# SPCSJ

# SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL4 No1
MARCH 2020

ISSN 2587-4667

**Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 1 - 13 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# Cyber Hygiene Assessment for end users – a case study of Georgia

# საბოლოო მომხმარებლების კიბერჰიგიენის შეფასება - კვლევა საქართველოს მაგალითზე

Giorgi Akhalaia
Caucasus University, Caucasus School of Technology

**აბსტრაქტი** საქართველოში ბოლო რამდენი ათწლეულია ტექნოლოგიური რეფორმა მიმდინარეობს. G2G, G2B, G2C, B2B ტიპის სერვისების უმეტესობამ ონლაინ პლათფორმებზე გადაინაცვლა. საინფორმაციო და საკომუნიკაციო ტექნოლოგიებზე (ICT) მზარდი დამოკიდებულება თავის მხრივ მნიშვნელოვანად ზრდის საფრთხეს პერსონალური, კორპორატიული თუ სახელმწიფო ინფორმაციისა და ინტერესების დაცვის კუთხით.

მომხმარებელი არის კიბერუსაფრთხოების ერთ-ერთი მთავარი და ამავდროულად ყველაზე სუსტი რგოლი. შესაბამისად კიბერუსაფრთხოების უზრუნველყოფა უნდა დაიწყოს მომხმარებელთა ცნობიერების ამაღლებით, კიბერჰიგიენის მოწესრიგებით. სტატია მიმართულია არსებული მდგომარეობის შეფასების, მოწყვლადი საფრთხეების იდენტიფიცირებისა და შესაბამისი რეკომენდაციების შემუშავებისაკენ. სამაგიდო კვლევის პარალელურად ჩატარდა კომპიუტერული სისტემის მომხმარებლების გამოკითხვა, რათა რეალურად გამოვლენილიყო ყველაზე ხშირად დაშვებული შეცდომები. კვლევისას ძირითადი აქცენტი გაკეთდა სოციალურ ინჟინერიაზე, პაროლის მართვის პოლიტიკაზე, ელექტრონული ფოსტის გამოყენების უნარჩვევებზე, უკაბელო ქსელის პარამეტრებსა და გამოყენების პრინციპებზე, არალიცენზირებულ პროგრამებსა და სხვა კიბერჰიგიენისთვის აუცილებელ პარამეტრებზე. კვლევამ აჩვენა, რომ ძალიან დაბალი ცნობიერებაა ამ კუთხით მომხმარებელში. სამწუხაროდ, უმეტეს შემთხვევაში მთავარი აქცენტი კეთდება აპარატურულ ნაწილზე და მომხმარებლის ფაქტორი ხშირად უყურადღებოდ რჩება. სტატიაზე მუშაობისას გამოვლინდა, რომ არ არსებობს შესაბამისი კანონმდებლობა, რომელიც კიბერუსაფრთხოების ეროვნული სტრატეგიის შესაბამისად დაარეგულირებს საქართველოს კიბერსივრცეს.

**საკვანძო სიტყვები**: Cyber Hygiene, Cyber Security, Cyber Crime in Georgia, Cyber hygiene assessment, end user awareness

**ABSTRACT.** Within the last decades, technological reforms are running in Georgia. A big part of G2G, G2B, G2C, B2B services moved to online platforms. With the grow of dependence on informational and communicational technologies (ICT) increases the risk of threats on personal, corporate or governmental informational and security. The user is the most important and together with this, the weakest point of cyber security. So, insuring cyber security must be started from raising awareness and cyber hygiene level of the users. The paper is focused on assessing the existing environment, identification of vulnerable weaknesses and on developing of corresponding recommendations. Together with the main research, the survey of the

users of the system was performed to identify most common mistakes from practice. The main accent of the research was made on social engineering. Passwords policies, skills of using e-mails, using of wireless network configuration parameters, use of illegal software and other required parameters of cyber hygiene. The research showed, that the awareness of the users in this field is very weak. Unfortunately, usually the main accent was made on hardware and user factor was left without needed attention. During the research was identified, that corresponding legislation, which would regulate security processes based on national strategic regulations, did not exist.

**Keywords:** *Cyber Hygiene, Cyber Security, Cyber Crime in Georgia, Cyber hygiene assessment, end user awareness*

იმის გათვალისწინებით, რომ მომხმარებელი არის კიბერუსაფრთხოების მთავარი და ამავდროულად ყველაზე სუსტი რგოლი, აუცილებელია შემუშავდეს სწორი სტრატეგია, რომლითაც მოხდება კიბერუსაფრთხოების ელემენტების ინტეგრირება ყოველდღიურ საქმიანობაში. სწორი სტრატეგიის წინაპირობაა არსებული მდგომარეობის, რეალობის შეფასება. კითხვარი ეხება მომხმარებლის ისეთ უნარ-ჩვევებს რომელსაც იგი ყოველდღიურად იყენებს და უმნიშვნელოვანესია პირადი, კორპორატიული თუ სახელმწიფო კიბერუსაფრთხოებისთვის. სამიზნე კატეგორია იყო კომპიუტერული მოწყობილობების ნებისმიერი ასაკობრივი თუ სოციალური ჯგუფის მომხმარებელი. განსაკუთრებით მნიშვნელოვანია რამდენიმე კატეგორია, მათ შორის სკოლის მოსწავლეების შედეგები. გამომდინარე იქიდან, რომ ამ ასაკში ყველაზე ნაკლებად ელოდება მოზარდი საფრთხეს და აქტიურად იყენებს ინტერნეტ სივრცეში არსებულ ინფორმაციას. ასევე იურისტები და ფინანსისტები, რომლებსაც შეხება აქვთ ფინანსურ და იურიდიულ დოკუმენტაციასთან. კრიტიკულად მნიშვნელოვანია მენეჯერულ პოზიციაზე მომუშავე ხალხის კიბერჰიგიენა, რადგან ისინი განსაზღვრავენ ძირითადად მიმართულებასა და სტრატეგიას. ამიტომ მაქსიმალურად უნდა იყვნენ გათვიცნობიერებულები კიბერუსაფრთხოების ძირითად პრინციპებში.

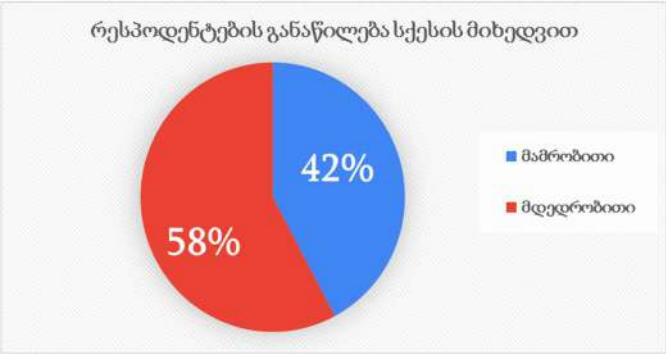
მნიშვნელოვანი იყო კვლევაში მონაწილეობა მიეღო გეოგრაფიულად სხვადასხვა არეალში მცხოვრებ მოსახლეობას, რადგან დაგვენახა ზოგადი სურათი და არა რომელიმე კონკრეტულად დასახლებული პუნქტის შედეგები.

რაც შეეხება უშუალოდ კითხვების სტრუქტურას, გამოყენებული იყო როგორც დახურული ასევე ღია კითხვები. კითხვები მაქსიმალურად მოიცავდა იმ თემებს რასაც მომხმარებელი ყოველდღიურად ეხება. კვლევა ჩატარებულია “Google Form” ის საშუალებით. რაც ამარტივებდა მის გავრცელებასა და შევსების ეტაპებს.

კვლევა იწყება ზოგადი ინფორმაციის შეგროვებით, როგორიცაა ასაკი, სქესი, დასაქმების ადგილი და სამუშაოს ტიპი, რადგან სწორად განისაზღვროს ყველაზე სუსტი კატეგორია. საინტერესოა მონაწილეების უკუკავშირი. რესპოდენტების ნაწილი თვლიდა, რომ აღნიშნული საკითხების ცოდნა სასურველია, მაგრამ არა აუცილებელი, რადგან უსაფრთხოება IT_ის პასუხისმგებლობაა. ვინც პროფესიით IT იყო, ისინი (უმეტესობა) პროტესტს გამოთქვამდნენ, თუ რატო უნდა ხვდებოდეს ჩვეულებრივი, არა IT განათლების მქონე

მომხმარებელი კვლევაში დასმულ კითხვებსაც კი. რეალურად, ეს პრობლემის სათავეა, რადგან კიბერუსაფრთხოება ყველას პასუხისმგებლობაა და შეუძლებელია მხოლოდ IT ჯგუფმა უზრუნველყოს მთლიანი კომპანიის უსაფრთხოება. მითუმეტეს კვლევა კონცენტრირებულია კიბერჰიგიენის იმ ზოგად უნარ-ჩვევებზე, რომლებიც აუცილებელია ყველასთვის, ვინც კომპიუტერულ სისტემას იყენებს, პირადი თუ კორპორატიული ინტერესებისთვის. ადამიანები დიდ ყურადღებას აქცევენ ჰიგიენას სტომატოლოგიურ კლინიკებში, სახლებსა და სასტუმროებში, სილამაზის სალონებსა და საავადმყოფოებში, მაგრამ ვერ ათვიცნობიერებენ რაოდენ მნიშვნელოვანია ეს უკანასკნელი კომპიუტერულ სისტემებში. სამწუხაროდ, საქართველოში ტექნიკური განათლების ხალხის უმეტესობა ვერ ხედავს კიბერჰიგიენის აუცილებლობას.

კვლევაში სულ მონაწილეობა მიიღო 154_მა ადამიანმა. აქედან 65 წარმოადგენდა მამრობით სქესს, ხოლო 89 მდედრობითს (იხ. Fig 1).



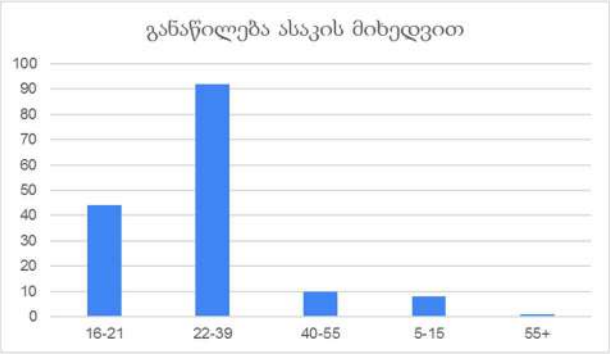




Fig. 1

განათლების მიხედვით კი ასე ნაწილდება (იხ. Fig. 2). 87 ს აქვს უმაღლესი განათლება, 45 სტუდენტია, საშუალოა განათლება აქვს 12 ს, ხოლო პროფესიული 6 ს გამოკითხულს.

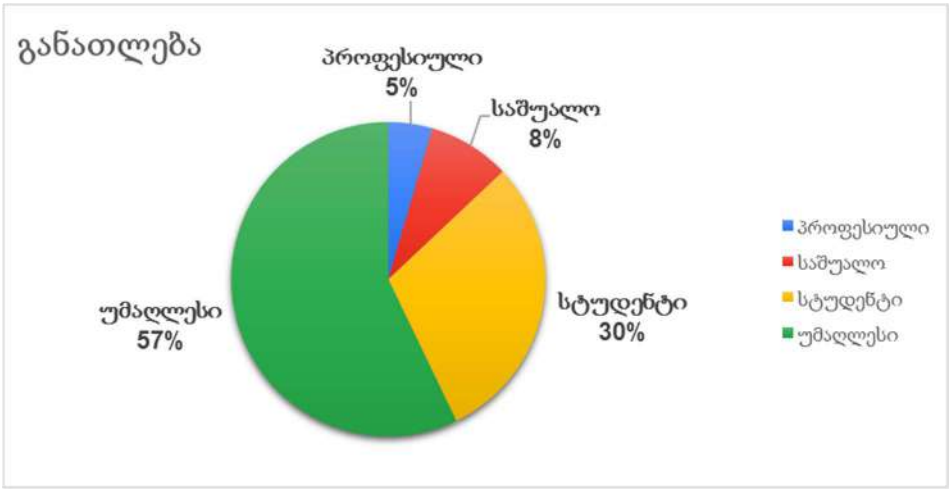



Fig2.

პირველი კითხვა ეხებოდა ზოგადად იყენებს თუ არა რესპოდენტი არალიცენზირებულ, ე.წ. გატეხილ პროგრამებს. ეს დეტალი მნიშვნელოვანია იმდენად, რამდენადაც ამ კითხვაზე დადებითი პასუხის შემთხვევაში აზრს კარგავს უსაფრთხოების სისტემები, რამდენადაც ძვირადღირებული არ უნდა იყოს ეს უკანასკნელი. გატეხილი პროგრამა თავდამსხმელის მხრიდან ე.წ. backdoor ის ინექციის პირდაპირი რისკია. ეს გულისხმობს, რომ მომხმარებელი საკუთარი ნებით აძლევს პოტენციურ თავდამსხმელს არსებულ კომპიუტერულ მოწყობილობაზე წვდომას. ანუ, შიგნიდან ვუხსნით არხს, რომლის საშუალებითაც შეძლებს კომპიუტერულ სისტემაში სხვადასხვა ტიპის მანიპულაციას.

იყენებენ ან გამოუყენებიათ თუ არა არალიცენზირებული, ე.წ. გატეხილი პროგრამები, გამოკითხულთა არანაკლებ 79% მა უპასუხა - კი (იხ. Fig. 3). რაც კრიტიკულად ცუდი შედეგია. თუ შემდეგი კითხვის პასუხებსაც გავაანალიზებთ, ვნახავთ, რომ რეალურად კიდევ უფრო უარესი მდგომარეობაა. კითხვაზე რამდენად ხშირად იყენებენ პროგრამის აქტივატორებს 69%_მა უპასუხა „იშვიათად“, ხოლო 27%_მა „ხშირად“ (იხ. Fig 4). აქედან გამომდინარე, რეალურად, 96% იყენებს არალიცენზირებულ, გატეხილ პროგრამებს.

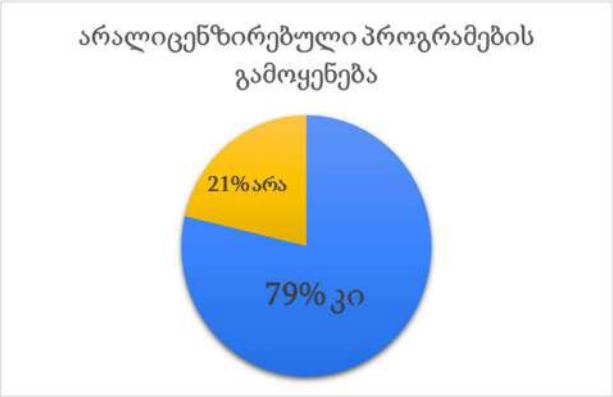



Fig. 3

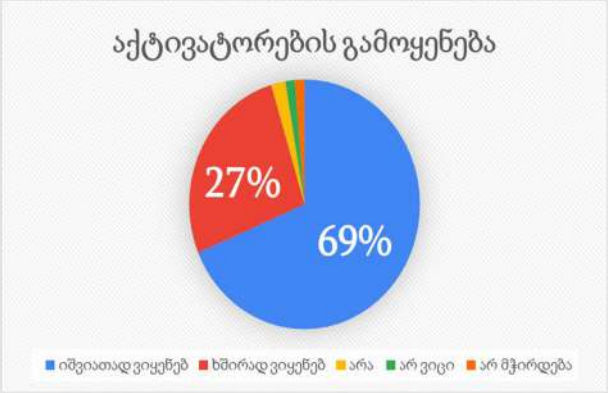



Fig. 4

ასევე ერთი კითხვა გამოყოფილი იყო კონკრეტულად ყიდულობენ თუ არა ოპერაციულ სისტემას. სამწუხაროდ ეს ერთ-ერთი ყველაზე გავრცელებული შეცდომაა რასაც საქართველოში უშვებენ. მკვეთრად მცირდება უსაფრთხოების დონე, თუ ვიყენებთ ე.წ. გატეხილ ოპერაციულ სისტემას. ამ შემთხვევაშიც წინასწარ, გამტეხის მიერ არის კოდში ჩარევა და ჩაკერებული აქვს თავისი კოდი. რა თქმა უნდა, ამ დროსაც backdoor_ის ძალიან დიდი რისკია. ასევე რიგ შემთხვევებში გაუქმებულია მწარმოებლის მიერ მოწოდებული ოპერაციული სისტემის განახლებები. პირველი ორი კითხვიდან უკვე გამოჩნდა, რომ მომხმარებელთა 96% გაუთვიცნობიერებლად თუ გათვიცნობიერებულად, იყენებს უკვე დაჰაკულ პროგრამულ უზრუნველყოფას. თუ ასეთი მომხმარებლების რიცხვს ჩავშლით დასაქმების ადგილის მიხედვით მივიღებთ შემდეგ სურათს (იხ. Fig. 5):

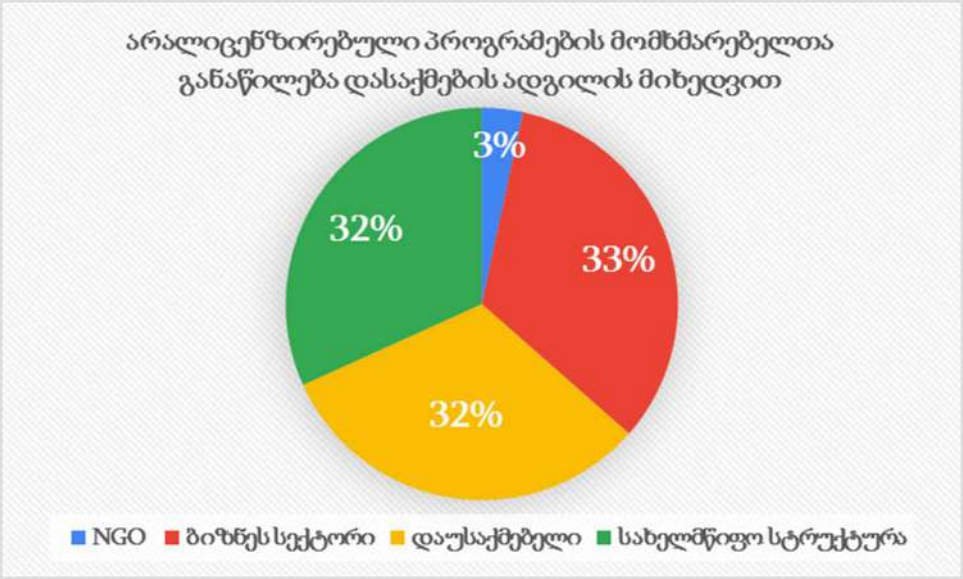



Fig. 5

როგორც დიაგრამაზე ჩანს 32% დასაქმებულია სახელმწიფო სტრუქტურაში, ხოლო 33% ბიზნეს სექტორში. ანუ მომხმარებლების 2/3, რომელთა ხელშიცაა საქართველოს კრიტიკული ინფრასტრუქტურა, იყენებს არალიცენზირებულ, გატეხილ პროგრამას. ანუ პირდაპირ საფრთხეს უქმნის ინფორმაციის, მონაცემების კონფიდენციალურობას. [1]

თავის მხრივ ცალკე პრობლემაა პერიოდული პროგრამული განახლებები. ამიტომ ამის შესახებაც იყო დასმული კითხვა - რამდენად ხშირად აკეთებენ ოპერაციული სისტემებისა და/ან პროგრამების განახლებებს. განახლებებში დამატებით ფუნქციონალთან ერთად მაღალი პრიორიტეტი აქვს უსაფრთხოებას. ყოველ განახლებაში, ეს იქნება ოპერაციული სისტემის თუ რომელიმე პროგრამული უზრუნველყოფის, გასწორებულია ე.წ. bug ები და vulnerabilities. ამიტომ აუცილებელია მომხმარებელმა სისტემატიურად აკეთოს გეგმიური პროგრამული განახლებები. რათა თავიდან აირიდოს არსებული სისუსტეებიდან მოსალოდნელი თავდასხმები. გამოკითხულთა დაახლოებით 63% არ ყიდულობს ოპერაციულ სისტემას. რამდენიმე პროცენტი იყენებს უფასო ოპერაციულ სისტემას(მაგალითად Linux) ხოლო დანარჩენები სხვადასხვა მიზეზის (უმეტესად ფასი) გამო უპირატესობას ანიჭებენ გატეხილ

ვერსიას. ანუ გარდა გატეხილი პროგრამებისა ძირითადად იყენებენ აქტივატორით გატეხილ ოპერაციულ სისტემებს. აქედან გამომდინარე, რამდენიმე გზა არსებობს სისტემაში ე.წ. Malware ების შემოსაღწევად.

გამოკითხულთა საკმაოდ დიდი ნაწილი, 21% არ აკეთებს პროგრამების პერიოდულ განახლებას (იხ. Fig. 6). ფორუმებზე პერიოდულად იდება პროგრამების ახალი სისუსტეების exploit ები. რომელიც საკმაოდ მარტივად ხელმისაწვდომია.


Fig. 6

პერიოდულ განახლებებში გათვალისწინებულია და გამოსწორებულია იმ დროისთვის არსებული სისუსტეები. მაგალითად ერთ-ერთ ყველაზე გავრცელებულ არქივატორს WinRar_ს რამდენიმე თვის წინ უპოვეს bug_ი, რომელიც თავდამსხმელს სისტემაში შეღწევის საშუალებას აძლევდა. ერთი შეხედვით უწყინარი პროგრამა, რომელიც უვადოდ დროებით, ე.წ. Trial ვერსიას თავაზობს მომხმარებელს, წარმოადგენდა და ალბათ ბევრი მომხმარებლისთვის ისევ წარმოადგენს დიდ საფრთხეს. პრობლემა მდგომარებდა შემდეგში: ძველი ვერსიები იყენებდნენ 2006 წელს დაკომპილირებულ .dll (dynamic link library) ფაილს, რომელსაც არ ქონდა დაცვის მექანიზმი. [2]

მომხმარებელთა 61% ძირითადად იყენებს Windows 10 ის ოპერაციულ სისტემას, 16% - Windows 7 და 10% - Windows 8/8.1 _ს. დანარჩენი კი ნაწილდება სხვა ოპერაციულ სისტემაზე. აღსანიშნავია, რომ მხოლოდ 74% აკეთებს ოპერაციული სისტემის განახლებას. რაც უფრო ახალია ოპერაციული სისტემა მით უფრო უსაფრთხოა, შეიძლება ითქვას გათვალისწინებულია წინა ვერსიებში დაშვებულ ხარვეზები. მაგალითად Windows 8/8.1 შედარებით უსაფრთხოა ვიდრე Windows 7. მაგრამ ამათზე უფრო უსაფრთხოა Windows 10. ზოგადად Microsoft ის ოპერაციულ სისტემებზე უსაფრთხოა Mac OS და Linux. ამიტომ უსაფრთხოებაზე საუბრისას აუცილებელია განხილული იყოს ოპერაციული სისტემის ნაწილიც. გამოკითხულთა საკმაოდ ნაწილმა იცის, რომ OS_ის განახლება საჭიროა

უსაფრთხოებისთვის, მაგრამ მიუხედავად ამისა, მაინც არ ანახლებს. ზოგ შემთხვევაში ამის მიზეზი ისევ არალიცენზირებული სისტემაა, რომელიც განახლების შემთხვევაში თავიდან საჭიროებს გააქტიურებას. მაგრამ უმეტეს შემთხვევაში ამის მიზეზია ცნობიერების არ ქონა. რადგან უმეტეს შემთხვევაში უსაფრთხოება მხოლო სიტყვად რჩება და რეალურად ვერ ათვიცნობიერებენ ამას რა შეიძლება მოყვეს.

