციების რეპუტაციის განადგურებას, ტექნოლოგიური წარუმატებლობის გამო შეფერხებებს,ასევე ეს ტერმინი გულისხმობს დეზინფომაცის გავრცელებას, საარჩევნო ადმინისტრაციებიდან ქსელური

უსაფრთხოების შესახებ ინფრმაციის მოპარვას, სუსტი პროგრამული უზრუნველყოფის გამოაშკარავებას და კიდევ ბევრ სხვა დამაზიანებელ ქმედებას. საბოლოო ჯამში, რისკები დაკავშირებულია როგორც კონკრეტულ ადამიანებთნ,ასევე აბსტრაქტულ მოვლენებთნ და ყველაზე მთვარ,უკონტროლო ინტერნეტთან და ონლაინ-სივრცესთან. ჩვენ უნდა შევძლოთ ძლიერი კიბერუსაფრთხოების პოლიტიკით და მოქნილი მექანიზმებით ამ საფრთხეების აღმოფხვრას და პრევენციას,მაგრამ არ უნდა დაგვავწიყდეს,რომ ყველა დიდი კიბერთავდასხმის უკან დგას ადამიანთა ჯგუფი, რომელიც სარგებლობს ავტორიტეტით,აქვს წვდომა მნიშვნელოვან ინფორმაციაზე და ხშირად ისინი არიან პოლიტიკური სპექტრის წარმომადგენლები,რომლებიც მიზანმიმარულად მოქმედებენ სამიზნის წინააღმდეგ. რაც შეეხება შემსრულებლებს,ისინი არიან უბრალო ჰაკერები კარგი ცოდნისა და გამოცდილების მქონე ადამიანები,რომლებიც უბრალოდ დავალებებს ასრულებენ.

საარჩევნო კიბერდანაშაული,როგორც პოლიტიკური დანაშაული

საარჩევნო კიბერთავდასხმა დანაშაულია,რომლის მოტივიც შეიძლება იყოს ანგარება, შურისძიება, პოლიტიკური და ა.შ. ის განიხილება პოლიტიკურ დანაშაულად,ვინაიდან თავისი არსით წარმოადგენს იდეოლოგიურად მოტივირებულ ქცევას,რომელიც იურიდიულად შეიძლება განისაზღვროს როგორც დანაშაულებრივი ქმედება.პოლიტიკურად მოტივირებული კომპიუტერული დანაშაული სტაბილურად იზრდება 1980-იანი წლების ბოლოდან[1]. საფრთხე ექმნებათ როგორც ერ-სახელმწიფოებს,ასევე პოლიტიკური დღისწესრიგის მქონე პირებსა და ჯგუფებს.საარჩევნო კიბერდანაშაული არსებითად მოტივირებულია პოლიტიკურად და მას შეუძლია ზიანი მიაყენოს, არა მხოლოდ პოლიტიკას,არამედ ეკონომიკას, ტექნოლოგიურ სფეროს, მედია საშუალებებსა და უსაფრთხოების მიზნებს. მიუხედავად იმისა,რომ კიბერთვდასხმა ითვლება პოლიტიკურ დანაშაულად, ჩვენთვის რთულია ვისაუბროთ მასთნ ბრძოლის გზებზე იგივე სტრატეგიით,როგორცაა ეს შესაძლებელია სხვა პოლიტიკურ დანაშაულთან ბრძოლისას. ძალზე რეალურია კიბერ ომისა და კიბერ ჯაშუშობის საფრთხე, რომელიც მჭიდროდაა დაკავშირებული საარჩევნო კიბერთვდასხმებთან.ამ საფრთხეების რაოდენობრივი შეფასება რთულია,ვინაიდან თავდასხმის ჭეშმარიტი წყაროს დადგენა ზოგჯერ შეუძლებელია რადგან თავდამსხმელთა უმეტესობა საკუთარ თავსა და მათ სამიზნეს შორის კავშირების ჯაჭვს იყენებს. მაგალითად, სადმე ევროპაში "ჰაკერმა" შეიძლება გამოიყენოს კომპიუტერის სისტემა ჩინეთში, გაერთიანებული სამეფოს სისტემაზე შეტევისთვის. ყურადსაღებია, ის ფაქტიც,რომ რთულია მოტივების ჩამოყალიბება ონლაინ შეტევებში,სწორედ ამიტომ არჩევნებზე თავდასხმა თავისთვად გულისხმობს პოლიტიკურ დამნაშავეობას,ვინაიდან ის პირდაპირააა მიმართული სახემწიფოში მიმდინარე პოლიტიკური მოვლენისაკენ. საარჩევნო ადმინისტრაციების მთავარი მიზანია მანიპულირების რისკების მართვა და მოსალოდნელი საფრთხეების თავიდან აცილება,რომელსაც ახორციელებენ აუდიტისა და კონტროლის

[1] Anderson,K, (29 sep,2008) „**How do we tackle political cyber-crime?“** https://www.computerweekly.com/opinion/How-do-we-tackle-political-cyber-crime?fbclid=IwAR1TO7nq7A-lKv_-7SQJzzpvYjiw1cEguaykCTudVWxHps7hQkAJdiDFkMk