რაც შეეხება ანტივირუსებს, საკმაოდ ჭრელი სურათია. მეტ ნაკლებად იყენებენ სხვადასხვა პროგრამულ უზრუნველყოფას. აქ ერთი საინტერესო ფაქტი გამოიკვეთა. გამოკითხულთა ნაწილმა არც იცის, რომ ანტივირუსს იყენებს. მაგალითად რესპოდენტების ნაწილს ოპერაციულ სისტემაში მითითებული აქვთ Windows 10, ხოლო იყენებენ თუ არა ანტივირუსს პასუხი აქვთ უარყოფითი. ანუ მომხმარებელთა გარკვეულმა კატეგორიამ ისიც არ იცის, რომ Microsoft ის ოპერაციული სისტემის ბოლო ვერსიებში ანტივირუსი ინტეგრირებულია და სტანდარტულად მოყვება ოპერაციულ სისტემას. მნიშვნელოვანია აქცევენ თუ არა ყურადღებას რომელ ქვეყანაშია ანტივირუსი დაწერილი. რადგან გასათვალისწინებელია ქვეყნის კიბერუსაფრთხოების სტრატეგია. მაგალითად, თუ ქვეყანა სტრატეგიის მიხედვით თვლის რომ რუსეთი კიბერსივრცეში აგრესორია და პოტენციურ თავდამსხმელს წარმოადგენს, მაშინ არ უნდა გამოვიყენოთ რუსეთის მიერ წარმოებული ანტივირუსები. გამომდინარე იქიდან, რომ თუ ანტივირუს აქვს ფაილებთან წვდომა, რაც ბუნებრივია, რადგან ასკანერებს(ამოწმებს საფრთხეებზე) ფაილებს, მაშინ თავისთავად ნათელია რომ ანტივირუსის მწარმოებელსაც ქონდეს ჩვენს სისტემაზე(ფაილებზე) წვდომა.

გამოკითხულთა 60%_ს ერთხელ მაინც გადმოუწერია ფაილი Torrent იდან ან ფორუმიდან. ასეთი ტიპის პლათფორმებზე ხშირად შეუმოწმებელი ფაილებია ატვირთული, რის გამოც კრიტიკულად მაღალია Malware_ის რისკი. ძირითადად გამოიყენებენ გატეხილი, არალიცენზირებული პროგრამების გადმოსაწერად. როგორც წინა პუნქტებში იყო აღნიშნული გატეხილი პროგრამა უკვე შეიცავს უცხო კოდს, რომელიც ავტორმა შესაძლოა თავისი ინტერესებიდან გამომდინარე ცვალოს და შედეგად მოიპოვოს არა ავტორიზებული წვდომა სისტემაზე.

თანამედროვე სამყაროში, საბანკო სერვისებმა, ფილიალებიდან ონლაინ პლათფორმებზე გადმოინაცვლა. საქართველოს პოლიტიკაც აქტიურად მიმართულია ელექტრონული მმართველობის დანერგვისაკენ. აქედან გამომდინარე ონლაინ პლათფორმებზე განთავსებულია როგორც პერსონალური ინფორმაცია ასევე საბანკო ტრანზაქციები. ამიტომ მნიშვნელოვანია მომხმარებელი სწორად, ანუ უსაფრთხოდ იყენებდეს ინტერნეტ და მობაილ ბანკის სერვისებს. რესპოდენტების 90% იყენებს გადახდების ონლაინ სერვისებს (იხ. Fig. 7). დეტალებში რო ჩაიშალოს: 66% ხშირად, ხოლო 24% იშვიათად, მაგრამ მაინც იყენებს ამ სერვისებს.

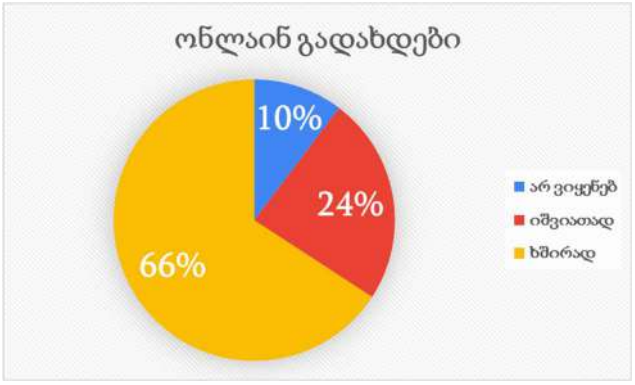



Fig. 7

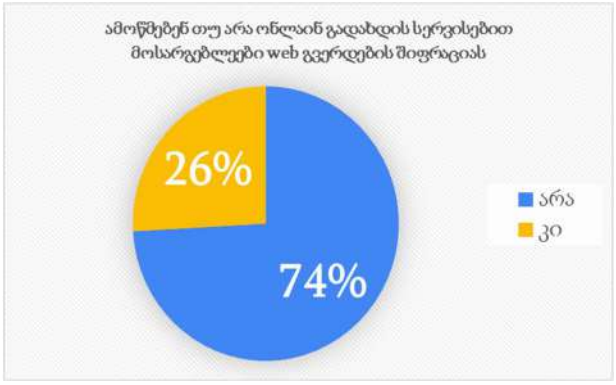



Fig. 8

კითხვაზე, ამოწმებენ თუ არა გახსნილი web გვერდის შიფრაციას, 75%_ს უარყოფითი პასუხი ქონდა. კვლევის თანახმად ონლაინ გადახდით მოსარგებლეთა 74% არ ამოწმებს გახსნილი web გვერდის შიფრაციას (იხ. Fig. 8). ამ ორი კითხვიდან გამომდინარე, კომპიუტერული სისტემით მოსარგებლეთა 66%_ი მარტივად შეიძლება გახდეს თუნდაც DNS spoofing_ის მსხვერპლი და მათი ანგარიშიდან მოხდეს არალეგალური ტრანზაქცია.

პაროლების შერჩევის პოლიტიკაშიც საკმაოდ სავალალო მდგომარეობაა. გამოკითხულთა 70% ერთსა და იმავე პაროლს იყენებს სხვადასხვა სერვისზე (იხ. Fig. 9). თუ რომელიმე ერთი სერვისის პაროლს გაიგებს თავდამსხმელი, მაშინ დიდი ალბათობით სხვა სერვისებზეც ექნება წვდომა.

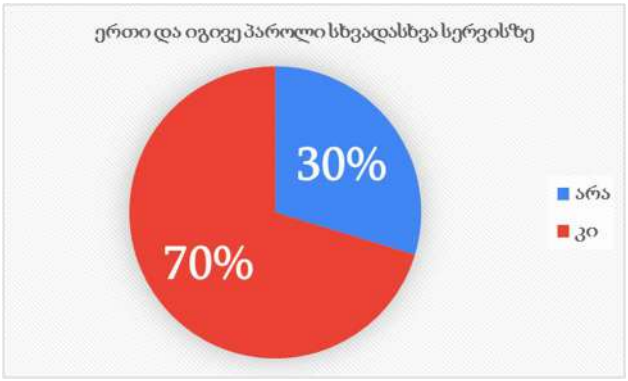



Fig 9

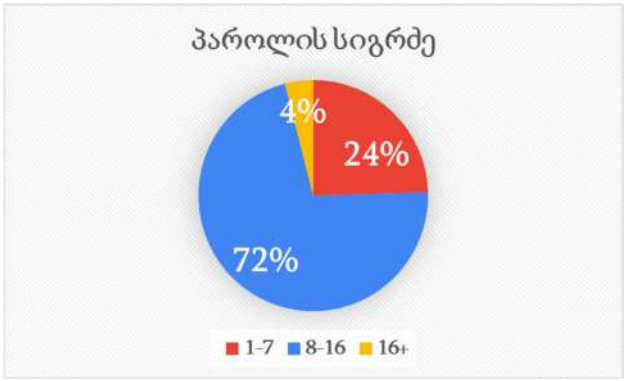



Fig. 10

72% იყენებს 8-16 სიგრძის პაროლს, რაც ნორმალურია (იხ. Fig. 10). მაგრამ აქ გასათვალისწინებელია ისიც, რომ დღესდღეობით ახალ სერვისებს შეზღუდვა აქვს პაროლის სიგრძეზე, რის გამოც ფიზიკურად ვერ გამოიყენებ 8 სიმბოლოზე ნაკლები სიგრძის პაროლს.

ამ კითხვარში, სპეციალურად იყო ერთი კითხვა ისე ფორმულირებული, რომ რესპოდენტს საშუალებას აძლევდა, სურვილის შემთხვევაში დაეწერა თავისი პაროლი. სამწუხაროდ რამდენიმე მომხმარებელმა თავისი პაროლი დაწერა. გარდა იმისა, რომ ღიად დაწერეს პაროლი, თვითონ პაროლის სტრუქტურაც ძალიან სუსტი იყო. ძირითადად გამოყენებული აქვთ ოჯახის წევრის, უმეტესად შვილის სახელი და თარიღები. რაც კრიტიკულად დაუშვებელია პაროლების მართვის პოლიტიკაში.

ერთ-ერთ ყველაზე გავრცელებულ კიბერსაფრთხეს წარმოადგენს ე.წ. phishing. ამიტომ საინტერესოა საქართველოს მოსახლეობის შეფასება email ებთან ყველაზე მეტად დაშვებული პრობლემების ჭრილში. გამოკითხულთა 63% ყოველდღე იყენებს ელექტრონულ ფოსტას (იხ. Fig. 11). თუ დავუმატებთ იმ რაოდენობას, რომელიც კვირაში რამდენჯერმე იყენებს email_ს, მაშინ 84% ს მივიღებთ. ეს კატეგორია მოწყვლადია მეილებთან დაკავშირებული კიბერშეტევებისთვის. მაგალითად phishing_ისთვის. გამოკითხულთა 77% არ ამოწმებს მიღებული ელექტრონული ფოსტის შიფრაციის დეტალებს (იხ. Fig. 12).


Fig. 11

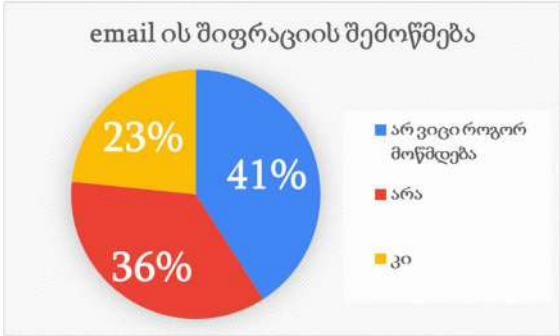



Fig. 12

გამოკითხულთა მინიმუმ 41%_მა არც კი იცის როგორ მოწმდება email ის უსაფრთხოება. რესპოდენტების 38% არ ამოწმებს ელ-ფოსტის გამომგზავნის მისამართის სისწორეს. ისინი ძალიან მარტივად შეიძლება აღმოჩდნენ email თაღლითობის მსხვერპლი. დაინტერესებულმა პირმა, შესაძლოა რეალური მეილის მისამართში ერთი რომელიმე ასოს ამოღებით ან სხვა მიმსგავსებულ სიმბოლოთი ჩანაცვლებით ისე შენიღბოს საკუთარი მეილი, რომ ზედმეტი ძალისხმევის გარეშე მოიპოვოს სასურველი ინფორმაცი. თუ ამ ორი პარამეტრის შედეგს დავთვლით მხოლოდ იმ რესპოდენტებისთვის, რომლებიც კვირაში რამდენჯერმე ან ყოველდღე იყენებენ ელექტრონულ ფოსტას მაშინ მივიღებთ შემდეგ სურათს:


Fig. 13

თუ კიდე უფრო ჩავუღრმავდებით, ვნახავთ, რომ email_ის აქტიურ მომხმარებელთა 73% დან, რომლებიც არ ამოწმებენ მიღებული შეტყობინების შიფრაციის დეტალებს (იხ. Fig. 13), 44% არც გამომგზავნის მისამართის სისწორეს ამოწმებს. აქედან გამომდინარე, შეიძლება ითქვას, რომ ასეთი მომხმარებლები, „მზად არიან“ გახდნენ email შეტყობინებებით განხორციელებულ კიბერკრიმინალის მსხვერპლი, მაგალითად phishing_ის. ეს კატეგორია წარმოადგენს, გამოკითხულთა საერთო რაოდენობის 27 %_ს. რაც საკმაოდ ცუდი მაჩვენებელია. თუ გავითვალისწინებთ, იმ ფაქტსაც, რომ ელექტრონულ ფოსტას აქვს იურიდიული ძალა, ანუ ასეთი წერილი შეიძლება გახდეს მნიშვნელოვანი გადაწყვეტილების წყარო, უნდა ვივარაუდოთ, რომ რეალურად გაცილებით მაშტაბური ზარალი/ზიანი შეიძლება მიადგეს კომპანიას ვიდრე მხოლოდ რომელიმე ერთი ფიზიკური პირის პირად თუ საბანკო ინფორმაციაზე წვდომის მოპოვებაა.

აღსანიშნავია ის ფაქტი, რომ მხოლო 21% ხსნის, გადადის ელექტრონული საშუალებებით მიღებულ რეკლამაზე. მსგავსი ტიპის რეკლამები რეალურად გარკვეულ რისკს შეიცავს. რადგან თითოეული ბმულის უკან შესაძლოა მავნე კოდი იმალებოდეს, რომელსაც ბმულზე გადასვლით გაშვების ნებართვას ვაძლევთ. შესაბამისად სანამ რეკლამაზე გადავა მომხმარებელი კარგად უნდა გადამოწმდეს ვისგან არის რეკლამა და რამდენად რეალურია იგი. მაგალითად თუ მეილის შინაარსი იწყება ზოგადი მომართვით და არა კერძო სახელით ან გვარით, ან გამომგზავნი ადრესატისგან რაღაცის დაუყონებლივ შესრულებას ითხოვს, ეს შეიძლება იყოს ბმულზე გადასვლა, რაღაცის გამოწერა, დათანხმება რაიმე საჩუქარზე და ასე შემდეგ - უკვე მაღალი რისკის შემცველია. ამით თავდამსხმელი ცდილობს ააჩქაროს ადრესატი და ნაკლები დრო დაუტოვოს შინაარსის გასააზრებლად.

გამოკითხულთა 55% არ ამოწმებს რომელი ქვეყნისთვისაა წარმოებული შესაძენი პროდუქტი. დანარჩენი 45% მიზეზად უთითებს თავსებადობას ქვეყნის სტანდარტებთან, როგორიცაა ძაბვა, სიხშირეები და ასე შემდეგ. ერთმა რესპოდენტმა მიუთითა რომ ამოწმებს ორი მიზეზის გამო. პირველი თავსებადობა ქართულ ტექნიკურ პარამეტრებთან და მეორე

რუსული ბაზრისთვის განკუთვნილი პროდუქციის აცილება. სამწუხაროდ მხოლოდ ერთ ადამიანთან იყო ნახსენები რუსეთი. რეგიონალური პროვაიდერების დონეზე, იმავე ფრთის ქვეშ ვართ, რომელშიც რუსეთის ფედერაციაა. ოფიციალური ტექნიკის იმპორტი კი რუსეთის გავლით ხდება. პრობლემა მდგომარეობს რუსეთის შიდა პოლიტიკაში (რასაც არ მალავენ). მათ აქვთ ყველა იმ მოწყობილობის შიფრაციის გასაღები, რომელიც მათი ქვეყნის გავლით მიეწოდება მიმღებს. შესაბამისად, ქვეყანაში, რომელსაც კიბერუსაფრთხოების ეროვნული სტრატეგიის მიხედვით (2017-2018 წლების) რუსეთის ფედერაცია განსაზღვრული ყავს როგორ კიბერდომეინში აგრესორად და საფრთხედ ჩვენი კიბერსივრცისთვის, არ უნდა შემოდიოდეს რუსეთის ფედერაცია გამოვლილი ტექნიკა. თუმცა ამ კუთხით საკმაოდ დიდი პრობლემაა საკანონმდებლო დონეზე. არათუ ფიზიკური პირისთვის, არამედ სახელმწიფო ტენდერებშიც კი არ არის ჩადებული მსგავსი შეზღუდვა.

კითხვაზე, იყენებენ თუ არა WiFi ქსელს საზოგადოებრივი თავშეყრის ადგილებში, ტრანსპორტში, კაფეებსა და სკვერებში იქ სადაც საერთო მოხმარების, ღია WiFi ქსელი არსებობს, შემდეგნაირად გადანაწილდა პასუხები:

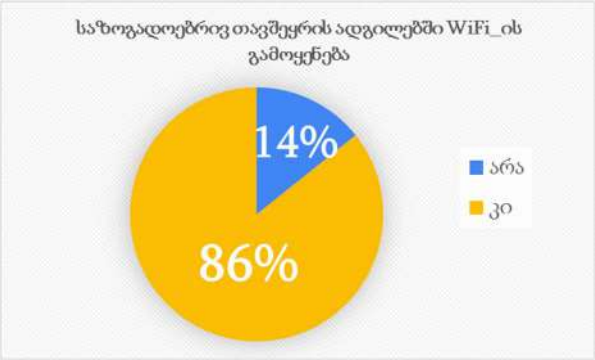



Fig. 14

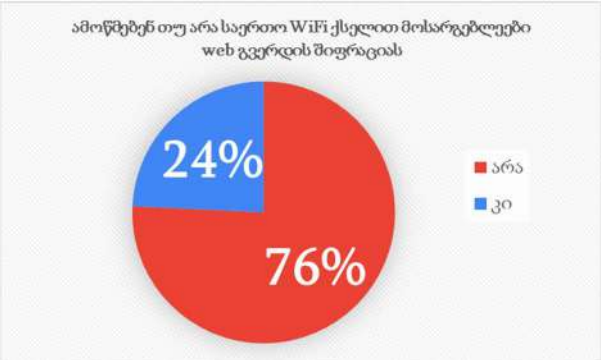



Fig. 15

ასეთი ტიპის ქსელი ძალიან სუსტადაა დაცული. შესაბამისად, მარტივია სხვადასხვა პროგრამული პაკეტით ქსელის მოსმენა და ინფორმაციის მოპარვა. გამოკითხულთა 86% იყენებს ღია, საერთო გამოყენების WiFi ქსელს (იხ. Fig. 14), აქედან 76% გახსნილი ვებ გვერდის შიფრაციასაც კი არ ამოწმებს (იხ. Fig. 15), რაც საერთო რაოდენობის 54%_ია. აქედან გამომდინარე, მომხმარებელთა 54%_სგან მარტივად შეიძლება ინფორმაციის, მონაცემების არალეგალურად მოპოვება. მათი ინფორმაცია საკმაოდ დაუცველია საზოგადოებრივი თავშეყრის ადგილებში. არ შეიძლება ასეთი ქსელით სარგებლობისას პერსონალური ინფორმაციის, ავტორიზაციის პარამეტრებისა და საბანკო ინფორმაციის ქსელში გამოყენება. მსგავსი ტიპის ქსელი უნდა გამოიყენონ მხოლოდ განსაკუთრებულ, გადაუდებელ სიტუაციებში ან ისეთი ინფორმაციის გასაზიარებლად რომლის მესამე პირის ხელში მოხვედრა, არ გამოიწვევს მატერიალურ, თუ ფიზიკურ ზარალს.

თუ ჰაკერი წვდომას მოიპოვებს კომპიუტერულ სისტემაზე, ბოლო ბარიერი ხდება შიფრაცია. წინამდებარე კითხვებით მიღებული შედეგებიდან გამომდინარე, ცხადია

მონაცემების დაშიფვრაზე რა პასუხებიც იქნება. გამოკითხულთა 94% არ აკეთებს მონაცემების შიფრაციას.

დასაქმებულთა მხოლოდ 9%_მა უპასუხა დადებითად კითხვას: აკეთებთ, თუ არა შეღწევადობის ტესტებს (pentesting) თქვენი ორგანიზაციის/კომპანიის web გვერდზე. 12%_მა მიუთითა, რომ ორგანიზაციას არ აქვს web გვერდი. ხოლო 79% მა უარყოფითი პასუხი დააფიქსირა. ბოლო პერიოდში, გახშირდა სხვადასხვა კომპანიის სერვერებზე თავდასხმა, რომელიც საკმაოდ წარმატებით გამოსდით. Pentesting არ ნიშნავს იმას, რომ სერვერი გაუტეხელი გახდება. ამ დროს შესაბამისი პროგრამული პაკეტებით სერვერი მოწმდება იმ დროისათვის ცნობილ exploit ებზე, სისუსტეებზე. ასე ვთქვათ, ჰაკერის, თავდასხმის სიმულაციას ასრულებს ტესტერი, ეთიკური ჰაკერი. ამიტომ თუ წინასწარ, პერიოდულად ჩაატარებენ ვებ გვერდის, სერვერების შეღწევადობის ტესტებს, მაშინ რისკები მინიმალურამდე იქნება დაყვანილი. სამწუხაროდ, ამის კულტურა საქართველოში არ არის და შესაბამის მარტივადაც ხდება ორგანიზაციების სერვერების პარალიზება მარტივი კიბერთავდასხმების დროსაც კი. რეალურად, თავდასხმის, და ზარალის დადგომის შემდეგ იწყებენ რეაგირებას, რაც არასწორი მიდგომაა.

საერთო ჯამში, შედგები კიდე უფრო თვალნათლივ აჩვენებს, რომ სამომხმარებლო გარემოში, კიბერუსაფრთხოების ცნობიერების ძალიან დაბალი დონეა. ფიზიკურ პირზე იქნება თუ ბიზნესზე კიბერშეტევა, საბოლოოდ მაინც სახელმწიფოზე აისახება. ამიტომ აუცილებელია სწორი მიდგომითა და სტრატეგიით, პირველ რიგში ამაღლდეს ცნობიერება მომხმარებლებში. კიბერუსაფრთხოება პირობითად შეიძლება დაიყოს ორ ნაწილად: აპარატურულ და ადამიანურ რესურსად. მხოლოდ აპარატურულ ნაწილს ეთმობა ძალიან დიდი ყურადღება. აქვე ხაზგასასმელია ის, რომ თუ სწორად არ გამოიყენებს ადამიანი შესაბამის ტექნოლოგიას, მაშინ მინიმუმამდე დადის მისი, აპარატურის ეფექტურობა.

## ბიბლიოგრაფია

1. 3. სვანაძე, ა.გოცირიძე. *კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები*, მოამზადა კიბერუსაფრთხოების ეროვნულმა ბიურომ, საქართველოს თავდაცვის სამინისტრო, 2015.

2. Mott Nathaniel.2019. Hackers Exploit 19-Year-Old WinRAR Vulnerability. *tom's HARDWARE: 18 of March,2019.* *https://www.tomshardware.com/news/winrar-vulnerability-mcafee-research-cybersecurity-stats,38845.html (ბოლო წვდომა: 17.11.2019)*

3. M. Iavich, S. Gnatyuk, G. Iashvili, A. Fesenko. Cyber security European standards in business. Scientific and Practical Cyber Security Journal (SPCSJ), 3(2):36-39, 2019

**ACKNOWLEDGMENT**

I would like to thank whole team of the SCSA, Caucasus University - Caucasus School of Technology and CYSEC for its valuable involvement and help to do research and develop the ideas presented here.

**Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 14 - 33 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# შრომითი მიგრაციის სამართლებრივი რეგულირების ასპექტები და მისი გავლენა სახლმწიფოს ეკონომიკურ უსაფრთხოებაზე

# Aspects of Legal Regulation of Labor Migration and It's Impact on The Economic Security of The State

**ილია ხუციშვილი**
ნიუ ვიჟენ უნივერსიტეტი, სამართლის დოქტორანტი

**Ilia Khutsishvili**
New Vision University, The Ph.D Programme in Law, Doctoral Student

**ABSTRAC.** International labour migration as a practice has a long history with some turning points. In the recent past, globalization has further enhanced migration, mainly through revolutionary changes in information technology.

The article mainly aims to identify and examine international labour migration theories, deal with the aspects of legal regulation of labor migration and its impact on the national security of the state as well as the economic security.

**Keywords:** Migration Law, Labour Migration, National Security, Economic Security

**ანოტაცია.** მსოფლიოში მიმდინარე გლობალიზაციური პროცესებიდან გამომდინარე, მიგრაცია იქცა გლობალურ ფენომენად და თანამედროვეობის ერთ-ერთ გამოწვევად, რომელიც გავლენას ახდენს ქვეყნის მოსახლეობის სოციალურ-ეკონომიკურ განვითარებაზე, მის უსაფრთხოებასა და სტაბილურობაზე.

მნიშვნელოვანია ისეთი ძირითადი ფაქტორებისა და რისკ-ჯგუფების გამოვეთა, რომლებიც წარმოადგენენ მიგრაციის წარმომშობ მიზეზებს, როგორებიცაა პოლიტიკური, სოციალურ-ეკონომიკური და ფსიქოლოგიური ფაქტორები.

ნაშრომის მიზანია გამოკვეთოს და განხილულ იქნას შრომითი მიგრაციის წარმომშობი თეორიები, გაანალიზდეს შრომითი მიგრაციის სამართლებრივი რეგულირების ასპექტები და მისი გავლენა როგორც სახლმწიფოს ეროვნულ უსაფრთხოებაზე, ისე ეკონომიკურ უსაფრთხოებაზე.

**საკვანძო სიტყვები: მიგრაციის სამართალი, შრომითი მიგრაცია, ეროვნული უსაფრთხოება, ეკონომიკური უსაფრთხოება**

# შესავალი*

სახელმწიფოს გეოპოლიტიკური მდებარეობის გათვალისწინებით, მიგრაციული პროცესების მართვა, არალეგალურ მიგრაციასთან ბრძოლა, ეკონომიკური უსაფრთხოების უზრუნველყოფა და დადებითი მიგრაციული სალდოს შენარჩუნება არის სახელმწიფოთა ერთ-ერთი მნიშვნელოვანი გამოწვევა.

დღესდღეობით მსოფლიოში მიმდინარე გლობალიზაციის პრცესებთან ერთად ერთ-ერთი აქტუალური საკითხია მოსახლეობის შრომითი მიგრაცია.[1] რთული სოციალურ-ეკონომიკური მდგომარეობა, მოსახლეობის უმრავლესობის დაუსაქმებლობა, სახელმწიფოს ძირითადად არასწორი პოლიტიკა ადამიანური რესურსების მართვის სფეროში ხელს უწყობს შიდა და გარე შრომითი მიგრაციის გაძლიერებას, ინტელექტუალურ მიგრაციას და არალეგალური მიგრაციის სხვადასხვა ფორმის განვითარებას და ისეთი დანაშაულების რიცხვის ზრდას, როგორიცაა ტრეფიკინგი და მიგრანტთა კონტრაბანდა.

ახალგაზრდები ნებისმიერი სახელმწიფოს დემოკრატიული და სოციო-ეკონომიკური განვითარების მთავარ ძალას წარმოადგენენ. სწორედ ახალგაზრდები არიან ცვლილებების მაპროვოცირებელი და სხვადასხვა სფეროებში ინოვატორები, ამიტომ როდესაც ახალგაზრდები სახელმწიფოში ბევრ გამოწვევას აწყდებიან პოლიტიკურ, სოციალურ-ეკონომიკურ თუ კულტურულ ცხოვრებაში ეს განაპირობებს მათ გადინებას უცხო ქვეყნებში უკეთესი ცხოვრებისეული პირობების საძიებლად,[2] რაც ქვეყნის დემოგრაფიულ უსაფრთხოებაზე უარყოფითად მოქმედი პირდაპირი ფაქტორია.[3] დემოგრაფიულ უსაფრთხოებას კი უშუალო კავშირი აქვს ქვეყნის ეკონომიკის სტაბილურ გრძელვადიან ზრდასთან.[4]

აქედან გამომდინარე, დღესდღეობით, საკმაოდ აქტუალური და მნიშვნელოვანია მიგრაციის საკითხების განხილვა სახელმწიფოს ეკონომიკურ უსაფრთხოებასთან კავშირში, მისი წარმომშობი მიზეზების გაანალიზება და შესაბამისი რეკომენდაციების გაცემა, აგრეთვე საერთაშორისო კანონმდებლობის განხილვა და შესაბამისი პოლიტიკის შემუშავების აუცილებლობის განსაზღვრა მიგრაციის მართვის სფეროში.

---

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

[1] Migration and Globalization, Why Does Migration Happen? <http://www.globalization101.org/uploads/File/Migration/migration.pdf > გვ. 9-14; [წვდომის თარიღი: 12.01.2020];

[2] ომანაძე ს., გაჩეჩილაძე ნ., ლებანიძე ა., ჩაჩანიძე ს., 2017. თაობა გარდამავალ პერიოდში ახალგაზრდობის კვლევა 2016 - საქართველო, ფრიდრიხ ებერტის ფონდი სამხრეთ კავკასიის რეგიონალური ოფისი, თბილისი, გვ. 7-11;

[3] საქართველოს პარლამენტის დადგენილება №5586-IIს, „საქართველოს დემოგრაფიული უსაფრთხოების კონცეფციის“ დამტკიცების შესახებ, საკანონმდებლო მაცნე, 24/06/2016;

[4] ბრუნი ბ.დ., ჭითანავა მ., 2017. მოსახლეობის დაბერება და ხანდაზმულები საქართველოში 2014 წლის მოსახლეობის საყოველთაო აღწერის შედეგებზე დაფუძნებული მიმოხილვა, საქართველოს სტატისტიკის ეროვნული სამსახური (საქსტატი), გაერთიანებული ერების ორგანიზაციის მოსახლეობის ფონდი (UNFPA), თბილისი, გვ. 6-7;

# 1. მიგრაციული პროცესების საერთაშორისო სამართლებრივი რეგულირება

მიგრაციული პროცესების სამართლებრივი რეგულირების საკითხების განხილვისას გასათვალისწინებელია როგორც სახელმწიფოს სუვერენიტეტი, ისე ადამიანის უფლებებისა და თავისუფლებების დაცვის სამართლებრივი ინტერესები. გარკვეულ შემთხვევებში, სახელმწიფო უფლებამოსილია შეზღუდოს ადამიანის უფლებები საჯარო ლეგიტიმური მიზნის მისაღწევად, თანაზომიერების პრინციპის დაცვით.

ვინაიდან მიგრაცია წარმოადგენს საერთაშორისო ფენომენს და მიგრაციული პროცესები დაკავშირებულია საზღვრის კვეთისა და გადაადგილების საკითხებთან, ამიტომ იგი მრავალი კონვენციისა, შეთანხმებისა და საერთაშორისო რეგულირების საგანს წარმოადგენს,* რომელიც მიგრაციის საერთაშორისო სამართლის დარგის რეგულირების სფეროს წარმოადგენს.

მიგრაციის საერთაშორისო სამართალი მოიცავს იმ ნორმათა ერთობლიობას, რომელბიც არეგულირებენ ადამიანთა საზღვარგარეთ გადაადგილებისა და მიმღებ სახელმწიფოში მათ სამართლებრივ მდგომარეობას. ეს კი მიგრაციის პროცესის ორ ნაწილს ემიგრაციასა და იმიგრაციას მოიცავს. აქედან გამომდინარე, მიგრაციის საერთაშორისო სამართალი არის მიგრაციის სფეროში სახელმწიფოს სუვერენული უფლებამოსილებიდან და ადამიანის უფლებებიდან გამომდინარე საერთაშორისო ნორმებისა და პრინციპების ერთობლიობა.

მიგრაცია მხოლოდ ქვეყნის ეროვნული კანონმდებლობის დონეზე ვერ მოწესრიგდება, ამიტომ იგი საჭიროებს ეფექტურ საერთაშორისო რეგულირებას. საერთაშორისო ორგანიზაციებიდან შრომით მიგრაციის რეგულირების საკითხებში აღსანიშნავია გაერთიანებული ერების ორგანიზაციის, [5] მიგრაციის საერთაშორისო ორგანიზაციისა[6] და შრომის საერთაშორისო ორგანიზაციის როლი.[7]

საერთაშორისო ხელშეკრულებებით დადგენილი საერთაშორისო სამართლის სახელშეკრულებო ნორმებთან ერთად მნიშვნელოვანია ადამიანის უფლებებთან დაკავშირებით განხილულ იქნას ადამიანის უფლებათა საყოველთაო დეკლარაცია, რომელშიც დადგენეილია მიგრაციასთან დაკავშირებული უფლებებიც. [8] დეკლარაციის თანახმად, ყველა ადამიანი დაბადებულია როგორც თავისუფალი და გააჩნია თანასწორი

---

* ამ მიმართულებით საყურადღებოა გაეროს 1951 წლის კონვენცია „ლტოლვილის სტატუსის შესახებ“, „იძულებით (საკუთარი სახელმწიფოს ტერიტორიის ფარგლებში) გადაადგილების შესახებ გაეროს სახელმძღვანელო პრინციპები“, „ყველა მიგრანტი მუშაკისა და მათი ოჯახის წევრების უფლებების დაცვის 1990 წლის საერთაშორისო კონვენცია“ და სხვ.

[5] The United Nations, <http://www.un.org/en/> [წვდომის თარიღი: 09.01.2010];

[6] The International Organization for Migration, <https://www.iom.int/about-iom,> [წვდომის თარიღი: 09.01.2020];

[7] The International Labour Organization, ერთა ლიგასთან არსებული ავტონომიური ორგანიზაცია, 1919 წელს ვერსალის სამშვიდობო კონფერენციაზე შეიქმნა. 1946 წლიდან კი ფუნქციონირებს როგორც გაეროს სპეციალიზებული დაწესებულება <https://www.ilo.org/dyn/normlex/en/f?p=1000:62:0::NO:62:P62_LIST_ENTRIE_ID:2453907:NO>, [წვდომის თარიღი: 09.01.2020];

[8] The Universal Declaration of Human Rights (UDHR), Adopted by the United Nations General Assembly, Resolution 217, Palais de Chaillot, Paris, France, 10 December, 1948, <https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217(III)> [წვდომის თარიღი: 06.01.2020];

ღირსება და უფლებები. ამავე დეკლარაციის მეორე მუხლის თანახმად ადამიანის უფლებების დაცვა და თავისუფლება ყველა პირისთვის ერთანირია მიუხედავად პირის ქვეყნის სტატუსისა.

მიგრაციის საკითხების რეგულირების კუთხით მნიშვნელოვანია დეკლარაციის მე-13, მე-14 და მე-15 მუხლები. მე-13 მუხლის თანახმად ყველა ადამიანს აქვს უფლება აირჩიოს საცხოვრებელი ადგილი, დატოვოს ან დაბრუნდეს ქვეყანაში.[9] მე-14 მუხლის მიხედვით ყველა ადამიანს აქვს უფლება მოიძიოს თავშესაფარი.[10] მე-15 მუხლის თანახმად, თითოეულ პირს აქვს უფლება ჰქონდეს მოქალაქეობა.[11]

როგორც აღინიშნა, მიგრაციული პროცესების საერთაშორისო რეგულირება არ გულისხმობს მხოლოდ მისი ნაკადის რეგულირებას, არამედ იგი აგრეთვე მოიაზრებს ადამიანის ფუნდამენტური უფლებებისა და თავისუფლებების დაცვასაც, მათ შორის შრომითი მიგრანტების უფლებების დაცვას, რადგან შრომის პირობების უზრუნველყოფა და საერთაშორისოდ აღიარებული შრომის უფლებების დაცვა სამართლებრივი სახელმწიფოს ერთ-ერთი უმთავრესი ვალდებულებაა. ამ მიზნით შრომის საერთაშორისო ორგანიზაციის მიერ მიღებულ იქნა რვა ფუნდამენტური კონვენცია, რომლებიც გაერთიანების თავისუფლებას და კოლექტიურ მოლაპარაკებას, დისკრიმინაციის აკრძალვას, იძულებითი შრომის აკრძალვას, ბავშვთა შრომის აკრძალვას და ადამიანის უფლებათა და თავისუფლებათა დაცვის სხვა მნიშვნელოვან საკითხებს ეხება.[12]

## 2. მიგრაციის კლასიფიკაცია და სახეები

საერთაშორისო მიგრანტების რაოდენობა მსოფლიოში ბოლო წლებში საგრძნობლად იზრდებოდა, 2017 წელს მიგრანტთა რაოდენობამ 258 მილიონს მიაღწია, 2010 წელს იგი 220 მილიონს, ხოლო 2000 წელს კი 173 მილიონს შეადგენდა. მიგრანტთა 60%-ზე მეტი ცხოვრობს აზიაში (80 მილიონი) ან ევროპაში (78 მილიონი). ამერიკის შეერთებულ შტატებში 58 მილიონი, აფრიკაში 25 მილიონი, ხოლო ლათინური ამერიკისა და კარიბის ქვეყნებში მათი რიცხვი 10 მილიონია.[13]

საერთაშორისო მიგრაციის კლასიფიკაციის საკითხთან დაკავშირებით არსებობს სხვადასხვა მოსაზრება, გამოყოფენ შემდეგ სახეებსა და ფორმებს: მუდმივი, ხანგრძლივვადიანი, დროებითი, ტრანზიტული, იძულებითი, ნებაყოფლობითი, ლეგალური, არალეგალური, უკანონო, შრომითი, სეზონური, ქანქარისებური, საზღვრისპირა,

[9] იქვე, Article 13;

[10] იქვე, Article 14;

[11] იქვე, Article 15;

[12] The International Labour Organization's Fundamental Conventions, (Freedom of Association and Protection of the Right to Organise Convention, 1948 (No. 87), Right to Organise and Collective Bargaining Convention, 1949 (No. 98), Forced Labour Convention, 1930 (No. 29), Abolition of Forced Labour Convention, 1957 (No. 105), Minimum Age Convention, 1973 (No. 138), Worst Forms of Child Labour Convention, 1999 (No. 182), Equal Remuneration Convention, 1951 (No. 100), Discrimination (Employment and Occupation) Convention, 1958 (No. 111);

[13] Department of Economic and Social Affairs, United Nations, International Migration Report, New York, 2017, 4-8;

კომერციული, ეპიზოდური, სასწავლო, რეკრეაციული, სამკურნალო, სამივლინებო მიგრაციები.[14]

საერთაშორისო შრომით მიგრაციას შეიძლება ჰქონდეს უმეტესი ზემოთ ჩამოთვლილი მიგრაციის დამახასიათებელი ელემენტი. [15] ის შეიძლება იყოს ხანგრძლივვადიანი, დროებითი, ნებაყოფლობითი, ლეგალური, არალეგალური, უკანონო, სეზონური, ქანქარისებური, საზღვრისპირა, კომერციული, ეპიზოდური, სასწავლოგანხორციელების ფორმის მიხედვით გამოყოფენ ნებაყოფლობით და იძულებით მიგრაციებს, ხოლო დროითი განზომილებით - მუდმივსა და დროებითს. [16] დოქტორი რ.ჯენისენი გამოყოფს მიგრაციის ოთხ ტიპს, ესენია: 1) შრომითი მიგრაცია, 2) დაბრუნებითი მიგრაცია (რეპატრიაცია), 3) ჯაჭვური მიგრაცია, 4) თავშესაფრის მაძიებელთა მიგრაცია (დევნილთა მიგრაცია)[17], აგრეთვე ს.ბელი, ს.ალვესი და სხვები თავიანთ ნაშრომში გამოყოფენ საერთაშორისო მიგრაციის ოთხ ტიპს. [18] რაც შეეხება მიგრანტის ტერმინის განმარტებას, მიგრაციის ევროპული ქსელის განმარტების თანახმად, მიგრანტი არის პირი, რომელიც ერთ წელზე მეტია იმყოფება უცხო ქვეყანაში მიუხედავად მისი იქ ყოფნის მიზეზისა.[19]

## 2.1 შრომითი მიგრაცია

მიგრაციის საერთაშორისო ორგანიზაციის თანახმად, ერთამნეთისაგან განასხვავაბენ შრომით და ეკონომიკურ მიგრაციას, რომლის თანახმად, შრომითი მიგრანტი არის ადამიანი, რომელიც გადადის ერთი ქვეყნიდან მეორეში დასაქმების მიზნით, [20] ეკონომიკური მიგრანტები კი არიან პირები, რომლებიც შედიან ქვეყანაში ეკონომიკური აქტივობების განხორციელების მიზნით, მათ შორის ბიზნეს მოგზაურები, ინვესტორები და ყველა პირი რომელიც დაინტერესებულია მიმღებ ქვეყანაში ეკონომიკური საქმიანობის განხორციელებით.[21]

გაერთიანებული ერების ორგანიზაციის „შრომითი მიგრანტებისა და მათი ოჯახის წევრების უფლებების დაცვის შესახებ“ საერთაშორისო კონვენციის მიხედვით შრომითი

---

[14] ჭელიძე ნ., 2006., შრომითი ემიგრაცია პოსტსაბჭოთა საქართველოში, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი მიგრაციის კვლევის ცენტრი, თბილისი, გვ. 5-7;

[15] ბადურაშვილი ი., 2017. მიგრაციის სახელმძღვანელო, მიგრაციის ფორმები, მიგრაციის პოლიტიკის განვითარების საერთაშორისო ცენტრი, თბილისი, გვ. 34-48;

[16] მიგრაციის საერთაშორისო ორგანიზაცია (IOM), 2004., მიგრაციის საკითხთა სამთავრობო კომისია, მიგრაციის ტერმინთა განმარტებითი ლექსიკონი, ჟენევა;

[17] Jennissen, R. P. W. 2004. Macro-economic determinants of international migration in Europe, Amsterdam, Rozenberg Publishers, P. 93-106;

[18] Bell, S., Alves, S., de Oliveira, E. S., & Zuin, A., 2010. Migration and Land Use Change in Europe: A Review, , Leibniz Centre for Agricultural Landscape Research (ZALF), Eberswalder Straße 84, 15374 M¨uncheberg, Germany. ISSN 1863-7329, P. 16-18;

[19] The European Migration Network, Asylum and Migration Glossary 3.0, 2014. a tool for better comparability produced by the European Migration Network, October, P. 187;

[20] Usher E, 2004. Migration and labour. In: Usher E, editor. Essentials of migration management: a guide for policy makers and practitioners. Geneva: United Nations Publications;

[21] Simon J, Kiss N, Łaszewska A., 2015. Public Health Aspects of Migrant Health: A Review of the Evidence on Health Status for Labour Migrants in the European Region. Health Evidence Network Synthesis Report, No. 43. et al. Copenhagen: WHO Regional Office for Europe, P. 39;

მიგრანტი არის პირი, რომელიც იმუშავებს, მუშაობს ან აქვს ანაზღაურებადი სამუშაო იმ ქვეყანაში რომლის მოქალაქეც იგი არ არის.[22]

როგორც აღინიშნა შრომითი მიგრაცის მაინსპირირებელი შეიძლება იყოს სხვადასხვა ფაქტორი, მათ შორის კი აღსანიშნავია სოციალურ-ეკონომიკური, პოლიტიკური და ფსიქოლოგიური ფაქტორები. გლობალიზაციის პირობებში მკვეთრად გაიზარდა მიგრაციული ნაკადები განვითარებადი ქვეყნებიდან განვითარებული ქვეყნებისაკენ. მიგრაციული პროცესი ძირითადად ეკონომიკური (შრომითი) ხასიათისაა, რაც განპირობებულია ორი ძირითადი მიზეზით: მიმღებ ქვეყნებში მუშახელზე არსებული მოთხოვნით და მშობლიურ ქვეყანაში სოციალურ-ეკონომიკური პრობლემებით, რომელსაც თან სდევს უმუშევრობა. აქედან გამომდინარე, მუშახელი, რომელიც დაუსაქმებელია, ან რომელსაც დაბალი ანაზღაურება აქვს, ცდილობს წავიდს იმ ქვეყნებში, სადაც მასზე არის მოთხოვნა და სადაც უკეთესი ანაზღაურების მიღების პერსპექტივაა.[23]

უკანასკნელი ათწლეულის განმავლობაში მიგრაციის საკითხებთან დაკავშირებული პრობლემები აქტუალური ხდება მთელი მსოფლიოსათვის, განსაკუთრებით კი პოსტკომუნისტური ქვეყნებისათვის, [24] მათ შორის საქართველოსთვის. საქართველოში მიგრაციასთან დაკავშირებული ნებისმიერი საკითხი თუ პრობლემა მნიშვნელოვანია ქვეყანაში არსებული დემოგრაფიული პროცესებისა და უმძიმესი სოციალურ-ეკონომიკური ვითარების გამო, ამიტომ საქართველოს მთავრობის დადგენილების საფუძველზე შეიქმნა მიგრაციის საკითხთა სამთავრობო კომისია. იგი არის მთავრობის სათათბირო ორგანო, რომელიც მსჯელობს და გადაწყვეტილებებს იღებს მიგრაციის მართვასთან დაკავშირებულ სხვადასხვა აქტუალურ საკითხზე.[*] კომისიას, რომელიც აერთიანებს 9 სახელმწიფო უწყებას, თავმჯდომარეობს იუსტიციის მინისტრი, ხოლო თანათავმჯდომარეა შინაგან საქმეთა მინისტრის მოადგილე.[25]

საქსტატის ბოლო სამი წლის მონაცემების თანახმად, (2014-2016 წწ.), იზრდება ემიგრანტთა ნაკადი საქართველოდან. 2014 წელს მათი რაოდენობა 88,704 შეადგენდა, რომელთა შორის 69,855 საქართველოს მოქალაქე იყო. 2015 წელს კი, უკვე 95,965 ემიგრანტი წავიდა საქართველოდან, რომელთა უმრავლესობა (67,452) საქართველოს მოქალაქე იყო, ხოლო 2016 წელს ემიგრანტთა რიცხვი გაიზარდა და 98,288-ს მიაღწია.[26]

---

[22] International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 2, Adopted by General Assembly resolution 45/158 of 18 December 1990;

[23] ქაჯაია მ., 2005, ახალგაზრდობის გარე მიგრაციული განწყობის ზოგიერთი საკითხის შესახებ, მიგრაციული პროცესები თანამედროვე გლობალიზებად მსოფლიოში, მიგრაციის კვლევის ცენტრი, თბილისი, გვ. 47;

[24] International Organization for Migration, World Migration Report 2018, The UN Migration Agency, Part I: Data and information on migration, 10-13;

[*] მიგრაციის საკითხთა სამთავრობო კომისიის წევრი უწყებებია: განათლების, მეცნიერების, კულტურისა და სპორტის სამინისტრო, საგარეო საქმეთა სამინისტრო, სახელმწიფო უსაფრთხოების სამსახური, სტატისტიკის ეროვნული სამსახური, ეკონომიკისა და მდგრადი განვითარების სამინისტრო, ფინანსთა სამინისტრო, იუსტიციის სამინისტრო, შინაგან საქმეთა სამინისტრო, ოკუპირებული ტერიტორიებიდან დევნილთა,შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო;

[25] საქართველოს მთავრობის დადგენილება #314, „მიგრაციის საკითხთა სამთავრობო კომისიის შექმნისა და დებულების დამტკიცების შესახებ“, საკანონმდებლო მაცნე, 13/10/2010;

[26] საქართველოს სტატისტიკის ეროვნული სამსახური, ცხრილი #2, <http://www.geostat.ge/?action=page&p_id=172&lang=geo> [წვდომა: 06.01.2020];

დღევანდელი მიგრაციული განწყობის მიზეზებიდან და ძირითადი მოტივებიდან შეიძლება გამოიყოს სამი ძირითადი ჯგუფი პოლიტიკური, სოციალურ-ეკონომიკური და ფსიქოლოგიური ფაქტორები[27], კერძოდ: 1) მძიმე სოციალურ-ეკონომიკური პირობების გამო საზღვარგარეთ მუშაობის სურვილი, 2) სწავლის სურვილი, 3) ქვეყანაში არსებული განუკითხაობა, კრიმინალური სიტუაცია და მდგომარეობის გამოსწორების რწმენისა და იმედის დაკარგვა.[28] ყოველივე ზემოთაღნიშნული კი ხელს უწყობს საკმაოდ მასშტაბურ გარე შრომით მიგრაციულ პროცესებს, განსაკუთრებით კი ახალგაზრდებში.