ღონისძიებებით.მაშინ როდესაც მსოფლიო ქვეყნების უმრავლესობას პრაქტიკაში აქვთ არჩევნების „ქაღალდებით“ ჩტარება, დღეს თნდათანობით იზრდება ტექნოლოგიური რესურსის გამოყენება,რომელიც თავის მხრივ საფუძველია დიდი კიბერშეტევებისა. გავრცელებულია არასწორი წარმოდგენა,რომ მხოლოდ ის ქვეყნები ხდებიან კიბერთავდასხმის მსხვერპლნი,რომლებსაც ელექტრონული ხმის მიცემის სისტემა აქვთ, თუმცა ყველა არჩევნები დამოკიდებულია ინფორმაციისა და საკომუნიკაციო ტექნოლოგიის ინსტრუმენტებზე.ბევრი ექსპერტი საუბრობს სწორედ ელექტრონულ სისტემასა და ქაღალდების სისტემის სხვაობა-უპირატესობებზე და თვლიან,რომ წარმატების გასაღები იქნება კიბერუსაფრთხოება, „ქაღალდის ბილიკები“, რისკების შემზღუდავი აუდიტი და უწყებათშორისი კომუნიკაცია.

კიბერთავდასხმების ფორმები არჩევნებში

არჩევნებზე თავდასხმა შესაძლოა განხორციელდეს რამდენიმე ფორმით. არსებობს წინა საარჩევნო პროცესზე თავდასხმის ფორმა,რომლის დროსაც თავდამსხმელების მოტივი და მიზანია წინასწარი წვდომის მიღება და შემდეგ პოლიტიკური ამინდის შეცვლა,რაც იწვევს არჩევნების გაჭიანურებას ან საერთოდ გაუქმებას. მეორე ფორმა ესაა უშუალოდ არჩევნების მიმდინარეობისას თავდასხმის განხორციელება,რომელიც მიმართულია კონკრეტულად ერთი პარტიის ან პოლიტიკური ფიგურის დეგრადაციისკენ. ძირითდად მეორე ფორმა ყველაზე გავრცელებულია და ვხვდებით მის კერძო სახეებსაც,როდესაც თვდასხმები ხორციელდება პოლიტიკურ კამპანიებზე, პარტიების საინფორმაციო და საკომუნიკაციო მედია-პლატფორმებზე და ის ყველაზე ხანგრძლივ მუშაობას მოითხოვს დამნაშავის მხრიდან,რათა მიაღწიოს მიზანს. მესამე ძირითდი ფორმა გახლავთ არჩევნებზე თვდასხმა,მისი შედეგების გამოქვეყნების,ე.ი. დასრულების შემდეგ. ეს ფორმა გამოირჩევა განსაკუთრებული სიმწვავით,რადგან კიბერშეტევა გავლენას ახდენს არა მხოლოდ არჩევნებში მონაწილე კანდიდანტებზე,არამედ მთლიან ელექტორატზე. განსაკუთრებულს მგრძნობელობას იწვევს საარჩევნო კიბერშეტევები საზოგადოებაში.რთულია სახელმწიფოსთის ახსნას მიზეზები და მიზნები თავდასხმებისა, რომლის თვიდან აცილებაზე პასუხსიმგებელი თავადაა. თითოეული ჩვენგანი შესაძლოა ისე გავხდეთ კიბერთავდასხმის მსხვერპლი,რომ ეს ვერც გავაანალიზოთ,მაგრამ როდესაც საქმე დემოკრატიულ ღირებულებებზე დაფუძნებულ ფარულ კენჭისყრას ეხება, საზოგადოება ვერ ეგუება პირადი ინფორმაციის თაღლითური მოპოვების ფაქტს. არსებობს თვდასხმის საჰაერო განხორციელების პრაქტიკა რომელიც ეფექტურად მუშაობს დეზინფორმაციის გავრცელებასთნ ერთად. რაც უფრო მარტივია საარჩევნო ინფრასტრუქტურა,მით უფრო ადვილია თვდასხმა მასზე. შეტევის განხორციელება სივრცეში განუსაზღვრელია შეიძლება ითქვას, ვინაიდან თანაბრად მოსალოდნელია როგორც ქვეყნის შიგნიდან თვდასხმა,ასევე სხვა სახელწმიფოებიდან. ბევრი მკვლევარი საუბრობს მომავალი არჩევნების საფრთხეებზე,რომლებიც მომდინარეობს კიბერსივრციდან და ეხება ინფორმაციის გასაჯაროვებას. მაგალითისთვის შეგვიძლია გავიხსენოთ სულ ახლახანს მომხდარი კიბერთვდასხმა რუსეთის მხრიდან საქართველოს სააარჩევნო სიებზე.[2] ამერიკული გამოძიების თანახმად, საქართველოს მოსახლეობის პირადი ინფორმაცია მოპარულ და განთვსებულ იქნა საერთშორისო მონაცემთა უცხოური ბაზის პორტალზე,სადაც ერთდროულად ასეულობით ქვეყნის უსაფრთხოების სამსახურს აქვს წვდომა და შეეძლოთ გასაჯაროვებული ინფორმაციის