## 3. მიგრაციული პროცესების გავლენა სახელმწიფოს ეკონომიკურ უსაფრთხოებაზე

შრომითი მიგრაცია თავისი არსითა და მნიშვნელობით, ერთ-ერთი სერიოზული და საინტერესო დემოგრაფიული პროცესია, რომელსაც აქვს თავისი დადებითი და უარყოფითი მხარეები. ერთის მხრივ მიგრაცია მიმღებ ქვეყანაში ხელს უწყობს კონკურენტუნარიანობის ამაღლებას, კვალიფიციური მუშახელის დეფიციტის შევსებას და აძლიერებს სასიცოცხლოდ მნიშვნელოვან სექტორებს მიმღებ ქვეყანაში, მეორე მხრივ კი მან მნიშვნელოვანი და მრავალმხრივი უარყოფითი შედეგი შეიძლება გამოიწვიოს, ერთის მხრივ კრიმინოგენური მდგომარეობის გაუარესება, ხოლო მეორეს მხრივ, წარმომშობი ქვეყნის ეკონომიკური უსაფრთხოებისათვის გახდეს უარყოფითი შედეგის მომტანი, რადგან ძირითადად მიგრაცილ ნაკადში ხვდებიან ახალგაზრდა, შრომისუნარიანი და მაღალკვალიფიციური ადამიანები, რომლებსაც სურთ უკეთესი საცხოვრებელი და სამუშაო პირობები და რომელიც საკუთარ სახელმწიფოში არ გააჩნიათ. არსებობს კიდევ ერთი მნიშვნელოვანი საფრთხე ეკონომიკური უსაფრთხოებისთვის, რომელიც შეიძლება დავუკავშიროთ როგორც შიდა, ასევე გარე ფაქტორებს, ესაა - ,,ტვინების გადინება".

ნებისმიერი ქვეყნისთვის წინსვლისა და განვითარების განმსაზღვრელი მაღალკვალიფიციური მოსახლეობაა, თუმცა როდესაც სახელმწიფოში არახელსაყრელი სოციალურ-ეკონომიკური თუ პოლიტიკური ვითარებაა, საქმე გვაქვს ე.წ ,,ტვინების გადინებასთან". როგორც აღინიშნა, აღნიშნულის ერთ-ერთ მამოძრავებელ ძალად აგრეთვე მიჩნეულია უფრო მაღალი ანაზღაურების მიღების სურვილი სხვა ქვეყანაში.[29] როდესაც ხდება განვითარებადი ქვეყნების მაღალკვალიფიციური კადრების გადინება, როგორც წესი, განვითარებულ ქვეყნებში, სუსტდება განვითარებადი ქვეყნების ეკონომიკური პოტენციალი. ,,ტვინების გადინების" პროცესი გრძევადიანი უარყოფითი შედეგის განმაპირობებელია სახელმწიფოს ეკონომიკური უსაფრთხოებისათვის, რადგან ხდება იმ კადრების გადინება რომლებისთვისაც სახელმწიფომ გარვეული კაპიტალი ჩადო განათლებაში და უცხო ქვეყანაში გასული ინტელექტუალი მოსახლეობის კვლავ დაბრუნების შანსი თავის სამშობლოში ბევრად ნაკლებია.

---

[27] ქაჯაია მ., 2005, ახალგაზრდობის გარე მიგრაციული განწყობის ზოგიერთი საკითხის შესახებ, მიგრაციული პროცესები თანამედროვე გლობალიზებად მსოფლიოში, მიგრაციის კვლევის ცენტრი, თბილისი, გვ. 48-49;

[28] საქართველოს სტატისტიკის ეროვნული სამსახური, ცხრილი #3, #4, <http://www.geostat.ge/?action=page&p_id=172&lang=geo> [წვდომა: 08.01.2020];

[29] Docquier F., Rapoport H., 2007. Skilled Migration: The Perspective of Developing Countries, IZA DP No. 2873, Forschungsinstitut zur Zukunft der Arbeit Institute for the Study of Labor, Bonn, June, P. 4-7;

სახელმწიფოს ეკონომიკური უსაფრთხოების უზრუნველსაყოფად აუცილებელია შემუშავებულ იქნეს ეკონომიკური განვითარების ეროვნული სტრატეგია, რომელიც მიზნად უნდა ისახავდეს ეკონომიკის სხვადასხვა სექტორების ფუნქციონირების და ქვეყნის სოციალური და ეკონომიკური პოლიტიკის ჰარმონიზებას, რათა მოხდეს სოციალურად პასუხისმგებელი ეკონომიკის განვითარება, მომავალი თაობებისთვის რესურსული ბაზის შენარჩუნების პირობებში.[30]

ქვეყნის ეკონომიკური განვითარების არასტაბილური ხასიათი მეტად ართულებს განათლების სფეროში პროგნოზირებისა და დაგეგმვის მექანიზმების გამოყენებას. როგორც პროფესორი, კ.კუტუბიძე აღნიშნავს „ეს ნოყიერ ნიადაგს ქმნის ინტელექტუალური შრომითი რესურსების ემიგრაციისთვის. მიგრაციის პროცესი უარყოფით ზეგავლენას ახდენს ქვეყნის განვითარებაზე, განსაკუთრებით მაშინ, როცა ემიგრანტები ხდებიან ყველაზე ნიჭიერი ადამიანები, პროფესიონალები. ე.წ. „ინტელექტის გადინება“ ჩვეულებრივ გამოიხატება იმაში, რომ ქვეყანას განსაკუთრებული ნიჭის მქონე მოქალაქეები ტოვებენ (მუსიკოსები, მხატვრები, ექიმები, ინჟინრები, მეცნიერები და სხვ.)“.[31]

ინტელექტუალური მიგრცია სახელმწიფოს ერთ-ერთ ყველაზე დიდ სოციალურ პრობლემას წარმოადგენს. აუცილებელია სახელმწიფოს ინტერესებიდან გამომდინარე ქმედითი ღონისძიებების გატარება, მიგრაციის სახელმწიფო პროგრამის შემუშავება, კომპლექსური მიდგომა და მჭიდრო თანამშრომლობა მიმღები ქვეყნის თითქმის ყველა შესაბამის სტრუქტურასთან შრომითი მიგრაციის რეგულირების ერთიანი სისტემის შექმნის მიზნით. აგრეთვე, მნიშვნელოვანია შრომითი მიგრაციის წარმომშობი ეკონომიკური ფაქტორებსა და თეორიების ანალიზი.

## 3.1 ეკომომიკური უსაფრთხოება როგორც ეროვნული უსაფრთხოების სეგმენტი

ეკონომიკის უსაფრთხო განვითარება სახელმწიფოს ეროვნული უსაფრთხოების უზრუნველყოფის ერთ-ერთი მნიშვნელოვანი წინაპირობაა. აღნიშნულიდან გამომდინარე, მეტად აქტუალური ხდება სახელმწიფოს ეკონომიკური უსაფრთხოების უზრუნველყოფის ფაქტორების გამოკვლევა, რომელშიც უდიდესი როლი უკავია მიგრაციული პროცესების რეგულირებას, მართვასა და დადებითი მიგრაციული სალდოს შენარჩუნებას.

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

[30] ჭელიძე ნ., 2005. საქართველოს მოსახლეობის შრომითი ემიგრაციის ფაქტორები და სოციალურ-ეკონომიკური შედეგები, მიგრაციის კვლევის ცენტრი, სტუდენტთა და ასპირანტთა სამეცნიერო საზოგადოება, მიგრაციული პროცესები პოსტსაბჭოთა საქართველოში, თბილისი, გვ. 55-64;

[31] კუტუბიძე კ., 2008. ინტელექტუალური რესურსები და ქართული რეალობა, ჟურნ. „ბიზნესი და კანონმდებლობა“, №17 გამოცემა, თბილისი;

ეკონომიკური უსაფრთხოების, შესახებ მეცნიერთა შეხედულებები შიძლება დაიყოს შემდეგნაირად: [32] **პირველი ჯგუფი** მიიჩნევს, რომ ეკონომიკური უსაფრთხოება არის ეკონომიკის და სახელმწიფო ინსტიტუტების მდგომარეობა, რომლის მიზანი და ამოცანებია ეკონომიკური უსაფრთხოების უზრუნველყოფა და ეროვნული ინტერესების გარანტირებული დაცვა, სახელმწიფოს სოციალური პოლიტიკის, საკმარისი თავდაცვითი პოტენციალის, საბანკო და საგარეო პროცესებისთვის დამაზიანებელი ქმედებებისა და პირობების აღმოფხვრა.

ი.ბოგდანოვი მიიჩნევს, რომ „ეკონომიკური უსაფრთხოება ეს არის ქვეყნის ეკონომიკის მდგომარეობა, რომელიც ჯერ ერთი, მოცულობითი და სტრუქტურული პარამეტრებით საკმარისია სახელმწიფოს არსებული სტატუსის, მისი საგარეო ზეწოლისაგან დამოუკიდებელი პოლიტიკური და სოციალურ-ეკონომიკური განვითარების უზრუნველსაყოფად და მეორე, რომელსაც უნარი აქვს დაიცვას ლეგალური შემოსავლების დონე მოსახლეობის აბსოლიტური უმრავლესობის ცივილიზებული ქვეყნების სტანდარტების შესაბამისი კეთილდღეობის უზრუნველსაყოფად“.[33]

რ.ოთინაშვილი-„სახელმწიფოს ეკონომიკური უსაფრთხოება ნიშნავს, ეკონომიკური განვითარების ისეთ დონეს, რომელიც ეროვნულ-სახელმწიფოებრივი ინტერესების (მოთხოვნილების) რეალიზაციას, პიროვნებისა და საზოგადოების არსებობისათვის ღირსეული ცხოვრების პირობებს უზრუნველყოფს და ქვეყნის პროგრესის შემაფერხებელი გარე და შიდა საფრთხეებს აღუდგება წინ“.[34]

მეცნიერთა **მეორე ჯგუფის** მოსაზრების მიხედვით კი ეკონომიკური უსაფრთხოება არის ,,ფაქტორების და პირობების ერთობლიობა, შეხამება, რომელიც უზრუნველყოფს ქვეყნის ეკონომიკური განვითარების აუცილებელ დონეს.

ლ.აბალკინი-ეკონომიკური უსაფრთხოება არის „როგორც იმ პირობებისა და ფაქტორების ერთობლიობა, რომლებიც უზრუნველყოფენ ეროვნული ეკონომიკის დამოუკიდებლობას, მის სტაბილურობას და მდგრადობას, მუდმივი განახლებისა და თვითსრულყოფის უნარს“.[35]

ე.ილარიონოვი-„ეკონომიკური უსაფრთხოების ქვეშ იგულისხმება ეკონომიკური, პოლიტიკური და სამართლებრივი პირობების ისეთი შეხამება, რომელიც უზრუნველყოფს ხანგრძლივვადიან პერსპექტივაში მოსახლეობის ერთ სულზე ეკომიკური რესურსების მაქსიმალური რაოდენობის წარმოებას ყველაზე ეფექტური ხერხებით“.[36]

ი.მესხია-„ეკონომიკური უსაფრთხოება იმ საშინაო და საგარეო პირობების ერთობლიობაა, რომელიც ქვეყნის ეკონომიკის დინამიური განვითარების საფუძველს ქმნის;მისი უნარია უზრუნველყოს ინვალიდის, სახელმწიფოს და საზოგადოების მოთხოვნილება, დააკმაყოფილოს კონკურენტუნარიანობა საგარეო ბაზარზე და შექმნას

[32] თეთრუაშვილი ზ., თეთრუაშვილი-ქარდავა მ., 2006. საქართველოს ეკონომიკური უსაფრთხოების უზრუნველყოფის ფინანსურ-ეკონომიკური ფაქტორები და მისი რეგულირების მექანიზმები საბაზრო ურთიერთობის ფორმირების პირობებში;

[33] Богданов И. П., Испиран М., 2001. Экономическая безопасность России, Ж. „Теория и практика“ Р. 28;

[34] ოთინაშვილი რ., 2002. ეკონომიკური უსაფრთხოების სახელმწიფო სტრატეგია. იხ. საქართველოს სტრატეგიული კვლევისა და განვითარების ცენტრი, ბიულეტენი № 73. აგვისტო, გვ. 3;

[35] Абалкин Л. 1994. Экономическая безопасность России утроз Ж. „Вопросы економики“ №Т12, Р. 5;

[36] Иларионов А., 1998. Критерии экономической безопасности, Ж. „Вопроси економики“ № 10, Р. 49;

სხვადასხვა სახის საშიშროებისა და მატერიალური დანაკარგების თავიდან აცილების გარანტია.[37]

**მესამე ჯგუფი** კი მიიჩნევს, რომ „ეკონომიკური უსაფრთხოება არის საშინაო ეკონომიკური სისტემის მატერიალობა.“

ს.აფონცევი - „ეროვნული ეკონომიკური უსაფრთხოება განიხილება, როგორც ეროვნული ეკონომიკური სისტემის მატერიალობა ეკონომიკური ან პოლიტიკური წარმოშობის ენდოგენური და ეგზოგენური შოკების მიმართ, რომელიც გამოვლინდება მის უნარში გაანეიტრალოს ნეგატიური შოკების პოტენციალური წყაროები და მინიმუმამდე დაიყვანოს ზიანი, რომელიც დაკავშირებულია რეალურად წარმოშობილ შოკებთან“.[38]

ა.სილაგაძე და თ. ჩიკვაიძე- „ეკონომიკური უსაფრთხოება არის იმ პირობებისა და ფაქტორების ერთობლიობა, რომელიც უზრუნველყოფს ეროვნული ეკონომიკის დამოუკიდებლობასა და მატერიალობას, სახელმწიფოებრივი მთლიანობისა და მოსახლეობის კეთილდღეობის ამაღლების მიზნით მისი მუდმივი მონაცემების სრულყოფასა და განვითარების უნარს“. მეოთხე, „ეკონომიკური უსაფრთხოება გულისხმობს ეროვნული ეკონომიკის დაცვას“.[39]

ს.გალკინა, გ. კლეინერი და ი.პეტრენკო მიიჩნევენ, რომ „ქვეყის ეკონომიკური უსაფრთხოების ქვეშ უნდა გავიგოთ ამ უკანასკნელის დაცულობის ხარისხი იმ ფასეულობების (საფრთხეების, ძალების) წარმოშობის დასაწყისი მოქმედებისგან, რომელთაც შეუძლიათ არსებითი ზიანი მიაყენონ ქვეყნის მთლიანობას, სუვერენიტეტს და დამოუკიდებლობას, ეროვნული მიზნების შესაბამისად შეარყიონ თავისუფალი განვითარება, ან სერიოზულად გააუარესონ მისი მდგომარეობა მსოფლიო გაერთიანებაში“.[40]

თ.მაღლაკელიძე-„ეკონომიკური უსაფრთხოება გულისხმობს ეროვნული ეკონომიკის დაცვას იმ შიდა და გარე ნეგატიური ფაქტორებისაგან, რომლებიც არღვევენ აღწარმოებითი პროცესების ნორმალურ ფუნქციონირებას, საფრთხეს უქმნის მის რესურსული და მეცნიერულ-ტექნოლოგიური პოტენციალის შენარჩუნებას, ეკონომიკის მდგრად განვითარებას და სოციალურად ორიენტირებულობას, აფერხებს ეკონომიკურ ზრდასა და ხელს უშლის სახელმწიფოებრიობის განმტკიცებას“.[41]

აქედან გამომდინარე, როგორც სხვადასხვა მეცნიერთა შეხედულებებიდან ჩანს, სახელმწიფოთა შენარჩუნება-განვითარების მნიშვნელოვანი წინაპირობა ქვეყანაში დადებითი ეკონომიკური მაჩვენებლების უზრუნველყოფაა. ამ მიმართებით ერთ-ერთ მნიშვნელოვან საკითხს წარმოადგენს სახელმწიფოში ზომიერი საგადასახადო სისტემის ჩამოყალიბება, დემოგრაფიული უსაფრთხოების, მიგრაციული პროცესების სათანადოდ მართვის უზრუნველყოფა და სახელმწიფოში შესაბამისი ეკონომიკური უსაფრთხოების პოლიტიკის განსაზღვრის აუცილებლობა, რაც თავისთავად გამორიცხავს სახელმწიფოში სოციალურ-ეკონომიკურ და პოლიტიკურ პრობლემებს, რითაც თავიდან იქნება აცილებული

---

[37] მესხია ი., 1966. საქარათველოს ეკონომიკური უსაფრთხოების კონცეპტუალური საკითხები. ჟურნ. „ეკონომიკა“ №1-3, გვ. 4;

[38] Афонцев С., 2001. Дискуссионные проблемыконцепции националной економической безапасности Россия XXI (Москва), P. 66;

[39] ბასილია თ., სილაგაძე ა., ჩიკვაიძე თ., 2001. პოსტსოციალისტური ტრანსფორმაცია: საქართველოს ეკონომიკა XXI საუკუნის მიჯნაზე, თბილისი, გვ. 462- 463;

[40] Галкина С., Клейнер Г., 2003. Высветление экономики и укрепление националной безопасности, Россыйскыи экономический журнал §5-6, P. 3;

[41] მაღლაკელიძე თ., 2002. ეკონომიკური უსაფრთხოება, თბილისი, გვ. 22;

სახელმწიფოსათვის დამაზიანებელი უამრავი ქმედება, მათ შორის უკონტროლო მიგრაციული პროცესები.

# 4. შრომითი მიგრაციის წარმოშობის ეკონომიკური თეორიები

## 4.1 ნეო-კლასიკური ეკონომიკური თეორია

ნეოკლასიკური ეკონომიკური თეორიის [42] თანახმად, საერთაშორისო შრომითი მიგრაციას წარმოშობს ქვეყნებს შორის ეკონომიკური განვითარების დონეების სხვაობით, კერძოდ, შრომის ანაზღაურებაში განსხვავებით. ბუნებრივია, სამუშაო ძალა მიემართება იქ, სადაც შრომის მაღალი ანაზღაურებაა. ამითაც ვლინდება საერთაშორისო შრომის ბაზრის თვითრეგულირებადი ხასიათი. ეკონომიკის აღმავლობისა და ემიგრაციის გაძლიერების კვალდაკვალ ხელფასის დონეებს შორის განსხვავებაც მცირდება და საემიგრაციო სტიმულიც იკლებს.[43] მუშახელის ექსპორტიორი ქვეყანა შეიძლება იმპორტიორადაც გადაიქცეს.*

## 4.2 ადამიანური კაპიტალის თეორია

ადამიანური კაპიტალის თეორიის თანახმად, [44] თითოეული მიგრანტი მოიაზრება როგორც მის განათლებაში, კვალიფიკაციასა და სამედიცინო მომსახურებაში ინვესტირების შედეგი. მიგრირების პროცესში ადამიანური კაპიტალის თეორია გარდა ეკონომიკურისა, მხედველობაში იღებს, ასევე ფსიქოლოგიურ დანაკარგებს, როგორიცაა: განშორება ახლობლებთან, არამატერიალური ფაქტორები – კლიმატი, უფრო მაღალი დონის კულტურასთან და სხვა საზოგადოებრივ სიკეთესთან ხელმისაწვდომობა და სხვა.

აღნიშნული თეორიის მიმდევარი ბარი ჩაისვიკი აღნიშნულ თეორიას შრომით მიგრანტთა სელექციურ მოდელად მიიჩნევს, რომელიც როგორც დონორ, ისე მიმღებ ქვეყნებში ახდენს ხელსაყრელ სელექციას შრომითი მიგრანტების მოთხოვნა-მიწოდების თვალსაზრისით.*

## 4.3 შრომითი მიგრაციის ახალი ეკონომიკური თეორია

მოცემული თეორია ეყრდნობა მიკროეკონომიკურ ფუნქციონალურ ანალიზს. მიგრაციაზე გადაწყვეტილება მიიღება არა ცალკეული ინდივიდების, არამედ

---

[42] Jennissen, R. P. W. 2004. Macro-economic determinants of international migration in Europe, Amsterdam, Rozenberg Publishers, P. 44-46;

[43] Öberg, S., 1997. Theories on inter-regional migration: an Overview. In: Blotevogel, H.H. and Fielding A.J. (eds.), People, jobs and mobility in the new Europe, Chichester: Wiley, P. 3-22

* ნეოკლასიკური ეკონომიკის თეორია გულისხმობს, რომ მიმღები და დონორი ქვეყნების შრომითი რესურსები აბსოლუტურად იდენტურია და ორივე ქვეყანაში მიგრაციის პროცესში ნარჩუნდება სრული დასაქმება, რაც უმეტეს შემთხვევაში, რეალობას არ შეესაბამება.

[44] Chiswick B.R., 2000, Are Immigrants Favorably Self-Selected? An Economic Analysis. Chapters 3. Migration Theory. Talking Across Disciplines. Edited by : Hollifield J.F., Brettel C.B., P. 61-76;

* სელექციური მიდგომა კიდევ უფრო წარმატებულია, თუ მიმღებ და გამგზავნ ქვეყნებში ხელფასებს შორის ფარდობითი სხვაობა მეტია მაღალკვალიფიციური მუშაკების სასარგებლოდ.

კოლექტიურად, ოჯახის წევრების მიერ.[45] მიგრაციის მიზანია არა მარტო მოსალოდნელი შემოსავლის მაქსიმიზაცია, არამედ საკუთარ ქვეყანაში შრომის ბაზრის, დაზღვევისა და სხვა ცხოვრებისეული პირობების განვითარებასთან დაკავშირებული რისკების შემცირება.[46]

თეორიის მიმდევრები ხსნიან მიგრაციის პროცესს მაკროდენეზე და ხაზს უსვამენ საერთაშორისო შრომითი მიგრაციის შედეგად ქვეყნებს შორის პოლიტიკურ-ეკონომიკური კავშირების გაღრმავებას.*

## 4.4 მსოფლიო სისტემების თეორია

აღნიშნული თეორიის თანახმად, შრომითი მიგრაცია განპირობებულია სხვადასხვა ფაქტორით, მისი ახსნისთვის აუცილებელია სისტემა განვიხილოთ მთლიანობაში. ეს თეორია გეოგრაფიული სიახლოვის ფაქტორს არ განსაზღვრავს როგორც აუცილებელ პირობას. [47] ტერიტორიულად დაშორებული ქვეყნები შეიძლება წარმოადგენდნენ გლობალური მიგრაციული სისტემის მნიშვნელოვან ნაწილს.[48]

## 4.5 მიგრაციის წარმომშობი Push and pull თეორია

აღნიშნული თეორია მკაფიოდ გამოხატავს დონორი ქვეყნიდან ემიგრირებაზე გადაწყვეტილების მიღებაში „განმზიდავი“ ფაქტორების როლს, მიმღებ ქვეყანაში კი შესაბამისად-„მიმზიდველი“ ფაქტორების როლს. [49] ემიგრირების პროცესი განისაზღვრება პოტენციური მიგრანტების მიერ ამ ფაქტორების სუბიექტური აღქმით ემიგრაციული ქვეყნების ხელფასებს შორის განსხვავება არ წარმოადგენს გადაადგილების მოტივაციის ერთადერთ და არც ყველაზე მნიშვნელოვან ფაქტორს.[50]

დუგლას მასეის მოსაზრების თანახმად, [51] საერთაშორისო შრომით მიგრაციას განაპირობებს არა ცალკეული ფაქტორები, არამედ ზემოთ ჩამოთვლილი ყველა თეორია ერთად.*

---

[45] Massey D., Joaquin A., Koucouci Ali, Pellegrino A., Taylor E.J., 1998. Worlds in Motion: Understanding International Migration at the End of the Millenium. Oxford: Oxford University Press.;

[46] Taylor, J.E., 1999. The new economics of labour migration and the role of remittances in the migration process. In: International Migration,37(1), P. 63-88;

* წარმომშობ ქვეყანაში ეკონომიკის აღმავლობას აქვს მასტიმულირებელი როლი, რადგან იგი თავის თავში მოიცავს ადგილობრივ ეკონომიკაში კაპიტალდაბანდებებისთვის დამატებით დაინტერესებას.

[47] Amankwaa, A.A., 1995.The world economic system and international migration in less developed countries: An ecological approach. In: International Migration, 33(1), P. 95-113;

[48] Massey D.A., 2002. Synthetic theory of international migration. World in the mirror of intarnational migration. International migration of population: Russia and contemporary world. Volume 10. Moscow, MSU, Max Press, P. 143;

[49] Lee S.E., 1966. A Theory of Migration, Demography, Vol. 3, No.1, P. 47-57;

[50] Jennissen, R. P. W., 2004. Macro-Economic Determinants of International Migration in Europe, Economic determinants of international migration types which are sensitive and insensitive to immigration policies, Amsterdam, , Rozenberg Publishers, P. 179-181;

[51] ჭელიძე ნ., 2006. შრომითი ემიგრაცია პოსტსაბჭოთა საქართველოში, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, მიგრაციის კვლევის ცენტრი, თბილისი, გვ. 16-20;

* ნეოკლასიკური თეორიის თანახმად რაციონალურად მოქმედი სუბიექტი ემიგრირდება იმიგრაციის ქვეყანაში მოსალოდნელი მაღალი ხელფასის გამო, მაშინ როცა შრომითი მიგრაციის ახალი ეკონომიკური თეორიის შესაბამისად, მიგრანტი ცდილობს გადალახოს თავის ქვეყანაში არსებული

# 5. კონტრასტები მიგრანტთა კონტრაბანდასა და ადამიანით ვაჭრობას (ტრეფიკინგი) შორის

## 5.1 ადამიანით ვაჭრობა (ტრეფიკინგი)

არალეგალურ მიგრაციას ყველთვის თან ახლავს ისეთი რისკ-ფაქტორები, როგორიცაა ინდივიდის ადამიანით ვაჭრობის (ტრეფიკინგი) მსხვერპლად ქცევა. არალეგალური მიგრაცია განისაზღვრება, როგორც ,,იმ პირთა განსაკუთრებულად არაორგანიზებული მიგრაციის ყველა სახე და ნაკადი, რომლებიც არ ითვალისწინებენ მიგრაციის წარმომშობი, ტრანზიტული და/ან მიმღები ქვეყნების შესაბამის კანონებსა და წესებს",[52] რომელიც მოიცავს როგორც ადამიანთა ტრეფიკინგს, ასევე მიგრანტთა კონტრაბანდას და მიგრაციის სხვა ფორმებს, რასაც შეიძლება ეწოდოს არალეგალური ან არადოკუმენტირებული.

ტრეფიკინგისა და მიგრანტთა კონტრაბანდის დანაშაულის შემადგენლობა ძალიან გვანან ერთმანეთს და სწორედ ეს ურთულებს სამართალდამცავებს ერთმანეთისაგან გამიჯნონ დანაშაულის ეს ორი სახე.

ადამიანით ვაჭრობა (ტრეფიკინგი)* ტრანსნაციონალური ორგანიზებული დანაშაულის სახეა, რომელიც თავისი ხასიათით წარმოადგენს ადამიანის უფლებების მძიმე დარღვევას.[53]

შემთხვევა ადამიანით ვაჭრობად (ტრეფიკინგად) დაკვალიფიცირდება თუ სახეზე გვაქვს, შემდეგი სამი ელემენტი: **ქმედება, საშუალება** და **მიზანი.**[54]

გაეროს კონვენციის თანახმად, „ტრეფიკინგი" ნიშნავს ადამიანთა გადაბირებას, ტრანსპორტირებას, გადაყვანას, შეფარებას ან მიღებას, მუქარის, ძალის გამოყენების ან იძულების სხვა საშუალებით, მოტაცებით, თაღლითობით, მოტყუებით, ძალაუფლების ან პირის უმწეობის ბოროტად გამოყენებით ან იმ პირის თანხმობის მისაღწევად თანხის ან სხვა

---

შრომის ბაზრისა და სხვა ცხოვრებისეული სირთულეები საზღვარგარეთ დროებითი დასაქმების მეშვეობით, გამომუშავებული თანხით კი მოახერხოს სამშობლოში შემოსავლის წყაროს შექმნა. ნათელი გახდა, რომ იმიგრაციული და ემიგრაციული ქვეყნების ხელფასებს შორის განსხვავება არ წარმოადგენს გადაადგილების მოტივაციის ერთადერთ და არც ყველაზე მნიშვნელოვან ფაქტორს.

[52] მიგრაციის საერთაშორისო ორგანიზაციის ანგარიში, 2000. სამოქალაქო განათლების განყოფილება, არალეგალური მიგრაცია და მიგრანტთა უკანონო გადაყვანა - საქართველო, თბილისი;

* 2003 წლიდან ადამიანით ვაჭრობა (ტრეფიკინგი) დასჯადი ქმედებაა, რომელიც რეგულირებულია საქართველოს სისხლის სამართლის კოდექსის $143^1$-ე (ადამიანით ვაჭრობა (ტრეფიკინგი)), $143^2$-ე (არასრულწლოვნით ვაჭრობა (ტრეფიკინგი)) და $143^3$-ე (ადამიანით ვაჭრობის (ტრეფიკინგის) მსხვერპლის (დაზარალებულის) მომსახურებით სარგებლობა) მუხლებით. 2006 წელს საქართველოს პარლამენტის მიერ მიღებულ იქნა, ასევე, საქართველოს კანონი „ადამიანით ვაჭრობის (ტრეფიკინგის) წინააღმდეგ ბრძოლის შესახებ";

[53] „საქართველოს კანონი ადამიანით ვაჭრობის (ტრეფიკინგის) წინააღმდეგ ბრძოლის შესახებ", საკანონმდებლო მაცნე, სსმ, 15, 16/05/2006;

[54] ადამიანით ვაჭრობის (ტრეფიკინგის) დანაშაულის მსხვერპლთა იდენტიფიცირების სახელმძღვანელო პრინციპები საქართველოს სახელმწიფო საზღვარზე (სასაზღვრო გამტარი და საბაჟო გამშვები პუნქტები, სახმელეთო და სანაპირო საზღვარი) მომუშავე პერსონალისთვის, დამტკიცებულია ადამიანით ვაჭრობის (ტრეფიკინგის) წინააღმდეგ მიმართული ღონისძიებების განმახორციელებელი საუწყებათაშორისო საკოორდინაციო საბჭოს მიერ 19 დეკემბერი, 2017; <http://www.justice.gov.ge/> [წვდომის თარიღი: 11.01.2020];

სარგებლის მიცემით ან მიღებით, ვისი დამოკიდებულების ქვეშაც იმყოფება მეორე პირი, ამ ადამიანთა ექსპლუატაციის მიზნით.[55]

ადამიანით ვაჭრობა (ტრეფიკინგი) შეიძლება განხორციელდეს როგორც მსხვერპლის საზღვარგარეთ გაყვანით (თუნდაც რამდენიმე სახელმწიფოს საზღვრის გადაკვეთით), ისე ერთი სახელმწიფოს ტერიტორიაზე, საზღვრის კვეთის გარეშე.

## 5.2 მიგრანტთა კონტრაბანდა

მიგრანტთა კონტრაბანდა არის არალეგალური მიგრაციის ერთ-ერთი სახე, რომელიც ხორციელდება გამგზავნი, სატრანზიტო და მიმღები ქვეყნების მარეგულირებელი ნორმების დარღვევით. სამართლებრივი საფუძვლის გარეშე მიგრაციის მკაფიო და საყოველთაოდ აღიარებული განსაზღვრება არ არსებობს. დანიშნულების ქვეყნის თვალთახედვით, ეს არის აღნიშნულ ქვეყანაში არალეგალური შესვლა, დარჩენა ან მუშაობა, რაც ნიშნავს იმას, რომ მიგრანტს არ აქვს ნებართვა, ან მოცემული ქვეყნის საიმიგრაციო რეგულაციებით განსაზღვრული (ქვეყანაში) შესვლის, დარჩენის ან მუშაობისთვის აუცილებელი დოკუმენტები.[56]

პალერმოს ოქმის, მესამე მუხლის თანახმად, მიგრანტთა კონტრაბანდა ნიშნავს პირდაპირი და არაპირდაპირი გზით შესყიდვას, ფინანსური ან სხვა მატერიალური სარგებლის მიღებისთვის და ამ მიზნით პირის (ან პირთა ჯგუფის) არალეგალური გზით შეყვანას სახელმწიფოში, როდესაც მიგრანტი ეროვნებით არა არის ამ სახელმწიფოს მუდმივი მაცხოვრებელი და არც დროებითი მოქალაქე.[57]

ადამიანის უკანონო (მიგრანტთა კონტრაბანდა) გადაყვანის დროს, როგორც წესი, როდესაც პიროვნება მიაღწევს დანიშნულების ადგილამდე, მისი საქმიანი ურთიერთობა შუამავალთან სრულდება,[*] ხოლო ტრეფიკინგის შემთხვევაში, როდესაც მსხვერპლი მიაღწევს საბოლოო დანიშნულების ადგილს, ის ხდება შემდგომი ექსპლუატაციის ობიექტი. ამასთან, საზღვარზე უკანონო გადამყვანი ცდილობს, ხელი შეუწყოს სხვა პირს საზღვრის არალეგალურ გადაკვეთაში ფინანსური ან სხვა მატერიალური სარგებლის მოპოვების

[55] United Nations Convention against Transnational Organized Crime, Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, Article 3, (a), Adopted by the UN General Assembly: 15 November 2000, by resolution 55/25;

[56] მიგრაციის საერთაშორისო ორგანიზაცია (IOM), 2004. მიგრაციის საკითხთა სამთავრობო კომისია, მიგრაციის ტერმინთა განმარტებითი ლექსიკონი, ჟენევა, გვ. 49;

[57] Protocol against the Smuggling of Migrants by Land, Sea and Air, Supplementing the United Nations Convention against Transnational Organized Crime, Article 3, "Smuggling of migrants", General Assembly resolution 54/212 of 22 December 1999;

[*] „ტრანსნაციონალურ ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლის შესახებ გაერო-ს კონვენციის ოქმი - სახმელეთო, საზღვაო და საჰაერო საშუალებებით მიგრანტთა საზღვარზე უკანონო გადაყვანის აღკვეთის შესახებ„ რატიფიცირებულ იქნა საქართველოს პარლამენტის მიერ 2006 წლის 7 ივნისის N 3201 – Iს დადგენილებით, გარდა ამისა, საქართველოს მიერ რატიფიცირებულია ,,ევროპის საბჭოს კონვენცია ადამიანით ვაჭრობის (ტრეფიკინგის) წინააღმდეგ ბრძოლის შესახებ".

მიზნით.[58] ადამიანით მოვაჭრე ცდილობს, გაუწიოს პიროვნებას ექსპლუატაცია და მიიღოს ფინანსური ან სხვა სახის სარგებელი ამ პიროვნების გამოყენებით.[59]

აქედან გამომდინარე ჩანს, რომ ამ ორ ქმედებას შორის მკაფიო განსხვავება არსებობს: უკანონო გადაყვანა გულისხმობს პირის უკანონო შესვლის ხელშეწყობას იმ სახელმწიფოში, რომლის მოქალაქეს ან მუდმივ ბინადარს ეს უკანასკნელი არ წარმოადგენს, ფინანსური ან სხვა მატერიალური სარგებლის მიღების მიზნით პირდაპირი ან არაპირდაპირი გზით. განსხვავებით ადამიანით ვაჭრობისგან, რომელსაც შესაძლებელია ადგილი ჰქონდეს ნებისმიერ სიტუაციაში, არ აქვს მნიშვნელობა მსხვერპლს გადაიყვანენ სხვა სახელმწიფოში თუ მხოლოდ ერთი ადგილიდან მეორეში, ქვეყნის ფარგლებს შიგნით, უკანონო გადაყვანა აუცილებლად გულისხმობს სახელმწიფოს საზღვრის კვეთას.

ტრეფიკინგი მოიცავს ისეთ ქმედებებს, რომელიც ინდივიდის მიმართ სისხლის სამართლებრივ დანაშაულს წარმოადგენს, ხოლო ადამიანთა კონტრაბანდის დროს ირღვევა სახელმწიფოს საზღვრის დაცვის მარეგულირებელი ნორმები.

აქედან გამომდინარე, შეიძლება მკაფიოდ გაიმიჯნოს ერთმანეთისაგან ქმედებები (აქტივობები), რომელიც ადამიანით კონტრაბანდისა და ადამიანით ვაჭრობისათვის (ტრეფიკინგი) არის დამახასიათებელი. ადამიანებით კონტრაბანდისათვის ურთიერთობა წყდება გადაყვანის მომენტიდან, ხოლო ტრეფიკინგის მიზანია, იძულების გზით, რაც შეიძლება ხანგრძლივი კონტაქტი შეინარჩუნოს ტრეფიკინგის მსხვერპლთან, რათა იგი მუდმივი ექსპლუატაციის რეჟიმში იმყოფებოდეს.[60]

[58] United Nations Office on Drugs and Crime, Global Study on Smuggling of Migrants 2018, United Nations publication, Sales No. E.18.IV.9, New York, 2018, 19-21;

[59] United Nations Convention against Transnational Organized Crime, Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime, Article 3, (a), Adopted by the UN General Assembly: 15 November 2000, by resolution 55/25;

[60] ჯანაშია ჯ., 2015. ადამიანით ვაჭრობის (ტრეფიკინგი) წინააღმდეგ ბრძოლის საერთაშორისო და შიდა ეროვნული სამართლებრივი მექანიზმები და რეგულაციები, თბილისი, გვ. 59;

# დასკვნა

როგორც ნაშრომში მოცემული ფაქტების ანალიზი გვიჩვენებს, სახელმწიფოში მიგრაციულ პროცესებს განსაზღვრავს დადებითი ეკონომიკური მაჩვენებლები. მიგრაციული პროცესების სწორად მართვისა და დარეგულირების შემთხვევაში, მიგრაციული პროცესები სახელმწიფოს ეკონომიკისათვის დადებითი ეფექტის მომტანი შეიძლება გახდეს.

კვლევის შედეგების ანალიზით დადგინდა, რომ სახელმწიფოში შექმნილი მძიმე ეკონომიკური ვითარება, მკვეთრად გაუარესებული მოსახლეობის ცხოვრების დონე, სიღარიბის ზღვარს მიღმა დარჩენილი მოსახლეობის ზრდა, უმუშევრობა, შრომის ბაზრის ნორმალური ფუნქციონირების შეუძლებლობა და არასტაბილურობა, ქვყნიდან მასშტაბური შრომითი მიგრაციის მთავარ მიზეზს წარმოადგენს, რომლის მოგვარებაც არა მარტო ერთი კონკრეტული ორგანოს, არამედ კომპლექსურად მთელი სახელმწიფო სტრუქტურების ამოცანაა.

სახელმწიფოთათვის სასიცოცხლოდ მნიშვნელოვანია სწორი, საშინაო და საგარეო პოლიტიკური კურსის გატარება, როგორც მიგრაციული პროცესების რეგულირების კუთხით, ისე ეკონომიკური უსაფრთხოების უზრუნველყოფის მხრივ. ეკონომიკის განვითარებაზეა დამოკიდებული სახელმწიფოთა სამხედრო პოტენციალი, მოსახლეობის განათლება, დემოგრაფიული მდგომარეობა, მიგრაცული უსაფრთხოება და სახელმწიფოთა განვითარების უამრავი სხვა ფაქტორი.

აქედან გამომდინარე, ეროვნული უსაფრთხოების უზრუნველმყოფელ ერთ-ერთ უმნიშვნელოვანეს სექტორს ეკონომიკა წარმოადგენს, რომელიც ქვეყნის თავდაცვისუნარიანობის მნიშვნელოვანი განმსაზღვრელია და დარგს ეროვნული უსაფრთხოების უზრუნველმყოფის სტატუსს ანიჭებს. ეკონომიკური უსაფრთხოების რღვევა სახელმწიფოში დემოგრაფიულ პრობლემებს, მასშტაბურ მიგრაციას, „ტვინების გადინებას“, შესაბამისად შრომისა და ბრძოლისუნარიანი მოსახლეობის შემცირებას იწვევს.

მნიშვნელოვანია სახელმწიფოშოი ჩამოყალიბდეს ის ძირითადი მიმართულებები, რომლებიც უზრუნველყოფენ სახელმწიფოში ეკონომიკური უსაფრთხოების ერთიანი კონცეფციის შექმნას, მიგრაციული პროცესების მართვის გაუმჯობესებას, რაც თავისთავად გულისხმობს ეროვნული უსაფრთხოების უზრუნველყოფას, რადგან სახელმწიფოს ეკონომიკურ უსაფრთხოებას პირდაპირ უკავშირდება პოლიტიკურ დამოუკიდებლობა და სუვერენიტეტი.

# ბიბლიოგრაფია


1. საქართველოს კანონი „ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ“, საქართველოს პარლამენტი, საკანონმდებლო მაცნე, 04/03/2015;
2. „საქართველოს კანონი ადამიანით ვაჭრობის (ტრეფიკინგის) წინააღმდეგ ბრძოლის შესახებ“, საკანონმდებლო მაცნე, სსმ, 15, 16/05/2006;
3. საქართველოს კანონი „შრომითი მიგრაციის შესახებ“, საქართველოს პარლამენტი, საკანონმდებლო მაცნე, 01/11/2015;
4. საქართველოს პარლამენტის დადგენილება „საქართველოს ეროვნული უსაფრთხოების კონცეფციის“ დამტკიცების შესახებ, საკანონმდებლო მაცნე, 23/12/2011;
5. საქართველოს პარლამენტის დადგენილება №5586-IIს, „საქართველოს დემოგრაფიული უსაფრთხოების კონცეფციის“ დამტკიცების შესახებ, საკანონმდებლო მაცნე, 24/06/2016;
6. საქართველოს მთავრობის დადგენილება №622, „საქართველოს 2016-2020 წლების მიგრაციის სტრატეგია“, საკანონმდებლო მაცნე, 14/12/2015;
7. საქართველოს მთავრობის დადგენილება #314, „მიგრაციის საკითხთა სამთავრობო კომისიის შექმნისა და დებულების დამტკიცების შესახებ“, საკანონმდებლო მაცნე, 13.10.2010;
8. საქართველოს მთავრობის დადგენილება №100, საქართველოს მცირე და საშუალო მეწარმეობის განვითარების სტრატეგიის 2016-2020 წლებისთვის და საქართველოს მცირე და საშუალო მეწარმეობის განვითარების სტრატეგიის 2016-2017 წლების სამოქმედო გეგმის დამტკიცების შესახებ, საკანონმდებლო მაცნე, 26/02/2016;
9. საქართველოს მთავრობის დადგენილება №100, საქართველოს მცირე და საშუალო მეწარმეობის განვითარების სტრატეგიის 2016-2020 წლებისთვის და საქართველოს მცირე და საშუალო მეწარმეობის განვითარების სტრატეგიის 2016-2017 წლების სამოქმედო გეგმის დამტკიცების შესახებ, 10-18;
10. ადამიანით ვაჭრობის (ტრეფიკინგის) დანაშაულის მსხვერპლთა იდენტიფიცირების სახელმძღვანელო პრინციპები საქართველოს სახელმწიფო საზღვარზე (სასაზღვრო გამტარი და საბაჟო გამშვები პუნქტები, სახმელეთო და სანაპირო საზღვარი) მომუშავე პერსონალისთვის, დამტკიცებულია ადამიანით ვაჭრობის (ტრეფიკინგის) წინააღმდეგ მიმართული ღონისძიებების განმახორციელებელი საუწყებათაშორისო საკოორდინაციო საბჭოს მიერ 19 დეკემბერი, 2017; <http://www.justice.gov.ge/> [წვდომის თარიღი: 11.01.2020];
11. ბადურაშვილი ი., 2017. მიგრაციის სახელმძღვანელო, მიგრაციის ფორმები, მიგრაციის პოლიტიკის განვითარების საერთაშორისო ცენტრი, თბილისი, გვ. 34-48;
12. ბრუნი ბ.დ., ჭითანავა მ., 2017. მოსახლეობის დაბერება და ხანდაზმულები საქართველოში 2014 წლის მოსახლეობის საყოველთაო აღწერის შედეგებზე დაფუძნებული მიმოხილვა, საქართველოს სტატისტიკის ეროვნული სამსახური (საქსტატი), გაერთიანებული ერების ორგანიზაციის მოსახლეობის ფონდი (UNFPA), თბილისი, გვ. 6-7;

13. ბასილია თ., სილაგაძე ა., ჩიკვაიძე თ., 2001. პოსტსოციალისტური ტრანსფორმაცია: საქართველოს ეკონომიკა XXI საუკუნის მიჯნაზე, თბილისი, გვ. 462- 463;
14. თეთრუაშვილი ზ., თეთრუაშვილი-ქარდავა მ., 2006. საქართველოს ეკონომიკური უსაფრთხოების უზრუნველყოფის ფინანსურ-ეკონომიკური ფაქტორები და მისი რეგულირების მექანიზმები საბაზრო ურთიერთობის ფორმირების პირობებში;
15. კუტუბიძე კ., 2008. ინტელექტუალური რესურსები და ქართული რეალობა, ჟურნ. „ბიზნესი და კანონმდებლობა“, №17 გამოცემა, თბილისი;
16. მიგრაციის საერთაშორისო ორგანიზაცია (IOM), 2004. მიგრაციის საკითხთა სამთავრობო კომისია, მიგრაციის ტერმინთა განმარტებითი ლექსიკონი, ჟენევა, გვ. 49;
17. მიგრაციის საერთაშორისო ორგანიზაცია (IOM), 2004., მიგრაციის საკითხთა სამთავრობო კომისია, მიგრაციის ტერმინთა განმარტებითი ლექსიკონი, ჟენევა;
18. მიგრაციის საერთაშორისო ორგანიზაციის ანგარიში, სამოქალაქო განათლების განყოფილება, არალეგალური მიგრაცია და მიგრანტთა უკანონო გადაყვანა - საქართველო, თბილისი, 2000 წელი;
19. მესხია ი., 1966. საქარათველოს ეკონომიკური უსაფრთხოების კონცეპტუალური საკითხები. ჟურნ. „ეკონომიკა“ №1-3, გვ. 4;
20. მაღლაკელიძე თ., 2002. ეკონომიკური უსაფრთხოება, თბილისი, გვ. 22;
21. ოთინაშვილი რ., 2002. ეკონომიკური უსაფრთხოების სახელმწიფო სტრატეგია. იხ. საქართველოს სტრატეგიული კვლევისა და განვითარების ცენტრი, ბიულეტენი № 73. აგვისტო, გვ. 3;
22. ომანაძე ს., გაჩეჩილაძე ნ., ლებანიძე ა., ჩაჩანიძე ს., 2017. თაობა გარდამავალ პერიოდში ახალგაზრდობის კვლევა 2016 - საქართველო, ფრიდრიხ ებერტის ფონდი სამხრეთ კავკასიის რეგიონალური ოფისი, თბილისი, გვ. 7-11;
23. საქართველოს სტატისტიკის ეროვნული სამსახური, ცხრილი #3, #4, <http://www.geostat.ge/?action=page&p_id=172&lang=geo> [წვდომა: 06.01.2020];
24. საქართველოს სტატისტიკის ეროვნული სამსახური, ცხრილი #2, <http://www.geostat.ge/?action=page&p_id=172&lang=geo> [წვდომა: 09.01.2020];
25. „ტრანსნაციონალურ ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლის შესახებ გაერო-ს კონვენციის ოქმი - სახმელეთო, საზღვაო და საჰაერო საშუალებებით მიგრანტთა საზღვარზე უკანონო გადაყვანის აღკვეთის შესახებ„ რატიფიცირებულ იქნა საქართველოს პარლამენტის მიერ 2006 წლის 7 ივნისის N 3201 – Iს დადგენილებით, გარდა ამისა, საქართველოს მიერ რატიფიცირებულია ,,ევროპის საბჭოს კონვენცია ადამიანით ვაჭრობის (ტრეფიკინგის) წინააღმდეგ ბრძოლის შესახებ“.\
26. ქაჯაია მ., 2005, ახალგაზრდობის გარე მიგრაციული განწყობის ზოგიერთი საკითხის შესახებ, მიგრაციული პროცესები თანამედროვე გლობალიზებად მსოფლიოში, მიგრაციის კვლევის ცენტრი, თბილისი, გვ. 48-49;
27. ჭელიძე ნ., 2006., შრომითი ემიგრაცია პოსტსაბჭოთა საქართველოში, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი მიგრაციის კვლევის ცენტრი, თბილისი, გვ. 5-7;
28. ჯანაშია ჯ., 2015. ადამიანით ვაჭრობის (ტრეფიკინგი) წინააღმდეგ ბრძოლის საერთაშორისო და შიდა ეროვნული სამართლებრივი მექანიზმები და რეგულაციები, თბილისი, გვ. 59;

29. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 2, Adopted by General Assembly resolution 45/158 of 18 December 1990;
30. The Universal Declaration of Human Rights (UDHR), Adopted by the United Nations General Assembly, Resolution 217, Palais de Chaillot, Paris, France, 10 December, 1948;
31. The International Labour Organization's Fundamental Conventions, (Freedom of Association and Protection of the Right to Organise Convention, 1948 (No. 87), Right to Organise and Collective Bargaining Convention, 1949 (No. 98), Forced Labour Convention, 1930 (No. 29), Abolition of Forced Labour Convention, 1957 (No. 105), Minimum Age Convention, 1973 (No. 138), Worst Forms of Child Labour Convention, 1999 (No. 182), Equal Remuneration Convention, 1951 (No. 100), Discrimination (Employment and Occupation) Convention, 1958 (No. 111);
32. United Nations Convention against Transnational Organized Crime, Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, Article 3, (a), Adopted by the UN General Assembly: 15 November 2000, by resolution 55/25;
33. United Nations Convention against Transnational Organized Crime, Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime, Article 3, (a), Adopted by the UN General Assembly: 15 November 2000, by resolution 55/25;
34. World Trade Organization (wto), World Trade Report, Geneva, 2011
35. Migration and Globalization, Why Does Migration Happen? <http://www.globalization101.org/uploads/File/Migration/migration.pdf 9-14>; [Access: 12.01.2020];
36. National Security Strategy of the United States of America, December 2017, Pillar II: Promote American Prosperity, P.18-22, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf > [Access:09.01.2020];
37. The United Nations, <http://www.un.org/en/> [Access:09.01.2020];
38. The International Organization for Migration, <https://www.iom.int/about-iom,> [Access: 09.01.2020];
39. The International Labour Organization, <https://www.ilo.org/dyn/normlex/en/f?p=1000:62:0::NO:62:P62_LIST_ENTRIE_ID:2453907:NO>, [Access: 09.01.2020];
40. Department of Economic and Social Affairs, United Nations, International Migration Report, New York, 2017, 4-8;
41. Jennissen, R. P. W. 2004. Macro-economic determinants of international migration in Europe, Amsterdam, , Rozenberg Publishers, P. 93-106;
42. Bell, S., Alves, S., de Oliveira, E. S., & Zuin, A., 2010. Migration and Land Use Change in Europe: A Review, , Leibniz Centre for Agricultural Landscape Research (ZALF), Eberswalder Straße 84, 15374 M¨uncheberg, Germany. ISSN 1863-7329, P. 16-18;
43. The European Migration Network, Asylum and Migration Glossary 3.0, 2014. a tool for better comparability produced by the European Migration Network, October, P. 187;
44. Usher E, 2004. Migration and labour. In: Usher E, editor. Essentials of migration management: a guide for policy makers and practitioners. Geneva: United Nations Publications;
45. Simon J, Kiss N, Łaszewska A., 2015. Public Health Aspects of Migrant Health: A Review of the Evidence on Health Status for Labour Migrants in the European Region. Health Evidence Network Synthesis Report, No. 43. et al. Copenhagen: WHO Regional Office for Europe, P. 39;
46. International Organization for Migration, World Migration Report 2018, The UN Migration Agency, Part I: Data and information on migration, P.10-13;

47. Jennissen, R. P. W. 2004. Macro-economic determinants of international migration in Europe, Amsterdam, Rozenberg Publishers, P. 44-46;
48. Öberg, S., 1997. Theories on inter-regional migration: an Overview. In: Blotevogel, H.H. and Fielding A.J. (eds.), People, jobs and mobility in the new Europe, Chichester: Wiley, P. 3-22
49. Chiswick B.R., 2000, Are Immigrants Favorably Self-Selected? An Economic Analysis. Chapters 3. Migration Theory. Talking Across Disciplines. Edited by : Hollifield J.F., Brettel C.B., P. 61-76;
50. Massey D., Joaquin A., Koucouci Ali, Pellegrino A., Taylor E.J., 1998. Worlds in Motion: Understanding International Migration at the End of the Millenium. Oxford: Oxford University Press.;
51. Taylor, J.E., 1999. The new economics of labour migration and the role of remittances in the migration process. In: International Migration,37(1), P. 63-88;
52. Amankwaa, A.A., 1995.The world economic system and international migration in less developed countries: An ecological approach. In: International Migration, 33(1), P. 95-113;
53. Massey D.A., 2002. Synthetic theory of international migration. World in the mirror of intarnational migration. International migration of population: Russia and contemporary world. Volume 10. Moscow, MSU, Max Press, P. 143;
54. Lee S.E., 1966. A Theory of Migration, Demography, Vol. 3, No.1, P. 47-57;
55. Jennissen, R. P. W., 2004. Macro-Economic Determinants of International Migration in Europe, Economic determinants of international migration types which are sensitive and insensitive to immigration policies, Amsterdam, , Rozenberg Publishers, P. 179-181;
56. Docquier F., Rapoport H., 2007. Skilled Migration: The Perspective of Developing Countries, IZA DP No. 2873, Forschungsinstitut zur Zukunft der Arbeit Institute for the Study of Labor, Bonn, June, P. 4-7;
57. Богданов И. П., Испиран М., 2001. Экономическая безопасность России, Ж. „Теория и практика“ P.. 28;
58. Абалкин Л. 1994. Экономическая безопасность России утроз Ж. „Вопросы економики“ №T12, P. 5;
59. Иларионов А., 1998. Критерии экономической безопасности, Ж. „Вопроси економики“ № 10, P. 49;
60. Афонцев С., 2001. Дискуссионные проблемыконцепции националной экономической безапасности Россия XXI (Москва), P. 66;
61. Галкина С., Клейнер Г., 2003. Высветление экономики и укрепление националной безопасности, Россыйскыи экономический журнал §5-6, P. 3;

Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 34 - 40 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

# EVALUATING CYBER THREATS IN CAUCASUS
# ACTORS POSING THREATS TO GEORGIAN CYBER SPACE

Salome Mikiashvili, PhD in American Studies
International Black Sea University

**ABSTRACT.** Cyber war is the action aimed at destroying information and communication systems, while web war is a deliberate action involving attempts by one or several actors via open or hidden channels, to transform the perception of the target actor so that the transformation will bring desirable results to the attacker. Apart from critical infrastructure of national importance, active membership of anti-terrorist coalition and considering the clear-cut Euro-Atlantic vector of the country, additional target is the Georgia-based information networks and infrastructure of other countries, international organizations and foreign businesses. In the paper is shown that the recent cyber security activities in the Caucasus region suggest that we are dealing with a completely new precedent related to the deployment of forces in the cyber security field. In fact, this case has clearly demonstrated the increasingly active use of cyber security elements in international relations, and primarily in terms of distribution of power.

**Keywords:** cyber, cyber threats, Caucasus, cyber space

Using cyber elements to reach political economic or military goals and to gain geopolitical advantage is the reality of the modern world. Western experts more and more frequently discuss the tendency accompanying transformation of cyber war into a web war. Cyber war is the action aimed at destroying information and communication systems, while web war is a deliberate action involving attempts by one or several actors via open or hidden channels, to transform the perception of the target actor so that the transformation will bring desirable results to the attacker. Georgian cyber space is not an exception from this. The recent conflicts on the post-soviet territories prove that politically motivated cyberattacks are relevant to Georgia as well. Apart from critical infrastructure of national importance, active membership of anti-terrorist coalition and considering the clear-cut Euro-Atlantic vector of the country, additional target is the Georgia-based information networks and infrastructure of other countries, international organizations and foreign businesses. The threat to the above-mentioned objects may be coming from such actors as:

- countries having well-developed, high cyber attacking potential (Russia, China Iran)
- cyber divisions of terrorist organisations and ideologically motivated or extremist hackers

•financially motivated cyber criminals. (L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi)

Let's discuss each actors separately. Studying their capabilities is very relevant for Georgia too. Russian Federation. The Ministry of Defence of Russia establishes its own cyber command, which according to the available information will be responsible for implementing attacking cyber events, including propaganda-based events and inserting malware in the administration and control systems of the adversary. Other divisions specializing in computer network operations are established in the armed forces of Russia. Reportedly, Russia is actively developing distance access tools for critical infrastructure industrial control system.(ICS)According to experts, unknown Russian actors have been successful in damaging several ICS manufacturers' software and inserting malicious code into legal software updates and thus providing direct access to the user's website.

"Today, there is no doubt that for political goals the Russian authorities are actively using the so-called method of information-psychological impact that Western scholars characterize as the initial phase of modern Russian conflict creation. This phase involves conducting unconventional operations to manipulate public opinion within the target country and in the international media. In light of the intensified activities, the Russian combat units begin to penetrate into the target area under the guise of local armed forces. This completes the unconventional operations phase. If the operation succeeds, the activities to legitimize intervention begins with the legend of " Defending Minority Rights".(L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi) [1]

"The second phase involves conventional actions, but the success of the first, non-conventional phase of the annexation of Crimea has greatly facilitated the conventional phase of the conflict in favour of Russia. Russia's political elite views information as a source of power, creating solid ground for implementing the country's information operations." (L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi). According to the national security concept, Russia views nationalist, separatist, and radical religious agitation measures as threat and considers it necessary to spread "true" information and develop a local platform (e.g its own social media). While analyzing future threats, the same document points out that "the global information battle will be intensified". Therefore, computer network operations are seen as an organic, unchanging part of information security. Russia seeks to process not only the technical part of the information, but also exercise control over the cognitive information constituent. For this reason, according to experts, the notion of "cyber security" in Russian doctrines and conceptual documents is replaced by the term "information security" .If we analyze the ongoing conflicts with Russia's involvement in the post-Soviet space, it becomes clear that it views the conflict areas as a type of polygon for probing kinetic types of weapons and cyberattack

potential. Thus, for Georgia it is vitally necessary to perform a thorough analysis of the Russian cyber activities and information warfare and to manage the arising risks. It should be considered that even less technologically advanced attacks, such as DDoS attacks or so-called “defacement” of websites, should, as a rule, be considered part of Russia's cyber-information warfare [2].

Generally the interests of the Russian hacking groups such as: APT28 are progovernmental. It serves the interests of Russian federation. The spheres of interests are: Eastern European governments and Caucasus as a whole (especially Georgia). The Caucasus, a region that includes independent states of Georgia, Armenia, and Azerbaijan continues to experience political disruption. The Georgian government’s strings to the West are a the reason of Moscow’s frustration, especially after the 2008 war. Overall, issues in the Caucasus likely serve as focal points for Russian intelligence collection efforts.

Since 2011, APT28 has been using bait written in Georgian makes us think that the targets are government agencies of Georgia as well as citizens of Georgia. According to the Fireeye report, called: “A Window Into Russia’s Cyber Espionage Operations”, APT28 is expected to seek information on Georgia's security and diplomatic positions. In particular, the group attacked the Ministry of Internal Affairs (MIA) and the Ministry of Defense. There was also an attempt to target a journalist working on the Caucasus problems and controversial news from Chechnya. “APT28 to the Ministry of Internal Affairs (MIA). The MIA possesses sensitive information on the internal structure of Georgia's security operations, its involvement in multilateral institutions, and the basis for government communications.” (FireEye, APT28: A Window into Russia’s Cyber Epionage Operations). According to the FIreeye investigation the hacking group APT28 had at least two specific attempts to attack the MIA. In one case, it was found that APT28 used malicious programs that attempted to disguise its activity as MIA legitimate mail. “This bait contained an Excel file containing malware, which was a bait document with a list of Georgian drivers. Backdoor attempted to establish a connection with the Georgian MIA Post Server and communicate with the MIA email addresses ending with mia.ge.gov ". After connecting to the Mail Server, the APT28 forwarder sent an email using the Driver License Title field (in Georgian). ) And attach a file containing the system intelligence info This tactic could have allowed APT28 to obtain data from the MIA in a less verifiable way, limiting the ability of the MIA's Department of Network Security to detect traffic. - Domain "MIA Users \ Ortachala ..." (Su Ten 1). This is probably the Interior Ministry in the object Ortachala district. bait document also contains metadata, which is named "Internal Affairs", as the company name and "Beka Nozadze" 4, as the author, it is the system administrator of a possible reference. The text of the document is intended to create a domain and user group [3].” (FireEye, APT28: A Window into Russia’s Cyber Epionage Operations). Since the Russo-Georgian War of 2008, Georgia and Russia have severed diplomatic relations, and Georgia has since sought to establish closer ties with Western security organizations. In in

June 2014, despite Russia's open political stance, Georgia, together with Ukraine and Moldova, signed association agreements with the EU. This move strengthened ties between these three countries and EU's political, economic and security spheres. Russian hacking groups are trying to steal information that exposes topics about US Georgia military cooperation and NATO. APT28 attacked a journalist covering the Caucasus news. Apt28s target became the journalist covering issues in the Caucasus region. In 2013, APT28 sent the false letter stating that the letter was authored by Reason magazine's "Principal Coordinator for the Caucasus Affairs Department". This section does not appear to exist. (Reason Magazine is American.) The letter invited the journalist as a journal contributor and was asking for the information regarding abovementioned political subject. Meanwhile, the bait-doc installed a SOURFACE backdoor in the victim's system. “From the content of the letter the experts came to conclusion that APT28 actors can read in at least two languages - Russian and English. The letter's grammar also indicates that English is not the author's native language, even though it appears to be from American journal. This fact clearly indicates that Russian may be the language preferred by the author APT28. Cyber Attacks on journalism can allow APT28 and its sponsors to monitor public opinion, identify dissidents, disseminate misinformation, or plan further attacks.” (FireEye, APT28: A Window into Russia’s Cyber Epionage Operations)

China. According to Chinese data, Chinese cyber operations are mainly for commercial purposes and therefore are not a direct threat to Georgia, although the networks of governmental and commercial structures of developed countries based in our country and information contained in their databases should not be overlooked. The Islamic Republic of Iran. Unlike China and Russia, Iran has trained hackers mainly on the basis of religious ideology. In particular, Iran has trained about a thousand hackers over the past five years with the influence of fundamental religious pathos. Their goal is to destroy critical infrastructure of their ideological adversary.” Iran is responsible for the DDoS attacks on US financial institutions in 2012-2013 and the February 2014 attack on the Las Vegas Sands Casino. According to the US intelligence community, Iran views its cyber project as a way to conduct asymmetric but proportionate actions against political adversaries and to seek intelligence. The fact that the US intends to ease sanctions on Iran and return it to the international oil market will not diminish the confrontation between the West and Israel in cyberspace. Authoritative US experts say Iran will increase cyberattacks, regardless of whether sanctions are in place. Moreover, if sanctions are eased, Iran will be able to mobilize and use its financial resources to develop its cyber capabilities, which in itself will increase the qualification of hacker groups and improve their methods of action.” (L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi. For Georgia, Iran's cyberattacks may pose a threat because, as Iran views it, there is infrastructure of hostile countries on our territory [4]. Also, given current trends, it is quite realistic for Iranian-backed terrorist organizations to exploit Georgian cyber networks for propaganda purposes. Given the above-mentioned, the scale of cyber threats facing Georgia is increasing in complexity

and diversity. Special attention should be paid to developing a mechanism for obtaining and analyzing information on cybercriminals' intentions, capabilities or activities and conducting active work in this regard.

The most real threat to Georgia's cyberspace is Russia's cyber activities, which are aimed at both disrupting critical infrastructure and using it for its own purposes.) It should be emphasized that even low-tech attacks, such as DDoS and Defacement attacks, can lead to disproportionate loss in poorly protected infrastructure. It should be noted that the Russian-implemented or backed cyberattack in Georgia could cause significant damages and even casualties. As for the cyber threats coming from Iran and China, first of all, we should not overlook the infrastructure and databases of the countries in Georgia, which these countries consider as their adversaries. These include Georgia's strategic partner USA, NATO member states and the European Union and the systems of these international organizations. “China's cyberattacks by major terrorist organizations [5,6]. There is a high probability of implementing a cyberattack that could lead to temporary, local damage to electronic services and websites. Organizing and executing cyberattacks that cause mass damage or casualties is unlikely at this stage. The probability of threats coming from profit-oriented cybercriminals is hard to predict. Raising public awareness, constant contact with critical infrastructure in the private sector, harmonization of local legislation with international one, active usage of international cooperation mechanisms for the fight against cybercrime are important. “(L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi)

One of the latest cyber-attacks conducted by Russia was on 28 October 2019, when a large scale cyber-attack was launched against the websites, servers and other operating systems of the Administration of the President of Georgia, the courts, various municipal assemblies, state bodies, private sector organisations and media outlets. As a result of the cyber-attack, the servers and operating systems of these organisations were significantly damaged, severely affecting their functionality.

“The above-mentioned cyber-attack was targeted at Georgia’s national security and was intended to harm Georgian citizens and government structures by disrupting and paralysing the functionality of various organisations, thereby causing anxiety among the general public. The investigation conducted by the Georgian authorities, together with information gathered through cooperation with partners, concluded that this cyber-attack was planned and carried out by the Main Division of the General Staff of the Armed Forces of the Russian Federation. Georgia condemns this cyber-attack, which goes against international norms and principles, once again infringing Georgia’s sovereignty in order to hinder the country’s European and Euro-Atlantic integration and democratic development.

The above-mentioned incident emphasises the importance of the Georgian Government’s efforts to strengthen cyber security at the national level and again demonstrates the need to build international

partnerships on cyber-security. Georgia, for its part, will continue close cooperation with partners, strengthening cyber-security at the national level in order to minimise such risks and potential threats in the future. We call on the international community to give an appropriate reaction to this development." (MFA OF Georgia, 2019)/ The Cyber attack was condemned by US, UK and many other EU and Nato countries The United States called on Russia to cease this behavior not only in Georgia but elsewhere. The government of US made special announcement on the US Department of State saying that: "On October 28, 2019, the Russian General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST, also known as Unit 74455 and Sandworm) carried out a widespread disruptive cyber attack against the country of Georgia. The incident, which directly affected the Georgian population, disrupted operations of several thousand Georgian government and privately-run websites and interrupted the broadcast of at least two major television stations. This action contradicts Russia's attempts to claim it is a responsible actor in cyberspace and demonstrates a continuing pattern of reckless Russian GRU cyber operations against a number of countries. These operations aim to sow division, create insecurity, and undermine democratic institutions. The United States calls on Russia to cease this behavior in Georgia and elsewhere. The stability of cyberspace depends on the responsible behavior of nations. We, together with the international community, will continue our efforts to uphold an international framework of responsible state behavior in cyberspace. We also pledge our support to Georgia and its people in enhancing their cybersecurity and countering malicious cyber actors. We will offer additional capacity building and technical assistance to help strengthen Georgia's public institutions and improve its ability to protect itself from these kinds of activities."

(Michael. R. Pompeo, The US condemns Russian Cyber attack against the country of Georgia, feb, 2020). Russia's reaction was feasible. Russia Duma representatives have denied the allegations and spoke about the political goals of US in the region.

Finally, it can be concluded that the recent cyber security activities in the Caucasus region suggest that we are dealing with a completely new precedent related to the deployment of forces in the cyber security field. This process was first revealed during the Azerbaijani-Armenian military confrontation in April 2016, when concurrent with the military action, there was also a more intense confrontation in cyberspace. In particular, in this case, the main players in the Caucasus region - Turkey and Russia - also engaged in a confrontation between the two countries [7]. The former supported Azerbaijan, the latter sided with the Armenia, and both countries are actively involved in the cyberspace confrontation. Of particular interest was the position of Iran, which preferred neutrality due to the fact that Iran has very good relations with both opposing countries in terms of politics, economics and trade.

In fact, this case has clearly demonstrated the increasingly active use of cyber security elements in international relations, and primarily in terms of distribution of power.

**REFERENCES**

1. L.Svanadze, A.Gociridze The Main Players of Cyber Space. CyberPolicy, Strategy and Challenges, 2015, Tbilisi
2. FireEye, APT28: A Window into Russia's Cyber Epionage Operations
3. საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდი:რუსეთ-საქართველოს 2008 წლის ომის კიბერგანზომილება, 2019, ა. გოცირიძე
4. CYBER ESPIONAGE Against Georgian Government (Georbot Botnet) LEPL Data Exchange Agency Ministry of Justice of Georgia
5. Cyberwar: How Russian Hackers and Trolls Helped Elect a President by Kathleen Hall Jamieson
6. Johnson P.A. (2002). M.N. Schmitt, B.T. O'Donnell (Eds.). Is It Time for a Treaty on Information Warfare?.
7. Michael. R. Pompeo, The US condemns Russian Cyber attack against the country of Georgia, feb, 2020

**Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 41 - 55 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# АНАЛИЗ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ КОДИРОВЩИКА HiSNeC НА ОСНОВАНИИ СТАТИСТИЧЕСКИХ ТЕСТОВ NIST STS

Пенкин Юрий, доктор физико-математических наук, профессор,
Национальный фармацевтический университет, Харьков, Украина
Хара Георгий, кандидат математических наук, доцент,
Национальный фармацевтический университет, Харьков, Украина
Федосеева Алина, кандидат технических наук,
Харьковский радиотехнический колледж, Харьков, Украина

# ANALYSIS OF THE CRYPTOGRAPHIC STRENGTH OF HiSNeC ENCODER BASED ON NIST STS STATISTICAL TESTS

Penkin Yuriy, Doctor of Science degree, Full professor,
National University of Pharmacy, Kharkiv, Ukraine
Khara Georgiy, PhD in Mathematical Sciences, Associate Professor,
National University of Pharmacy, Kharkiv, Ukraine
Fedoseeva Alina, PhD in Computer Science,
Kharkiv Radiotechnical College, Kharkiv, Ukraine

**АННОТАЦИЯ:** Представлено описание нового алгоритма генерации ключей шифрования, основанного на нелинейных трансформациях матричных структур в виде сеток Судоку. Рассмотрена реализация такого способа построения криптографических примитивов в работе блочного кодировщика *HiSNeC*. С помощью стандартных тестов *NIST STS* проведен анализ статистических свойств кодовых последовательностей шифротекстов, сгенерированных кодировщиком в режиме динамически изменяющихся входных ключей. Результатами тестирования подтверждена высокая криптографическая стойкость кодировщика, что позволяет рекомендовать *HiSNeC* для использования в системах низкоресурсной (lightweight) криптографической защиты.

**ABSTRACT:** The description of a new encryption key generation algorithm based on non-linear transformations of matrix structures in the form of Sudoku grids presented. The implementation of such a method for constructing cryptographic primitives in the work of the *HiSNeC* block encoder is considered. With standard NIST STS tests, we analyzed the statistical properties of cipher-text code sequences generated by the encoder in the mode of dynamically changing input keys. The test results is confirmed the high cryptographic strength of the encoder. This allows us to recommend the *HiSNeC* encoder for use in low-resource cryptographic protection systems.

**КЛЮЧЕВЫЕ СЛОВА:** *низкоресурсная защита данных; криптографический алгоритм; нелинейные операции матричных трансформаций; динамическая генерации ключа; блочный кодировщик HiSNeC; статистическое тестирование.*

**KEYWORDS***: lightweight data protection, cryptographic algorithm, nonlinear operations of matrix transformations, dynamic key generation, block encoder HiSNeC, statistic testing.*

**ВВЕДЕНИЕ.** В последние годы отмечается стремительный рост объема передаваемого интернет-трафика. Наряду с традиционными интернет-устройствами, такими как персональные компьютеры, ноутбуки, смартфоны, стали появляться устройства бытовой техники, транспорта, а также различные датчики, имеющие доступ в Интернет. Это явление получило название «Internet-things». Согласно прогнозам экспертов из Gartner в 2020 году количество устройств

интернета вещей должно достигнуть отметки в 7 миллиардов единиц. Интернет для «вещей» представляет собой самоконфигурированную беспроводную сеть между объектами типа бытовых приборов, транспортных средств, различных сенсоров и датчиков (Wireless sensors), а также меток радиочастотной идентификации (Radio Frequency Identification, RFID). Уже сейчас абсолютное большинство всех изготовленных (микро) процессоров используется во встроенных Smart-устройствах или системах (all embedded CPUs 4…32 bit) и лишь единицы процентов – в традиционных компьютерах (PC & workstation CPUs 32 bit). Следует заметить, что ключевой программно-технической особенностью подавляющего большинства таких приложений является использование ограниченного количества постоянных команд управления объектами, квазипостоянных потоков данных в сенсорных сетях либо постоянных сигналов коммуникации для RFID-меток.