[2] Cimpanu, C. (March 30,2020 -- 02:07 GMT (03:07 BST) **“Personal details for the entire country of Georgia published online”** https://www.zdnet.com/article/personal-details-for-the-entire-country-of-georgia-published-online/

მოპარვა და რა თმა უნდა საჭიროებისამებრს გამოყენება. დიდი კიბერშეტევის მსხვერპლი იყო 2016 წლის არჩევნები ამერიკის შეერთეული შტატები,რომელსაც მსოფლიოში ყველაზე ძლიერი კიბერუსაფრთხოების პოლიტიკა აქვს და სწორედ მისი მაგალითით დასტურდება ჩემი ჰიპოთეზა,რომ ისეთ ძლიერ საფრთხესთნ ბრძოლა,როგორიც საარჩევნო სისტემებზე კიბერთვდასხმებია, მარტო რთულია და მოითხოვს საერთაშორისო საზოგადოების ურთიერთთანამშრომლობას.სწორედ ამას გულისხმობს უწყებათშორისი კომუნიკაცია,რაც აშშ-ს მთავარი ბერკეტია კიბერუსაფრთხოების გაძლიერებისთვის.2017 წლის ივნისში შეერთებული შტატების მასშტაბით, 100-მა საარჩევნო ექსპერტმა კონგრესს მიმართა ღია წერილით აღნიშნა, რომ მრავალი იურისდიქცია „არასათანადოდ იყო მომზადებული, რათა გაუმკლავდეს კიბერუსაფრთხოების რისკების ზრდას“[3]. ეს ნიშნავს,რომ ბევრ პრობლემას და გამოწვევას აწყდება მსოფლიოში ყველა სახელმწიფო როდესაც საქმე ეხება კიბერსივრცეს.

საარჩევნო კიბერუსაფრთხოება(უსაფრთხოების დაცვის მექანიზმები) საფრთხე და პრევენცია

როდესაც ჩვენ ვსაუბრობთ საფრთხეებზე და მათ მიერ გამოწვეულ ზიანზე,აუცილებელია პარლელურად განვიხილოთ კიბერუსაფრთხოების მნიშვნელობა და ის მექანიზმები,რომლითაც შესაძლებელია რისკების თავიდან აცილება და უსაფრთხოების უზრუნველყოფა. ყველაზე მთავარი,როდესაც საქმე ეხება საარჩევნო კიბერთავდასხმას,არის თავდამსხმელსა და სამიზნეს შორის ურთიერთკავშირის დადგენაა. შემდეგი ნაბიჯი არის შესაბამისი სტრუქტურებისა და სახლმწიფო აპარატების მხრიდან რისკების სწორი შეფასება,რასაც მოჰყვება საბრძოლო სტრატეგიის შემუშავება. ცნობილია,რომ იდენტური კიბერშეტევა არ არსებობს,ვინაიდან არ არსებობს იდენტური ქსელი,შესაბამისად თითოეული შეტევის ფაქტს სჭირდება კონკრეტული დეტალური გამოძიება. საბოლოო ნაბიჯი არის პრობლემის აღმოფხვრა, მოქნილი ბერკეტებით ბრძოლა და ყველაზე რადიკალური ფორმა არის კონტრშეტევა. რაც შეეხება,კონტრშეტევას, ის პრაქტიკაში ჯერ არ განხორციელებულა,ქმედების კვალიფიკაცია არ მომხდარა როგორც-კონტრშეტევა,თუმცა აშშ-ს კიბერუსაფრთხოების პოლიტიკა ითვალისწინებს მსგავს ღონისძიებებსაც.

საარჩევნო სისტემის ქსელური უსაფრთხოება გულისხმობს „ონლაინ“ და „ოფლაინ“ მდგომარეობაში პროგრამული უზრუნველყოფის თანაბარ სიძლიერეს. ყველაზე გახშირებული თავდასხმები მაინც ხდება პირად ინფორმაციულ ბაზებზე და საჯარო მედია პლათფორმებზე, საიდანაც უფრო მარტივია ინფორმაციის აღება და ბოროტად გამოყენება ვიდრე პირადი მონაცემებით მანიპულირება. დღეს უკვე ბევრი დიდი ორგანიზაცია და კორპორაცია იბრძვის კიბერსივრციდან მომავალი საფრთხეების წინააღმდეგ,ისინი თანამშრომლობენ ცალკეული სახლემწიფოების უსაფრთხოების სამსახურებთნ და ქმნიან ერთგვარ ვაკუუმ სისტემას რათა კანონიერად დაიცვან ის,რასაც „ჰაკერები“ უკანონოდ ართმევენ. საერთაშორისო სამართალი,რომელიც აწესრიგებს კიბერსამართალს და იცავს საერთაშორისოდ ყველა ქვეყნის ეროვნული სამართლის მიერ აღიარებულ ნორმებს,ითვალისწინებს კიბერთავდასხმების წინააღმდეგ მიმართულ პრევენციურ ღონისძიებებს.მინდა სტრუქტურის რთული აგებულების

[3] National Election Defense Coalition (June 21,2017) **“Election Integrity Open Letter to Congress,”** https://www.electiondefense.org/election-integrity-expert-letter