Развитие указанных технологий делает чрезвычайно актуальными вопросы, связанные с их информационной безопасностью. Экспертами в области безопасности использование уязвимостей умных домов и интернета вещей рассматривается как один из основных методов кибер атак. В силу условий функционирования Internet-things, а также жестких ценовых рамок (свойственных массовому производству), эти устройства характеризуются значительными ограничениями на используемые ресурсы памяти, вычислительную мощность, источники питания и т.д. Отсюда следуют ограничения [1] на используемые технологические решения для средств низкоресурсной криптографии (LWC - Lightweight Cryptography). Многие требования, предъявляемые к алгоритмам LWC, были закреплены международным стандартом ISO/IEC FDIS 29192 – Information technology – Security techniques – Lightweight cryptography. Эти требования затрагивают вопросы обеспечения секретности, аутентичности, идентификации, безотказности и ключевого обмена (data confidentiality, authentication, identification, non-repudiation and key exchange). Разумеется, при разработке решений для LWC необходимо выдерживать требуемый баланс между безопасностью, ценой и производительностью.

Наиболее продуктивными среди шифров LWC на практике оказались алгоритмы блочного шифрования, развитие которых шло по двум направлениям:

- модификация известных алгоритмов блочного шифрования в сторону их ресурсного «облегчения» (при условии незначительного снижения криптографических свойств);
- разработка новых блочных шифров, ориентированных на оптимальную реализацию (на микропрограммном или аппаратном уровне).

Так во вторую часть стандарта ISO/IEC 29192-2 (Block ciphers) уже в 2012 году были включены два алгоритма: блочный шифр PRESENT (размер информационного блока – 64-бит, размер ключа – 80 или 128 бит) и блочный шифр CLEFIA (размер информационного блока – 128-бит, размер ключа – 128, 192 или 256 бит). Также конкурентоспособными считаются реализации алгоритмов ГОСТ 28147-89 – 615 GE, KATAN– 802-1054 GE, KTANTAN – 462-688 GE, Piccolo – 683 GE, PRESENT – 1075 GE, PRINT – 402-967 GE (существуют версии для разных размеров информационных блоков), SIMON&SPECK – 763-1396, TWINE и XTEA. Основные сравнительные характеристики этих алгоритмов приведены в [1], где обоснован вывод, что с общих позиций криптоанализа практически все блочные шифры LWC на платформах 8-разрядных микроконтроллеров типа AVR и ПЛИС (FPGA) являются уязвимыми. Указанный недостаток дополняется тем, что специальной адаптации к условиям работы с постоянными командами управления объектами, квазипостоянными потоками данных в сенсорных сетях либо постоянными сигналами для RFID-меток не имеет ни один из существующих шифров LWC (включая варианты AES).

Такая ситуация определяет актуальность дальнейших разработок алгоритмов и шифров LWC, которые продолжаются и в настоящее время. Однако в ближайшей перспективе получение «идеального» (неуязвимого) решения на традиционных принципах для LWC остается маловероятным. Более того разработчики, прежде всего, обеспокоены увеличением криптостойкости шифроключей и алгоритмов их расширения. За рамками анализа остается основная угроза, связанная с практической возможностью прямой внешней атаки типа «Попугай» (название авторское). Дадим краткое описание такой атаки. В условиях использования постоянных команд управления объектами или постоянных потоков данных, а также применении постоянного входного ключа, в передаваемых зашифрованных последовательностях могут быть достаточно просто выявлены однотипные фрагменты. Эта

ситуация является подобной к известным методам атак с избранными текстами. Отличие для «Internet-things» состоит в том, что злоумышленнику, имеющему перехваченный фрагмент шифротекста, нет необходимости определять секретные ключи. Ему достаточно при энергетическом перехвате канала коммуникации многократно ретранслировать этот фрагмент шифротекста (то есть, «как попугай», многократно повторять этот сигнальный фрагмент, даже не понимая его истинного смысла). В итоге при аварийной остановке управляемого объекта (при условии срабатывания защиты от многократно повторяемых одинаковых команд), а также подлоге данных сенсоров или RFID-меток злоумышленник добивается потери со стороны истинного пользователя контроля над текущим состоянием системы управления. В любом случае перспективной для устранения этих рисков является технология динамически изменяющихся входных ключей. Один из возможных вариантов реализации такой технологии осуществлен в авторском проекте *HiSNeC* (High Speed Network Coder).

Целью данной статьи является представление способа построения криптографических примитивов, используемого в работе блочного кодировщика *HiSNeC,* и подтверждение его криптографической стойкости на основании статистических исследований с помощью тестов NIST STS.

## ПРИНЦИП РАБОТЫ АЛГОРИТМА HISNEC

В основу алгоритма *HiSNeC* положен новый способ построение криптографических примитивов на основе операций нелинейной трансформации матричных структур, представленный в Патенте Украины на полезную модель № 129836 от 12.11.2018 года «Способ генерации ключей для симметричных блочных алгоритмов шифрования». Здесь математические принципы кодирования базируются на новой теории детерминированного хаоса в колебаниях дискретных структур матричного типа в виде сеток Судоку, предложенной проф. Пенкиным Ю.М. в [2].

Целесообразно напомнить, что большинство существующих алгоритмов блочного шифрования активно используют для формирования ключей шифрования данных операции: подстановок (замены одних элементов данных на другие при установке взаимно однозначного соответствия между множествами, содержащими эти данные) и перестановок (изменение порядка следования элементов данных). Например, способ, предложенный в патенте [3], базируется на аппаратной реализации контролируемых операций перестановок - криптографических примитивов, что позволяет существенно ускорить процессы шифрования. Однако следует иметь ввиду, что характерным для подобных скоростных шифров является использование предвычислений, в том числе осуществляющих и расширение секретного ключа. При этом требования по частоте смены ключей вступают в противоречие со скоростным применением шифров на базе предвычислений, поскольку необходимость многократного выполнения последних вносит существенные ограничения по быстродействию. В связи с этим весьма важным становится условие уменьшение сложности предвычислений (или отказ от них) при сохранении высокой криптостойкости преобразований. Таким образом, практически значимой является разработка скоростных шифров нового поколения, базирующихся на новых способах генерации динамических ключей, допускающих как эффективную аппаратную реализацию, так и сохраняющих высокую скорость шифрования при частой смене ключей.

В полной мере это относится и к разработкам систем LWC, для которых технология динамически изменяющихся ключей принципиально должна базироваться на «минимальной математике» (в связи с ограниченными ресурсными возможностями). Также нужно иметь ввиду, что в силу специфики представления информации в цифровых устройствах наибольший интерес представляют блочные шифры, позволяющие кодировать информацию без изменения ее структурированности, то есть позволяющие шифровать информацию, которая предварительно структурирована в соответствии с каким-либо методом протокольной защиты. Именно таким требованиям и отвечают принципы работы кодировщика *HiSNeC*.

Здесь подчеркнем ключевые моменты его программной реализации. Пусть имеется два конечных множества $\boldsymbol{\Omega_1}$ и $\boldsymbol{\Omega_2}$, каждое из которых содержит $\boldsymbol{n}$ различных элементов.

Подстановкой $\sigma$ будем называть взаимно однозначное отображение $\Omega_1$ на $\Omega_2$. Например, если $\Omega_1 = (1,2,3)$, а $\Omega_2 = (7,11,9)$, то одна из 6-ти возможных подстановок будет иметь вид:

$$\sigma = \begin{pmatrix} 1, & 2, & 3 \\ 7, & 11, & 9 \end{pmatrix}.$$

Если количество элементов в каждом из множеств – $n$, то количество возможных подстановок равно факториалу $n$ (то есть каждому элементу множества $\Omega_1$ может соответствовать любой элемент из множества $\Omega_2$). В частном случае множества $\Omega_1$ и $\Omega_2$ могут совпадать. Взаимно однозначное отображение множества на себя будем называть ***перестановкой*** ($\pi$). Например, если $\Omega = (1,2,3)$, существует 6 (или $3!$) перестановок:

$$\pi_1 = \begin{pmatrix} 1, & 2, & 3 \\ 1, & 2, & 3 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 3, & 1 \end{pmatrix}, \quad \pi_3 = \begin{pmatrix} 1, & 2, & 3 \\ 3, & 1, & 2 \end{pmatrix},$$

$$\pi_4 = \begin{pmatrix} 1, & 2, & 3 \\ 1, & 3, & 2 \end{pmatrix}, \quad \pi_5 = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 1, & 3 \end{pmatrix}, \quad \pi_6 = \begin{pmatrix} 1, & 2, & 3 \\ 3, & 2, & 1 \end{pmatrix}.$$

Определим множество $\Omega$ как множество натуральных чисел $1,2,\ldots,n$. Латинский квадрат $L$ будем представлять как квадратную таблицу $n \times n$, в каждой строке и в каждом столбце которой любой элемент множества $\Omega$ встречается точно один раз. Выберем значение $n$ таким образом, чтобы $n = k^2$. Тогда латинский квадрат $L$ с размерами $n \times n$ можно разбить на $n$ смежных, непересекающихся квадратов размером $k \times k$. Потребуем дополнительно, чтобы в каждом малом квадрате $k \times k$ любой элемент множества $\Omega$ также встречается точно один раз (требования сетки Судоку [2]). Такой латинский квадрат назовем $S$-квадратом, малые квадраты которого имеют размер $k \times k$ и содержат $n = k^2$ элементов.

Пусть построен $S$-квадрат порядка $n = k^2$. Выберем один из малых квадратов и предположим, что он заполнен так, как изображено на рис. 1a. Такое расположение описывается перестановкой

$$\pi_1 = \begin{pmatrix} 1, 2, 3, 4, 5, & 6, & 7, & 8, & 9, 10, 11.\ 12, 13, 14, 15, 16 \\ 1, 2, 3, 4, 5, & 6, & 7, & 8, & 9, 10, 11.\ 12, 13, 14, 15, 16 \end{pmatrix}.$$

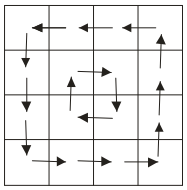
Если переставить элементы квадрата по алгоритму вихревого сдвига [2] так, как показано на рис. 1b, получим перестановку, изображенную на рис. 1c:

$$\pi_2 = \begin{pmatrix} 1, 2, 3, 4, 5, & 6, & 7, & 8, & 9, 10, 11.12, 13, 14, 15, 16 \\ 2, 3, 4, 8, 1, 10, & 6, & 12, & 5, & 11, 7, \ 16, \ \ 9, 13, 14, 15 \end{pmatrix}.$$

Отметим, что здесь применяются перестановки циклического типа, которые позволяют обеспечить существенно различные матричные трансформации.

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 |

a



b

| | | | |
|---|---|---|---|
| 2 | 3 | 4 | 8 |
| 1 | 10 | 6 | 12 |
| 5 | 11 | 7 | 16 |
| 9 | 13 | 14 | 15 |

c

***Рис. 1****. Пример перестановки элементов малого квадрата для* $k = 4$, $n = 16$.

На рис. 1b можно выделить две циклические перестановки: первая – продвижение против часовой стрелки приграничных клеток и продвижение по часовой стрелке центральных клеток таблицы. Сопоставление нижних строк перестановок $\pi_1$ и $\pi_2$ задает правила переобозначений чисел малого квадрата при выполнении перестановки $\pi_2$. Действительно 1 меняется на 2, 2 – на 3, …, 11 – на 7, …, 16 – на 15. Проведя одновременно такую же групповую замену чисел во всех малых квадратах, получим новую матричную форму большого S-квадрата.

Далее полагаем исходной нумерацию клеток малых квадратов матричной структуры в соответствии с рис. 1а. Тогда любую перестановку элементов малого квадрата можно описать вектором размерности 16. Условимся, что запись $\pi = (2,3,4,8.1,10,6,12,5,11,7,16,9,13,14,15)$, определяет следующие действия: элемент из клетки 1 переставляется в клетку 2, из клетки 2 – в клетку 3, …, из 6 – в 10, из 7 – в 6, … , из 16 – в 15. Таким образом, порядковый номер координаты вектора указывает, из какой клетки следует брать элемент для перестановки. Значение координаты вектора определяет, в какую клетку следует поместить выбранный элемент.

В анализируемом варианте работы кодировщика будем полагать, что ключи шифрования генерируются для 128-ми битной версии криптографического алгоритма AES (Advanced Encryption Standard). В связи с этим, выберем в качестве начального $S$-квадрата некоторый квадрат $S_0$ (n = 16). Набор операций перестановок определим посредством задания векторов перестановки размерностью 16. Назовем эти перестановки базисными. Количество таких векторов целесообразно выбрать равным степени 2. В проводимых авторами статистических экспериментах это количество $m$ выбиралось равным 32. Таблица операций ($T_{op}$) над $S$-квадратами будет иметь размер $n \times m$ (в этом случае моделирования использовалась таблица $16 \times 32$). В общем случае, получаемые в результате этих операций структурные компоненты (строки, столбцы или малые квадраты) матриц $S$-квадратов могут рассматриваться как генерации множеств новых ключей кодировки или их составляющих. Здесь важно подчеркнуть, что за один раунд коллективных перестановок реализуется возможность одновременной генерации не одного, а множества («связки») ключей шифрования. Причем эти генерации осуществляются без использования каких-либо дополнительных математических процедур. Более того, знание только последовательности (расписания) используемых операций $T_{op}$ исключает необходимость хранения таблиц $S$-квадратов после каждой выполненной операции в отличие от используемых сейчас многораундовых технологий генерации ключей. Перечисленные особенности способа генерации ключей, прежде всего, позволяют декларировать его существенные преимущества над прототипами в скорости реализации процессов кодирования и декодирования информационных потоков.

С целью «маскировки» передачи в открытом канале связи кодированных последовательностей (пусть и случайных) с постоянно используемыми натуральными числами (от 1 до 16) дополнительно формируются квадратные таблицы $R_0$ и $R_i$ размером $n^2$ каждая. Причем матрица $R_0$ должна быть сформирована предварительно с помощью генератора случайных чисел (с заданной равномерностью распределения) из диапазона 0…255. Для дальнейшего получения из $R_0$ матрицы $R_i$ будет использоваться та же таблица операций $T_{op}$, которые теперь будут определять конкретные перестановки мест ячеек этой матрицы вместе с содержащимися в них случайными числами.

Таким образом, в рассматриваемом варианте предлагаемый алгоритм генерации ключа объединяет следующую последовательность шагов:

1) вычисляются произведения $M_r$ матриц $R_0$ и $R_i$ (используются операции сложения и умножения по модулю 256);
2) вычисляются суммы $s_r$ элементов таблицы $M_r$ по модулю $m$;
3) используя $s_r$ в качестве указателя, из таблицы $T_{op}$ выбирается вектор перестановки;
4) выбранная операция перестановки выполняется над $S_0$-квадратом, в результате которой формируется новый $S_i$-квадрат;
5) по заданному правилу из $S_i$ выбирается либо строка (одна из 16 строк), либо столбец (один из 16 столбцов), либо малый квадрат (один из 16). Полученные 16 чисел образуют вектор перестановки. Отметим, что в модельной реализации авторами использовались только эти 48 вариантов, хотя нет причин и для использования других вариантов выборки;
6) для формирования выборки из матрицы $M_r$ строится вспомогательная функция $G(i,R)$, результатом которой является назначенная последовательность из 16 элементов матрицы $M_r$, которые и образуют текущий динамический ключ для алгоритма шифрования AES.

При оговоренных выше условиях, в соответствии с приведенным алгоритмом можно сформировать $48 \times 256 = 12288$ ключей шифрования. Далее может использоваться следующий за $s_r$ указатель на таблицу $T_{op}$, и повторение шагов 3…6. Это обеспечит генерацию очередного множества из $12288$ ключей. Таким образом, использование 32-х векторов перестановок, содержащихся в таблице $T_{op}$, обеспечивает генерацию множества из $48 \times 256 \times 32 = 393216$ существенно разных ключей шифрования, что позволяет зашифровать в рамках одного полного цикла 393216 блоков по 16 байт каждый (свыше 6 Мбайт информации). При необходимости далее следует переход к новой форме таблицы операций $T_{op}$. Для использования рассмотренного алгоритма следует «закрыть» в постоянной памяти контроллеров начальный $S_0$-квадрат и таблицы операций $T_{op}$. Таблица случайных чисел $R_0$ хранится в оперативной памяти процессоров и может при необходимости обновляться заново. Разумеется, матрицы $S_0$, $T_{op}$ и $R_0$ должны быть одинаковыми (заданными) для всей группы устройств, которые будут обмениваться кодированной информацией.

При практической реализации защиты канала передачи информации между двумя устройствами $T_t$ (передатчик) и $T_r$ (приемник) осуществляется следующая последовательность процедур: 1) передатчик $T_t$ обращается к приемнику $T_r$, передавая запрос на передачу; 2) при получении от $T_t$ разрешения на передачу $T_r$ генерирует таблицу случайных чисел $R_0$ и передает ее приемнику; 3) приемник и передатчик одновременно вычисляют матрицу $M_r$; 4) приемник и передатчик в соответствии с рассмотренным выше алгоритмом готовят синхронную генерацию одинаковых ключей: $T_t$ для кодирования, а $T_r$ для декодирования информационного потока. Подчеркнем, что при этом устройства различных групп (с различными $S_0$, $T_{op}$ $R_0$) не смогут обмениваться информацией. Тоже можно утверждать и о попытке несанкционированного доступа к сеансу связи, поскольку получение действующих ключей в реальный момент времени возможно только при использовании исходных $S_0$, $T_{op}$ и $R_0$. Эти параметры, в соответствии с вышеизложенным, являются недоступными не только гипотетическому “злоумышленнику”, но и пользователю устройства защиты канала связи.

## РЕЗУЛЬТАТЫ ПРОХОЖДЕНИЯ ТЕСТОВ NIST STS

Каждый из тестов в [4], предлагаемых NIST, получает на вход конечную исследуемую двоичную последовательность из знаков 0 и 1 (рекомендуемая длина последовательности 1000000 бит). Далее вычисляется статистика, характеризующая некое свойство данной последовательности. Это может быть и единичное значение, и множество значений. После чего эта статистика сравнивается с эталонной теоретической статистикой, которая характерна для идеально случайной последовательности.

В основе такого сопоставления лежит общий алгоритм сравнений статистических гипотез. При этом за нулевую гипотезу принимается предположение, что исследуемая последовательность является действительно случайной (знаки которой появляются равновероятно и независимо от друга). В каждом тесте вычисляется так называемое P-значение: это вероятность того, что исследуемый алгоритм генерации случайной последовательности создал последовательность не хуже, чем гипотетический истинный. Если P-значение = 1, то исследуемая последовательность идеально случайна, а если оно = 0, то последовательность полностью предсказуема. В дальнейшем P-значение сравнивается с α (уровнем статистической значимости), и если оно больше α, то нулевая гипотеза принимается и последовательность признается близкой к случайной. В противном случае — отбраковывается.

В тестах NIST STS фиксируется α = 0.01. Из этого следует, что:

- если P-значение ≥ 0.01, то последовательность признается случайной с уровнем доверительной вероятности 0.99;
- если P-значение < 0.01, то последовательность отбраковывается с 99%-ным уровнем надежности.

При прохождении тестов использовались кодовые последовательности, сгенерированные кодировщиком *HiSNeC*, длиной 1000000 битов (согласно рекомендациям NIST

STS). Статистические исследования были проведены для двух режимов использования кодировщика. В первом случае обеспечивался режим динамически изменяемых 128-ми битных ключей для стандартного шифратора Rijndael (AES) с минимальным количеством раундовых процедур *Nr*=10. Во втором кодовая последовательность формировалась потоком динамически изменяемых ключей генератора *HiSNeC*, хешированных с помощью известного алгоритма MD5 (для устранения постоянных групп данных, появляющихся в представлениях используемых чисел в двоичной системе счисления).

В первом случае в качестве исходной информации для кодирования использовалась электронная версия книги [5], которая содержит множество разноформатных материалов (текст, рисунки, диаграммы, таблицы и т.д.). Тест-контролю были подвержены 300 разных кодовых последовательностей, из которых 100% последовательностей успешно прошли все 15 предлагаемых тестов. На рис. 2, как типичные, представлены результаты одного из вариантов в проведенной серии тестирования для величин P-значений. Оригиналы протокольных отчетов прохождения тестов для этого варианта приведены в Приложении к статье. Следует указать, что в этом случае параллельно был проведен эксперимент по определению времени шифрования данных с использованием предложенного способа генерации ключей в совокупности с алгоритмом AES. Эксперимент показал несущественное (0.3%) увеличение затрат процессорного времени при использовании режима динамического изменения ключа (при шифровании каждого 16-байтового блока) по сравнению с использованием алгоритма AES с постоянным ключом. При этом относительное увеличение объема кодовых последовательностей составляло не более 3%. Такие результаты тестирования позволяют полагать, что технология динамически изменяемых ключей *HiSNeC* может быть успешно совмещена и с другими типами шифраторов LWC.

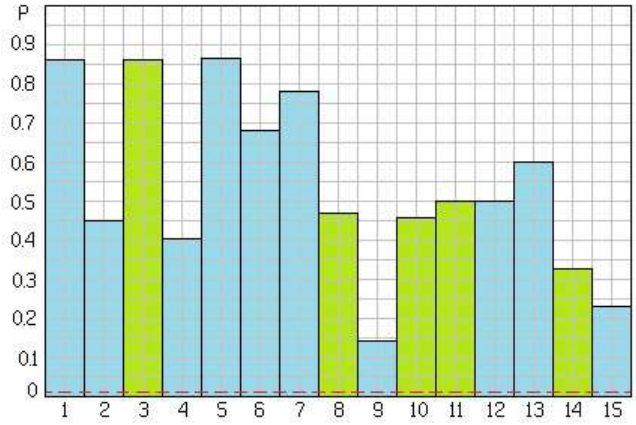



Рис. 2. *Диаграмма общих результатов тестирования*.

На рис. 2 натуральные числа, расположенные по горизонтальной оси, соответствуют номерам тестов: *1 - Approximate entropy test; 2 - Block frequency test; 3 - Cumulative sums (forward) test; 4 - FFT test; 5 - Frequency test; 6 - Linear complexity; 7 - Longest runs of ones test; 8 - Nonperiodic templates test; 9 - Overlapping template of all ones test; 10 - Random excursions test; 11 - Random excursions variant test; 12 - Rank test; 13 - Runs test; 14 - Serial test; 15 - Universal statistical test.* Голубым цветом показаны уровни единичных выходных значений вероятностей, а салатным (3,8,10,11,14) – среднее значение множества выходных P-значений.

Во втором случае из 100 исследованных кодовых последовательностей 96 успешно преодолели 11 тестов. Проблемные результаты наблюдались по тестам с номерами 10-11 и 14-15, связанных с анализом перекрывающихся шаблонов. Прежде всего, это свидетельствует, о неоптимальном порядке размещения ключей при формировании случайной последовательности. Однако, при условии дальнейшей доработки алгоритма (с целью минимизации этой уязвимости) автономное использование кодировщика на базе *HiSNeC* может быть вполне достаточным для многих практических приложений.

Таким образом статистические исследования подтвердили возможность успешного использования технологии *HiSNeC* в обеих случаях рассмотренных реализаций. Кроме того,

анализ тестированных последовательностей показал, что предложенная технология может обеспечивать режимы их генерации в соответствии с принципом шифра Г. Вернама по предварительно выбранному модулю цикличности.

## ВЫВОДЫ

В статье представлено описание нового алгоритма генерации ключей шифрования, реализованного в работе блочного кодировщика *HiSNeC*. На основании тестов NIST STS исследованы статистические свойства кодовых последовательностей кодировщика, полученных в режиме динамически изменяющихся входных ключей. Результаты тестирования подтвердили требуемую криптографическую стойкость кодировщика *HiSNeC*, что позволяет рекомендовать его ПО для использования в LWC системах.