გასააზრებლად მოვიყვანო "FIREEYE"-ის ექსპერტთა კვლევა[4] მაგალითად და მოკლედ განვიხილო თუ რა კონკრეტული ნაბიჯებია იმისთის,რომ არჩევნებზე კიბერთავდასხმა იქნას თავიდან აცილებული და საფრთხეები განეიტრალებული. პირველ რიგში, ექსპერტები გამოყოფენ სამ ძირითად დაუცველ კატეგორიას,რომლებიც ყველაზე ხშირად ხდებიან ამგვარი თვდასხმების სამიზნეებში. პირველი ეს არის ძირითადი საარცევნო სისტემები,მეორე -საარჩევნო ადმინისტრატორები და ბოლოს საარცევნო კამპანიები,რომლებშიც თავის მხრივ იგულისხმება (პარტიები,სოც.მედიის პლათფორმები,საინფორმაციო ორგანიზაციები,დონორი ჯგუფები...). თვდაცვის მექანიზმები კი ასე გამოიყურება- პირველი ნაბიჯი არის საარცევნო ინფრასტრუქტურის კრიტიკული შეფასება, შემდეგი ნაბიჯია ხარვეზების გამოვლენა და ხმის მიცემის გეგმის ტესტრიება,შემდეგი ეტაპია საარცევნო ინფრასტრუქტურის მოდერნიზება,რაც გულისხმობს უსაფრთხოების პროგრამულ გაუმჯობესებას და ბოლო ნაბიჯი არის არსებული ტექნოლოგიური კავშირების მუდმივი განახლება.არსებობს რადიკალური გზით ამ პრობლემის გადაჭრის საშუალებაც,რაც პირდაპირ მოიაზრებს საარჩევნო სისტემების შეცვლას, ინფორმაციის ნაკლებ საჯაროობას და ტექნოლოგიების როლის შემცირებას საარჩევნო ინფრასტრუქტურაში. ევროპის მოწინავე ქვეყნბში ფიქრობენ,რომ არჩევნების ელექტრონული სისტემით ჩატარება ყველაზე დიდი საფრთხის შემცველია,მაშინ როდესაც აშშ-ში ეს პრაქტიკა უკვე წლებს ითვლის და ის მაინც დემოკრატიის უპირობო ნიმუშია.

დასკვნა

ამრიგად, მინდა ჩემი მსჯელობა შევაჯამო და ვთქვა,რომ საარჩევნო კიბერდანაშაული ნამდვილად არის ერთ-ერთი ყველაზე კომპლექსური სტრუქტურის მქონე დანაშაული,რომლის წინააღმდეგ ბრძოლაც მოითხოვს სიფრთხილეს და ძალების კონსტრუირებას ერთობლივად. ბუნებრივია,საფრთხეები ზრდადი ფუნქციაა და შესაბამისად მისი პრევენცია პირდაპირპროპორციულად უნდა მოხდეს.მე მიმაჩნია,რომ ეროვნულ დონეზე სახელმწიფოები სისხლის სამართლის კოდექსით ვერ დაარეგულირებენ მსგავსს კიბერშეტევებს,გარდა ამისა საერთაშორისო სამართალი ყოველთვის ვერ უმკლავდება ქსელურ თავდასმხებს და საჭიროა კიბერუსაფრთხოების გაძლიერება,აშშ-ს მრავალწლიანი პრქტიკის გაზიარება და რაც ყველაზე მთავარია საზოგადოების ცნობიერების დონის ამაღლება,რადგან მაშინაც კი,როდესაც თავს უსაფრთხოდ ვგრძნობთ,ვიღაცები დაკავებულები არიან ჩვენს შესახებ ინფორმაციის მოპოვებით,დამუშავებითა და სწორ დროს ,სწორ ადგილას გამოყენებით.

ბიბლიოგრაფია:

1. Anderson,K, (29 sep,2008) „**How do we tackle political cyber-crime?"** https://www.computerweekly.com/opinion/How-do-we-tackle-political-cyber-crime?fbclid=IwAR1TO7nq7A-lKv_-7SQJzzpvYjiw1cEguaykCTudVWxHps7hQkAJdiDFkMk
2. Cimpanu, C. (March 30,2020 -- 02:07 GMT (03:07 BST) **"Personal details for the entire country of Georgia published online"** https://www.zdnet.com/article/personal-details-for-the-entire-country-of-georgia-published-online/
3. National Election Defense Coalition (June 21,2017) **"Election Integrity Open Letter to Congress,"** https://www.electiondefense.org/election-integrity-expert-letter

[4] Seen (29 April,2020) "**Cyber threats and elections: understanding the security risk".** https://vision.fireeye.com/editions/06/06-cyber-threats-and-elections.html?fbclid=IwAR1j9LtiMEtFkCZcAOJqbGu62IzyLY_mqLTI5Y-kvAl4JtLbaKTq0cNF5Vc#

4. Seen (29 April,2020) "**Cyber threats and elections: understanding the security risk".** https://vision.fireeye.com/editions/06/06-cyber-threats-and-elections.html?fbclid=IwAR1j9LtiMEtFkCZcAOJqbGu62IzyLY_mqLTI5Y-kvAl4JtLbaKTq0cNF5Vc#
5. Jakobsson, M. and Ramzan, Z. (Apr 23,2008) **"Cybercrime and Politics: The Dangers of the Internet in Elections"** https://www.informit.com/articles/article.aspx?p=1190114&ranMID=24808&fbclid=IwAR0tnKJGmtgqfK5AeoT1L892KBPN2SGCA_yhndhK7SO0nIQjCggGvkWPaFQ
6. Rafter,D. (Seen – may 3,2020) **"2020 election cybersecurity: Protecting U.S. elections against cybercrime"** https://us.norton.com/internetsecurity-emerging-threats-2020-election-cybersecurity.html?fbclid=IwAR0HoTAl4coxa8nmkX8ts9cbuoIhugSKiSxDmhRPffcPZHPWm4oImbk107Q
7. Fidler, D.P (2016**) "The U.S. Election Hacks, Cybersecurity, and International Law"** DOI: https://doi.org/10.1017/aju.2017.5
8. Ivanova, A.X. (September,2019) **"Online voting as an element of cybersecurity of megacities" https://www.researchgate.net/publication/339143499_Online_voting_as_an_element_of_cybersecurity_of_megacities?fbclid=IwAR0Yq9SaLkOWcP4fJdhgL6mau9c_GO5_C-it-5dkTrTYkoozEKXttiRSiLY**
9. Morris, D. Baccio, M. Klein,D. Nixon. A. (April 28,2020) **"Cyber Threats to Elections"** Webinar **https://www.brighttalk.com/webcast/574/387719/cyber-threats-to-elections?fbclid=IwAR2YFZ2dCFoeq5Phfmu4c1MNV9rB03KyOMLsK--cx2A1dlVTrsd1X6-_fTo**
10. Thomas,D. (October 26,2017) **"Protecting elections from cyberattacks"** **https://www.raconteur.net/technology/protecting-elections-from-cyberattacks**
11. Staak.S.V. and Wolf,P. (seen April 30,2020) **"Cybersecurity in Elections" (Models of Interagency Collaboration) https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf?fbclid=IwAR3EPnVTRkIm6rwncCm1uL-llPeHqmXYPgRpE6OYa1EJaAisWQcP7RQXb_s**
12. Seen (May 2,2020) **National Counterintelligence and Security Centre- "Foreign Threats to U.S. elections ,election security information needs"** **https://www.odni.gov/files/ODNI/documents/DNI_NCSC_Elections_Brochure_Final.pdf**
13. Agawu, E. A. (April 3, 2018) **"How to Think About Election Cybersecurity: A Guide for Policymakers." https://www.newamerica.org/cybersecurity-initiative/policy-papers/how-to-think-about-election-cybersecurity/**
14. Hawkins, D. (June 5, 2018) **"The Cybersecurity 202: Voters' Distrust of Election Security Is Just as Powerful as an Actual Hack, Officials Worry"-** *Washington Post* **https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/05/the-cybersecurity-202-voters-distrust-of-election-security-is-just-as-powerful-as-an-actual-hack-officials-worry/5b1567091b326b08e883912f/%3futm_term%3d.7a03e7805651**

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 45-51 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

THE USE OF GAME THEORY TO STUDY PROCESSES IN THE INFORMATIONAL CONFRONTATION
ПРИМЕНЕНИЕ ТЕОРИИ ИГР ДЛЯ ИССЛЕДОВАНИЯ ПРОЦЕССОВ В ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ

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).
Ruslan Hryshchuk, National Aviation University, Doctor of Engineering Science, Full Professor, Kiev, Ukraine
Грищюк Руслан Валентинович, доктор технических наук, профессор, профессор Национального авиационного университета (г. Киев).
Nikolay Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor Kiev, Ukraine
Браиловский Николай Николаевич, кандидат технических наук, доцент, доцент Киевского национального университета имени Тараса Шевченко (г. Киев).

Tatyana Shcherbak, National Aviation University, PhD in Engineering Science, Associate Professor Kiev, Ukraine
Щербак Татьяна Леонидовна, кандидат технических наук, доцент, доцент Национального авиационного университета (г. Киев).

ABSTRACT: This paper is presented the application of the games' theory for the analysis of processes in the informational warfare. The analysis of information warfare in cyberspace is presented. It is shown that today the solution to the problems of information warfare is impossible without the development of new theoretical and methodological provisions for the analysis of the processes of attack and counteraction in the information space. The scheme of finding sustainable strategies that ensure the neutralization of the enemy is investigated.

АННОТАЦИЯ: В данной работе представлено применение теории игор для исследования процессов в информационном противоборстве. Проведен анализ информационного противоборства в киберпространстве. Показано, что на сегодня решение проблем информационного противоборства невозможно без разработки новых теоретико-методологических положений анализа процессов нападения и противодействия в информационном пространстве. Исследована схема нахождения устойчивых стратегий, которые обеспечивают нейтрализацию противника.

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

Стремительное развитие научно-технического процесса в начале XXI века в области информационно-коммуникационных технологий связано с повсеместным внедрением ее во все сферы деятельности общества: военную, политическую, социальную, научную, экономическую, нормативно-правовую, технологическую и другие. В результате этого

открываются широкие возможности в несанкционированном доступе к информационным ресурсам неавторизированным пользователям.

Небезопасный характер современных угроз информации, что переходит в разряд стратегических ресурсов как предмет информационной безопасности, определило противодействие им и принципиальным аспектом укрепления стратегической стабильности общества, национальной, региональной и международной безопасности.

Анализ конфликтов конца XX – начала XXI века свидетельствует о появлении новых форм и методов не только вооруженной борьбы между государствами для расширения соответствующих политических целей и разрешения межгосударственных противоречий. На смену классическим формам вооруженной борьбы пришли так называемые «гибридные войны». Они имеют скрытый характер и проводятся преимущественно в политической, экономической, информационной и других сферах. Суть таких войн является смещение центра усилий с физического уничтожения противника в рамках масштабной войны на применение средств так называемой «мягкой силы» против страны-противника в целях дезинтеграции, изменения ее руководства и включения в сферу своего влияния. [1]

В современных условиях глобальной информатизации и гибридных войн, с учетом большого количества подходов и решенных проблем защиты информации и противодействия атакам и операциям информационных воздействий, они остаются актуальными не только для Украины, но и для всего мирового сообщества. [2]

Существующие математические модели процессов нападения на информационное пространство и его защиту, на которых основываются оценки уровня защищённости не учитывают динамику изменения множества возможных несанкционированных воздействий и вариаций их параметров как в реальном масштабе времени, так и в процессе эксплуатации информационно-коммуникационных систем.

Системность исследования поведения сложных динамических процессов требует рассмотрения большого числа особенностей и взаимосвязей, характерных процессу нападения на информацию и информационных воздействий. Исследованные особенности, созданные антагонистической природой, противоречат одна другой, однако пренебрегать каждой из них нельзя так как они дают нам полное представление о процессе, который исследуется или моделируется. Некоторая некорректность решаемых задач, порождаемых антагонистичностью целей субъектов, проявляется в их многокритериальности постановки, где частичными критериями качества выступают ресурсы игроков.

Таким образом, дальнейшее решение проблемы информационного противоборства в киберпространстве включает в себя разработки новых процессов и методик, которые базируются на теоретико-обоснованных и опробованных на практике методов анализа. Отсутствие в области информационного противоборства теоретико-методологических положений анализа процессов нападения и противодействия в информационном пространстве на основании методов теории игр, что сдерживает в какой-то мере дальнейшее развитие высокоэффективных принципов противодействия гибридной войне. [3, 4, 5, 6] Кроме того, широкое применение теории игр при анализе атак и противодействия им может значительно уменьшить ошибки и просчеты, которые имеют место в управлении информационной безопасностью, что в свою очередь минимизирует негативные и нежелательные политические, социальные и финансовые последствия для субъектов информационного противоборства. То

есть применение для этих исследований устойчивых стратегий теории игр позволяет обеспечить нейтрализацию нападающей стороны или обеспечивают игроку устойчивое положение в некотором подинтервале единичного интервала.

ЦЕЛЬ РАБОТЫ

Целью работы является исследование возможности применения теории игр для анализа процессов информационного противоборства.

ОСНОВНАЯ ЧАСТЬ

Основной теоремой теории игр является теорема о равенстве максимина и минимакса, впервые сформулированная и доказанная Дж. фон Нейманом. Эта теорема устанавливает условия существования оптимальных стратегий и цены игры.

Для прямоугольных игр вопрос существования решения игры решается на основании следующей теоремы. [7]

Теорема 1. Пусть

$$\mathrm{A} = \begin{Vmatrix} \mathrm{a}_{11} & \mathrm{a}_{12} & \dots & \mathrm{a}_{1m} \\ \dots & \dots & \dots & \dots \\ \mathrm{a}_{n1} & \mathrm{a}_{n2} & \dots & \mathrm{a}_{nm} \end{Vmatrix}$$

- платежная матрица, $X = \|x_1, x_2, \dots, x_n\|$ и $Y = \|y_1, y_2, \dots, y_m\|$ - смешанные стратегии игроков $И_1$ и $И_2$ соответственно, математическое ожидание выигрыша игрока $И_1$ определено следующим образом

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

тогда величины $\underset{X \in S_n}{max}\ \underset{Y \in S_m}{min}\ E(X,Y)$ и $\underset{Y \in S_m}{min}\ \underset{X \in S_n}{max}\ E(X,Y)$ существуют и равны между собой.

Для непрерывных игр эта теорема формулируется следующим образом. [8]

Теорема 2. Если $M(x,y)$ есть непрерывная функция двух переменных в замкнутом единичном квадрате, то величины

$$\underset{F \epsilon D}{max}\ \underset{G \epsilon D}{min} \int_0^1 \int_0^1 M(x,y)\,dF(x)\,dG(y) \quad (1)$$

$$\underset{G \epsilon D}{min}\ \underset{F \epsilon D}{max} \int_0^1 \int_0^1 M(x,y)\,dF(x)\,dG(y) \quad (2)$$

В дальнейшем доказательству этой теоремы при различных предположениях относительных функций выигрыша и пространств стратегий игроков были посвящены очень многие работы [7, 8, 9]. Ценность этих теорем существования огромная, так как они устанавливают классы функций выигрыша, для которых решения игр существуют.

В ряде случаев знание возможностей структуры решения игры позволяют находить оптимальные стратегии И цену игры путем "отгадывания". На основе теоремы 2 можно вывести ряд правил, позволяющих в случае непрерывной функции выигрыша определять, являются ли угаданные стратегии оптимальными.

Правило 1. Функции $F_0(x)$ и $G_0(y)$ являются оптимальными стратегиями И1 и И2 соответственно, если выполняется одно из двух условий:

1) $E(F, G_0) \leq E(F_0, G_0) \leq E(F_0, G)$ для любых функций распределения $F(x)$ и $G(y)$:
2) $\int_0^1 M(z, y) dG_0(y) \leq E(F_0, G_0) \leq \int_0^1 M(x, w) dF_0(x)$ для любых $z, w \in [0,1]$.

Правило 2. Пусть цена игры равна V, тогда:

1) Функция распределения $F_0(x)$ будет оптимальной стратегией игрока И1 тогда и только тогда, когда для всякого $y \in [0,1]$ $V \leq \int_0^1 M(x,y) d F_0(x)$;

2) Функция распределения $G_0(y)$ будет оптимальной стратегией игрока И2 тогда и только тогда, когда для всякого $x \in [0,1]$ $\int_0^1 M(x,y) d G_0(x) \leq V$;

Правило 3. Действительное число V и функции распределения $F_0(x)$ и $G_0(y)$, одновременно удовлетворяющие условию $\int_0^1 M(x,y) d G_0(x) \leq V \leq \int_0^1 M(x,y) d F_0(x)$, являются соответственно ценой игры и оптимальными стратегиями для первого и второго игроков.

Правило 4. Пусть известна либо оптимальная стратегия $F_0(x)$ игрока И1, либо оптимальная стратегия $G_0(y)$ игрока И2. Тогда цена игры может быть найдена по одной из формул

$$V = \max_{0 \leq x \leq 1} \int_0^1 M(x,y) d G_0(x)$$

$$V = \min_{0 \leq y \leq 1} \int_0^1 M(x,y) d F_0(x)$$

Справедливость этих правил непосредственно следует из теоремы 2. При этом, первое условие правила 1 является определением седловой точки функционала E(F,G), а второе условие вытекает из первого если в нем взять

$$F(x)=I_z(x)=\begin{cases}1, x \geq z \\ 0, x < z\end{cases}$$

$$G(y)=I\omega\,(y)=\begin{cases}1, y \geq \omega \\ 0, y < \omega\end{cases}$$

Чтобы убедится в том, что из второго условия вытекает первое, предположим, что для всех z и ω в $[0,1]$ имеем:

$$\int_0^1 M(z, y) dG_0(y) \leq E(F_0, G_0) \leq \int_0^1 M(x, \omega) dF_0(x)$$

Тогда для любых функций распределения F(x) и G(y) получим

$$\iint_{0\,0}^{1\,1} M(z,y)dG_0(y)dF(z) \leq$$

$$\leq \int_0^1 E(F_0,G_0)dF(z) = E(F_0,G_0) =$$

$$= \int_0^1 E(F_0,G_0)dG(\omega) \leq \iint M(x,\omega)dF_0(z)dG(\omega)$$

Этим и завершается доказательство правила 1. Все остальные правила являются различными модификациями правила 1.

Решением игры И(M,[0,1]) с функцией выигрыша M(x,y) (0≤x,y≤1) называют пару функцией распределения F* G*(стратегии) и вещественное число V (значение игры), удовлетворяющее условию

$$\int_0^1 M(x,y)dG^*(y) \leq V \leq \int_0^1 M(x,y)d\,F^*(x),\ \ 0 \leq x,y \leq 1$$

Отсюда следует, что если игрок И1 использует стратегию F^* то средний выигрыш:

$$F(F^*,G) = \iint_{0\,0}^{1\,1} M(x,y)dF^*(x)dG(y)$$

не может быть меньше числа V, т.е. игрок И1 как бы нейтрализует действия противника. И, наоборот, если игрок И2 принимает стратегию G^*, то его средний проигрыш $F(F,G^*)$ будет всегда не больше V, независимо от действий игрока И1. Поэтому естественно, что каждый игрок должен стремится к выбору таких функций распределения F* и G*, которые бы нейтрализовали действия противника. Ведь для игрока И1 лучшей является такая стратегия, которая делает в пределах разумного как можно большим его средний выигрыш вне зависимости от действий противника. Наоборот, игрок И2 должен подобрать себе стратегию, которая обеспечивала бы ему в пределах разумного как можно меньший проигрыш, не зависящий от действий игрока И1. Естественно, что если в игре существует положение равновесия на пространстве функций распределения, то только в этом случае игроки могут выбрать оптимальные стратегии.

Вообще игрок И1 может гарантировать себе выигрыш не менее

$$V_1 = \max_F \min_G \int_0^1 E_1(F)dG(y) = \max_F \min_y E_1[F(y)], \qquad (3)$$

где $E_1(F) = \int_0^1 M(x,y)dF(x)$

Аналогично игрок И2 соответствующим выбором функции распределения G(y) может гарантировать себе проигрыш не более

$$V_2 = \min_G \max_F \int_0^1 E_2\,(G)dF(x) = \min_G \max_x E_2[G(x)], \qquad (4)$$

где $E_2(G) = \int_0^1 M(x,y)dG(y)$

Из (3) и (4) получаем

$$V_1 > \min_y E_1(F), \quad (5)$$

$$V_2 \leq \max_x E_2(G).$$

Пусть теперь игрок И2 выбрал в качестве своей стратегии функцию, распределения $G_0(y)$, и пусть этот выбор стал известен игроку И1. Естественно, предполагая такую возможность, игрок И2 должен стремится найти устойчивую стратегию. Из (5) ясно, что если величина $E_2(G)$ имеет максимум, то игрок И1 всегда будет получать наилучший результат, выбирая такую точку x_0, которая соответствует этому максимуму:

$$V_2 \leq E_2[G(x_0)] = \max_x E_2[G(x)]$$

Для игрока И2 было бы выгоднее довести величину $E_2[G(x)]$ до минимума, но это возможно не всегда, так как он не может влиять на вид функции выигрыша и выбор x_0 игроком И1. Тем не менее игрок И2 может в любом случае попытаться так выбрать стратегию $G_0(y)$, чтобы величина $E_2(G)$ не имела единственного максимума, т.е. чтобы ее «кривая» имела плоскую вершину.

Аналогично, если игрок И2 узнал стратегию игрока И1, то он всегда выберет точку y_0, в которой функция $E_1[F(y)]$ минимальная. В этом случае задачей игрока И1 является выбор такой стратегии $F_0(x)$, чтобы функция$E_1[F(y)]$ не имела единственного минимума.

Обозначим $\theta_1 = \{x: E_2[G(x)] = \gamma_1 = const\}$ и $\theta_2 = \{y: E_1[F(y)] = \gamma_2 = const\}$, где γ_1и γ_2 – произвольные действительные числа, причем $V_1 \leq \gamma_1 \leq \gamma_2 \leq V_2$.

Если существует такая пара действительных чисел (γ_1, γ_2) и пара функций распределения (F, G), что одновременно удовлетворяет условия:

$$E_1[F(y)]\begin{cases} = \gamma_1 \text{ при } y = \theta_2, \\ > \gamma_1 \text{при } y \neq \theta_2, \end{cases} \quad (6)$$

$$E_2[G(x)]\begin{cases} = \gamma_2 \text{ при } x = \theta_1, \\ < \gamma_2 \text{при } x \neq \theta_1, \end{cases} \quad (7)$$

тогда функции Fи G будем называть устой живыми (выравнивающими [8, 9, 10]) стратегиями.

Выводы

Вопрос о существовании устойчивых стратегий для функции выигрыша M(x,y) в большинстве случаев информационного противоборства весьма важно. Сама схема похождения устойчивых стратегий оказывается очень полезной во многих задачах и, в частности, в теории игр с выбором момента времени. Для таких игр не требуется определения стратегий, которые обеспечивают нейтрализацию противника. Вместо них можно использовать частично устойчивые стратегии т.е. стратегии, которые обеспечивают игроку устойчивое положение в некотором подинтервале единичного интервала. Следовательно, она позволяет

проанализировать и обеспечить действенное противодействие в информационном противоборстве двух сторон.

ЛИТЕРАТУРА

1. Пирцхалава Л.Г., Хорошко В.А., Хохлачёва Ю.Е., Шелест М.Е. Информационное противоборство в современных условиях – К: ЦП «Компринт», 2019. – 226с.
2. Грищук Р.В., Каптін І.О., Охрімчук В.В. Технологічні аспекти інформаційного протиборства на сучасному етапі // Загист інформації, 2015, Т.17, №1. – С. 80-86.
3. Хорошко В.О., Іванченко І.С. Інформаційне протиборство в геополітичному просторі // Сучасна спеціальна техніка, 2019, №3 (58). – С. 26-37.
4. Грищук Р.В., Левченко О.В. Аналіз сучасно стану методичного апарату побудови та функціонування систем забезпечення інформаційної безпеки та оборони // Інформаційна безпека, 2018, №3 (31). – С. 5-15.
5. Браіловський М. М., І. С. Іванченко, І. Р. Опірський, В. О. Хорошко Інформаційно-психологічне протиборство в Україні // Безпека інформації. Том 25, № 3 (2019) С.144-149
6. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кібер простори: проблеми безпеки, методи та засоби боротьби – К: ТОВ «СІК ГРУП Україна», 2015. – 449с.
7. Блекуэлл Д., Гиршик М. Теория игр и статистических решений. Изд. 2-е – М.: Изд. Иностранной лит., 2008-260с.
8. Карлин С. Математические методы в теории игр, программировании и экономике. Изд.2 – М: Изд. «Мир»; 2000.-366с.
9. Воробьев Н.Н. Основы теории игр. – М:Изд. Нация, 1984.-496с.
10. Мулен Э. Теория игр – М:Изд. Мир, 1983 – 199с.