Следует также уточнить, что предлагаемый кодировщик относится к программно-аппаратным средствам защиты. Совместно с декодировщиком его целесообразно на практике производить в виде пары структурно автономных микромодулей, для которых хранилищем секретного ключа является автономная (от сети) флэш-память микроконтроллеров. Для взлома этой памяти необходим физический захват самого контроллера с программным обеспечением, а также наличие сложного специального оборудования. Кроме того, даже после предполагаемого прочтения контента этой памяти нужна серьезная работа по криптоанализу снятой информации. То есть использование в *HiSNeC* автономных модулей на базе микроконтроллеров полностью снимает риск внутренних угроз сетевого типа. Для борьбы с атаками внешнего типа здесь использован принцип хранения не самих ключей, а только цепочка процедур их генерации из исходной матрицы. Такая информация о генерации ключей состоится из двух компонентов: один из которых храниться в постоянной флэш-памяти устройств защиты, а второй является изменяемым программным способом. Последнее позволяет при необходимости производить перенастройку системы защиты без изменения прошивки флэш-памяти микромодулей.

## СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Жуков А.Е. Легковесная криптография. Часть 1 / А.Е. Жуков // Вопросы кибербезопасности, 2015. - №1(9). – С. 26 – 43.
2. Penkin Yu., Khara G. Deterministic Chaos in Vibrations of Discrete Structures of Matrix Type / Yu. Penkin, G. Khara // Proc. Inter. Scien.-Pract. Conf. on Problems of Infocommunications Science and Technology (PIC S&T 2018), October 9-12, Kharkiv (Ukr.), 2018. – Vol. 2. – P. 548 – 552.
3. Патент РФ №2309549 от 27.10.2007 г. «Способ криптографического преобразования цифровых данных».
4. Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J., Vo S. A statistical test suite for random and pseudorandom number generators for cryptographic applications // NIST Spec. Publ. 2001. 800 - 22 revision 1a: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SPS00-22b.pdf.
5. Микробиология. Руководство к лабораторным занятиям: Учеб. пособие для студентов высш. учеб. заведений / Под ред. д.м.н., проф. И.Л. Дикого. – Х.: НФаУ: Золотые страницы,2002. – 444 с.

## ПРИЛОЖЕНИЕ. Оригиналы протокольных отчетов прохождения тестов

Листинги протоколов представлены в алфавитном порядке согласно названий тестов.

***Тест 1.***

```
          APPROXIMATE ENTROPY TEST
-----------------------------------------
COMPUTATIONAL INFORMATION:
-----------------------------------------
(a) m (block length)    = 10
(b) n (sequence length) = 1000000
(c) Chi^2               = 974.915528
(d) Phi(m)           = -6.931020
(e) Phi(m+1)         = -7.623679
(f) ApEn                = 0.692660
(g) Log(2)              = 0.693147
```

```
                -----------------------------------------
SUCCESS               p_value = 0.861628
```

***Комментарий.*** Тест приблизительной энтропии проверяет близость соотношения числа вхождений перекрывающихся шаблонов длины *t* и длины *t+1* ожидаемому для случайной последовательности.

***Тест 2.***

```
                BLOCK FREQUENCY TEST
                -----------------------------------------
                COMPUTATIONAL INFORMATION:
                -----------------------------------------
                (a) Chi^2           = 7827.000000
                (b) # of substrings = 7812
                (c) block length    = 128
                (d) Note: 64 bits were discarded.
                -----------------------------------------
SUCCESS               p_value = 0.450159
```

***Комментарий.*** Частотный блочный тест делит исследуемую последовательность на блоки одинаковой длины и проверяет равномерность распределения числа единиц в этих блоках.

***Тест 3.***

```
              CUMULATIVE SUMS (FORWARD) TEST
              -----------------------------------------
              COMPUTATIONAL INFORMATION:
              -----------------------------------------
              (a) The maximum partial sum = 737
              -----------------------------------------
SUCCESS             p_value = 0.868630

             CUMULATIVE SUMS (REVERSE) TEST
              -----------------------------------------
              COMPUTATIONAL INFORMATION:
              -----------------------------------------
              (a) The maximum partial sum = 760
              -----------------------------------------
SUCCESS             p_value = 0.849583
```

***Комментарий.*** Тест кумулятивных сумм. Биты исследуемой последовательности трактуются как целые числа, причем все нули заменяются на -1. Далее вычисляются суммы первых *t* членов последовательности. Тест проверяет соответствие значения максимальной по абсолютной величине суммы ожидаемому.

***Тест 4.***

```
                FFT TEST
              -----------------------------------------
              COMPUTATIONAL INFORMATION:
              -----------------------------------------
              (a) Percentile = 94.981800
              (b) N_l        = 474909.000000
              (c) N_o        = 475000.000000
              (d) d          = -0.835073
              -----------------------------------------
SUCCESS             p_value = 0.403676
```

***Комментарий.*** В тесте дискретного преобразования Фурье (еще имеет название Spectral Text) биты исследуемой последовательности рассматриваются как вещественные числа при условии замены каждого нуля на -1. От полученной последовательности вычисляется дискретное преобразование Фурье. Далее проверяется близость числа спектральных компонент, амплитуда которых превышает 95% к ожидаемому для случайной последовательности.

***Тест 5.***

```
                FREQUENCY TEST
              -----------------------------------------
              COMPUTATIONAL INFORMATION:
```

```
               -----------------------------------------
               (a) The nth partial sum = 170
               (b) S_n/n               = 0.000170
               -----------------------------------------
SUCCESS              p_value = 0.865010
```

***Комментарий.*** Частотный побитовый тест (Frequency Monobit Text) проверяет, что в исследуемой последовательности число единиц приблизительно равно числу нулей.

***Тест 6.***

```
                    LINEAR COMPLEXITY
               -----------------------------------------
               M (substring length)     = 500
               N (number of substrings) = 2000
               -----------------------------------------
                     FREQUENCY
               -----------------------------------------
                 C0   C1   C2   C3   C4   C5   C6    CHI2    P-value
               -----------------------------------------
               Note: 0 bits were discarded!
                 16   56  269  987  510  119   43  3.985116 0.678691
```

***Комментарий.*** Тест проверяет исследуемую последовательность на линейную сложность. Линейной сложностью последовательности называется наименьшая длина регистра сдвига с линейной обратной связью, ее порождающего. Исследуемая последовательность разделяется на подпоследовательности определенной длины. Для каждой из них вычисляется линейная сложность с помощью алгоритма Берлекэмпа - Месси. Тест проверяет соответствие распределения линейной сложности этих подпоследовательностей и ожидаемого.

***Тест 7.***

```
                  LONGEST RUNS OF ONES TEST
               -----------------------------------------
               COMPUTATIONAL INFORMATION:
               -----------------------------------------
               (a) N (# of substrings)  = 100
               (b) M (Substring Length) = 10000
               (c) Chi^2                = 3.270145
               -----------------------------------------
                      FREQUENCY
               -----------------------------------------
               <=10  11  12  13  14  15 >=16 P-value  Assignment
                  6  24  22  24  12   5    7 SUCCESS   p_value = 0.774256
```

***Комментарий.*** Тест на самую длинную последовательность единиц в блоке разбивает исследуемую последовательность на блоки фиксированной длины и проверяет соответствие распределения максимальных длин непрерывных последовательностей из единиц внутри блоков ожидаемому для случайной последовательности.

***Тест 8.***

```
                  NONPERIODIC TEMPLATES TEST
               -----------------------------------------
                 COMPUTATIONAL INFORMATION
               -------------------------------------------------
       LAMBDA = 244.125000 M = 125000    N = 8  m = 9  n = 1000000
               -------------------------------------------------
               FREQUENCY
Template   W_1  W_2  W_3  W_4  W_5  W_6  W_7  W_8    Chi^2   P_value Assignment
Index
-------------------------------------------------------------------------------------
--
000000001  258  238  260  241  218  261  242  252  6.463571 0.595451 SUCCESS   0
000000011  246  241  281  246  236  253  226  261  9.043703 0.338623 SUCCESS   1
000000101  240  244  240  227  239  258  273  238  6.004951 0.646677 SUCCESS   2
000000111  245  214  275  242  244  243  237  238  8.285339 0.406105 SUCCESS   3
000001001  246  263  232  246  213  281  262  250 13.527160 0.094953 SUCCESS   4
000001011  230  246  244  238  237  243  271  214  8.144470 0.419487 SUCCESS   5
```

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 000001101 | 260 | 241 | 244 | 267 | 242 | 238 | 275 | 226 | 8.934609 | 0.347842 | SUCCESS | 6 |
| 000001111 | 246 | 250 | 245 | 239 | 216 | 251 | 231 | 253 | 4.890707 | 0.769191 | SUCCESS | 7 |
| 000010001 | 259 | 212 | 224 | 260 | 267 | 237 | 249 | 214 | 14.470878 | 0.070288 | SUCCESS | 8 |
| 000010011 | 251 | 228 | 217 | 243 | 229 | 261 | 231 | 252 | 7.592643 | 0.474238 | SUCCESS | 9 |
| 000010101 | 244 | 252 | 273 | 233 | 255 | 251 | 247 | 252 | 5.318610 | 0.723043 | SUCCESS | 10 |
| 000010111 | 240 | 245 | 251 | 251 | 261 | 223 | 235 | 232 | 4.548596 | 0.804552 | SUCCESS | 11 |
| 000011001 | 232 | 255 | 265 | 234 | 230 | 236 | 260 | 267 | 7.814010 | 0.451846 | SUCCESS | 12 |
| 000011011 | 216 | 255 | 245 | 247 | 229 | 224 | 242 | 213 | 10.699182 | 0.219333 | SUCCESS | 13 |
| 000011101 | 262 | 231 | 260 | 237 | 267 | 246 | 266 | 235 | 7.978181 | 0.435604 | SUCCESS | 14 |
| 000011111 | 260 | 248 | 252 | 223 | 218 | 247 | 231 | 243 | 6.946551 | 0.542410 | SUCCESS | 15 |
| 000100011 | 245 | 215 | 208 | 247 | 259 | 226 | 228 | 227 | 13.834319 | 0.086187 | SUCCESS | 16 |
| 000100101 | 235 | 224 | 218 | 236 | 238 | 253 | 247 | 221 | 8.033257 | 0.430228 | SUCCESS | 17 |
| 000100111 | 238 | 241 | 237 | 241 | 234 | 260 | 232 | 241 | 2.623029 | 0.955747 | SUCCESS | 18 |
| 000101001 | 230 | 264 | 260 | 208 | 262 | 265 | 226 | 255 | 14.208205 | 0.076497 | SUCCESS | 19 |
| 000101011 | 250 | 240 | 248 | 226 | 230 | 248 | 263 | 265 | 5.938224 | 0.654152 | SUCCESS | 20 |
| 000101101 | 255 | 234 | 249 | 254 | 230 | 257 | 276 | 231 | 8.031139 | 0.430434 | SUCCESS | 21 |
| 000101111 | 216 | 251 | 258 | 272 | 255 | 239 | 219 | 223 | 12.836583 | 0.117597 | SUCCESS | 22 |
| 000110011 | 231 | 258 | 259 | 247 | 230 | 247 | 241 | 265 | 5.285776 | 0.726641 | SUCCESS | 23 |
| 000110101 | 251 | 241 | 224 | 255 | 270 | 221 | 257 | 226 | 9.654843 | 0.290092 | SUCCESS | 24 |
| 000110111 | 237 | 265 | 265 | 253 | 224 | 218 | 219 | 245 | 11.526392 | 0.173619 | SUCCESS | 25 |
| 000111001 | 241 | 251 | 252 | 248 | 231 | 248 | 244 | 240 | 1.433583 | 0.993757 | SUCCESS | 26 |
| 000111011 | 250 | 225 | 254 | 239 | 274 | 251 | 270 | 241 | 9.079715 | 0.335616 | SUCCESS | 27 |
| 000111101 | 263 | 240 | 254 | 224 | 256 | 230 | 263 | 240 | 6.734718 | 0.565506 | SUCCESS | 28 |
| 000111111 | 234 | 224 | 221 | 233 | 251 | 231 | 246 | 241 | 5.926573 | 0.655457 | SUCCESS | 29 |
| 001000011 | 253 | 258 | 234 | 236 | 238 | 234 | 282 | 221 | 10.799803 | 0.213303 | SUCCESS | 30 |
| 001000101 | 251 | 237 | 269 | 265 | 271 | 227 | 233 | 203 | 16.875189 | 0.031435 | SUCCESS | 31 |
| 001000111 | 264 | 203 | 236 | 245 | 234 | 258 | 220 | 227 | 14.080046 | 0.079703 | SUCCESS | 32 |
| 001001011 | 231 | 227 | 227 | 244 | 236 | 245 | 242 | 272 | 6.808859 | 0.557389 | SUCCESS | 33 |
| 001001101 | 268 | 226 | 216 | 259 | 255 | 243 | 242 | 226 | 10.012842 | 0.264126 | SUCCESS | 34 |
| 001001111 | 230 | 232 | 249 | 236 | 239 | 250 | 257 | 251 | 3.008566 | 0.933819 | SUCCESS | 35 |
| 001010011 | 260 | 254 | 254 | 260 | 267 | 240 | 228 | 258 | 7.167917 | 0.518629 | SUCCESS | 36 |
| 001010101 | 208 | 278 | 241 | 218 | 228 | 261 | 227 | 229 | 17.843268 | 0.022433 | SUCCESS | 37 |
| 001010111 | 269 | 257 | 246 | 237 | 234 | 257 | 248 | 246 | 4.768902 | 0.781966 | SUCCESS | 38 |
| 001011011 | 240 | 250 | 231 | 247 | 241 | 255 | 261 | 241 | 2.773431 | 0.947762 | SUCCESS | 39 |
| 001011101 | 253 | 246 | 215 | 242 | 264 | 228 | 245 | 278 | 11.601593 | 0.169884 | SUCCESS | 40 |
| 001011111 | 238 | 227 | 232 | 257 | 219 | 256 | 221 | 226 | 9.655902 | 0.290012 | SUCCESS | 41 |
| 001100101 | 218 | 252 | 248 | 268 | 247 | 237 | 245 | 248 | 5.949874 | 0.652847 | SUCCESS | 42 |
| 001100111 | 235 | 258 | 225 | 248 | 224 | 243 | 245 | 255 | 5.007215 | 0.756805 | SUCCESS | 43 |
| 001101011 | 251 | 266 | 213 | 239 | 262 | 226 | 266 | 249 | 11.316677 | 0.184393 | SUCCESS | 44 |
| 001101101 | 213 | 260 | 245 | 248 | 246 | 246 | 239 | 216 | 8.731249 | 0.365472 | SUCCESS | 45 |
| 001101111 | 237 | 256 | 255 | 250 | 279 | 237 | 230 | 243 | 7.678436 | 0.465495 | SUCCESS | 46 |
| 001110101 | 272 | 226 | 253 | 241 | 260 | 227 | 245 | 265 | 9.218466 | 0.324203 | SUCCESS | 47 |
| 001110111 | 258 | 235 | 231 | 241 | 270 | 244 | 232 | 245 | 5.402285 | 0.713840 | SUCCESS | 48 |
| 001111011 | 256 | 251 | 243 | 238 | 240 | 237 | 254 | 260 | 2.730005 | 0.950143 | SUCCESS | 49 |
| 001111101 | 230 | 243 | 247 | 246 | 241 | 280 | 263 | 236 | 8.183659 | 0.415739 | SUCCESS | 50 |
| 001111111 | 238 | 245 | 230 | 232 | 241 | 246 | 228 | 227 | 4.030663 | 0.854346 | SUCCESS | 51 |
| 010000011 | 258 | 232 | 264 | 261 | 242 | 250 | 238 | 250 | 4.789027 | 0.779869 | SUCCESS | 52 |
| 010000111 | 280 | 253 | 247 | 230 | 240 | 222 | 271 | 222 | 13.946590 | 0.083168 | SUCCESS | 53 |
| 010001011 | 251 | 246 | 250 | 258 | 254 | 223 | 220 | 223 | 7.837311 | 0.449521 | SUCCESS | 54 |
| 010001111 | 237 | 229 | 254 | 258 | 257 | 256 | 248 | 223 | 5.667077 | 0.684467 | SUCCESS | 55 |
| 010010011 | 241 | 247 | 222 | 245 | 251 | 254 | 261 | 232 | 4.596258 | 0.799727 | SUCCESS | 56 |
| 010010111 | 236 | 222 | 235 | 250 | 256 | 280 | 246 | 264 | 10.591147 | 0.225958 | SUCCESS | 57 |
| 010011011 | 248 | 228 | 233 | 256 | 290 | 254 | 225 | 237 | 13.380995 | 0.099396 | SUCCESS | 58 |
| 010011111 | 230 | 245 | 235 | 246 | 238 | 238 | 250 | 214 | 5.525148 | 0.700252 | SUCCESS | 59 |
| 010100011 | 240 | 253 | 239 | 252 | 276 | 242 | 243 | 223 | 6.999510 | 0.536686 | SUCCESS | 60 |
| 010100111 | 259 | 236 | 243 | 255 | 254 | 226 | 237 | 229 | 4.712767 | 0.787788 | SUCCESS | 61 |
| 010101011 | 243 | 243 | 234 | 222 | 245 | 253 | 247 | 220 | 5.356741 | 0.718855 | SUCCESS | 62 |
| 010101111 | 264 | 266 | 239 | 229 | 226 | 231 | 253 | 230 | 8.081979 | 0.425503 | SUCCESS | 63 |
| 010110011 | 241 | 256 | 248 | 255 | 255 | 234 | 250 | 265 | 4.131284 | 0.845089 | SUCCESS | 64 |
| 010110111 | 222 | 235 | 249 | 243 | 243 | 266 | 254 | 273 | 8.510942 | 0.385214 | SUCCESS | 65 |
| 010111011 | 269 | 260 | 234 | 239 | 268 | 226 | 261 | 286 | 16.677125 | 0.033652 | SUCCESS | 66 |
| 010111111 | 258 | 226 | 223 | 249 | 235 | 263 | 258 | 232 | 7.499437 | 0.483826 | SUCCESS | 67 |
| 011000111 | 249 | 243 | 232 | 236 | 226 | 255 | 260 | 257 | 4.671459 | 0.792044 | SUCCESS | 68 |
| 011001111 | 214 | 249 | 240 | 243 | 236 | 236 | 249 | 242 | 4.702175 | 0.788882 | SUCCESS | 69 |
| 011010111 | 243 | 261 | 240 | 244 | 262 | 243 | 253 | 256 | 3.574161 | 0.893358 | SUCCESS | 70 |
| 011011111 | 235 | 242 | 234 | 268 | 273 | 238 | 228 | 260 | 9.081833 | 0.335440 | SUCCESS | 71 |
| 011101111 | 243 | 239 | 230 | 239 | 279 | 221 | 235 | 273 | 12.376904 | 0.135163 | SUCCESS | 72 |
| 011111111 | 257 | 225 | 234 | 247 | 257 | 240 | 235 | 227 | 5.090889 | 0.747819 | SUCCESS | 73 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 100000000 | 258 | 238 | 260 | 241 | 218 | 261 | 242 | 252 | 6.463571 | 0.595451 | SUCCESS 74 |
| 100010000 | 241 | 238 | 231 | 227 | 238 | 261 | 251 | 191 | 15.695276 | 0.046955 | SUCCESS 75 |
| 100100000 | 246 | 216 | 281 | 255 | 225 | 278 | 275 | 243 | 20.083408 | 0.010025 | SUCCESS 76 |
| 100101000 | 246 | 234 | 259 | 229 | 228 | 242 | 230 | 243 | 4.327230 | 0.826459 | SUCCESS 77 |
| 100110000 | 228 | 232 | 247 | 249 | 253 | 232 | 250 | 239 | 3.074234 | 0.929613 | SUCCESS 78 |
| 100111000 | 264 | 238 | 237 | 224 | 245 | 266 | 244 | 235 | 6.146880 | 0.630783 | SUCCESS 79 |
| 101000000 | 270 | 226 | 258 | 258 | 239 | 264 | 229 | 267 | 10.830519 | 0.211488 | SUCCESS 80 |
| 101000100 | 243 | 231 | 210 | 243 | 252 | 276 | 248 | 225 | 11.854734 | 0.157804 | SUCCESS 81 |
| 101001000 | 249 | 236 | 280 | 252 | 241 | 219 | 222 | 236 | 11.165216 | 0.192512 | SUCCESS 82 |
| 101001100 | 228 | 253 | 239 | 229 | 238 | 239 | 260 | 216 | 7.204988 | 0.514686 | SUCCESS 83 |
| 101010000 | 249 | 233 | 242 | 257 | 257 | 223 | 217 | 249 | 7.157326 | 0.519758 | SUCCESS 84 |
| 101010100 | 232 | 249 | 243 | 252 | 243 | 242 | 255 | 241 | 1.558565 | 0.991692 | SUCCESS 85 |
| 101011000 | 221 | 254 | 222 | 234 | 228 | 241 | 254 | 235 | 7.095894 | 0.526323 | SUCCESS 86 |
| 101011100 | 241 | 245 | 252 | 237 | 256 | 277 | 266 | 246 | 7.740927 | 0.459178 | SUCCESS 87 |
| 101100000 | 239 | 239 | 245 | 214 | 216 | 247 | 238 | 242 | 7.635010 | 0.469910 | SUCCESS 88 |
| 101100100 | 253 | 218 | 254 | 249 | 254 | 226 | 252 | 232 | 6.429677 | 0.599218 | SUCCESS 89 |
| 101101000 | 239 | 262 | 233 | 259 | 250 | 243 | 267 | 227 | 6.537712 | 0.587228 | SUCCESS 90 |
| 101101100 | 244 | 222 | 245 | 251 | 230 | 231 | 239 | 245 | 3.967113 | 0.860078 | SUCCESS 91 |
| 101110000 | 235 | 260 | 256 | 245 | 242 | 262 | 291 | 226 | 14.094874 | 0.079326 | SUCCESS 92 |
| 101110100 | 254 | 262 | 237 | 240 | 252 | 258 | 225 | 274 | 8.463279 | 0.389571 | SUCCESS 93 |
| 101111000 | 242 | 263 | 256 | 254 | 263 | 222 | 252 | 253 | 6.718830 | 0.567250 | SUCCESS 94 |
| 101111100 | 242 | 244 | 229 | 249 | 251 | 237 | 250 | 262 | 3.004329 | 0.934086 | SUCCESS 95 |
| 110000000 | 246 | 247 | 251 | 227 | 218 | 249 | 265 | 252 | 6.593848 | 0.581018 | SUCCESS 96 |
| 110000010 | 235 | 259 | 230 | 258 | 236 | 228 | 248 | 224 | 6.111927 | 0.634696 | SUCCESS 97 |
| 110000100 | 227 | 229 | 222 | 224 | 248 | 235 | 271 | 234 | 9.912221 | 0.271241 | SUCCESS 98 |
| 110001000 | 233 | 242 | 233 | 230 | 268 | 229 | 226 | 225 | 8.238736 | 0.410504 | SUCCESS 99 |
| 110001010 | 240 | 266 | 230 | 241 | 212 | 242 | 239 | 267 | 9.705683 | 0.286294 | SUCCESS 100 |
| 110010000 | 260 | 244 | 275 | 261 | 247 | 258 | 270 | 236 | 10.279752 | 0.245937 | SUCCESS 101 |
| 110010010 | 226 | 249 | 244 | 242 | 240 | 231 | 253 | 277 | 7.226171 | 0.512439 | SUCCESS 102 |
| 110010100 | 220 | 238 | 260 | 247 | 247 | 237 | 243 | 237 | 4.198011 | 0.838831 | SUCCESS 103 |
| 110011000 | 227 | 238 | 258 | 259 | 223 | 219 | 234 | 259 | 9.091366 | 0.334647 | SUCCESS 104 |
| 110011010 | 249 | 256 | 251 | 245 | 237 | 234 | 254 | 268 | 4.379129 | 0.821401 | SUCCESS 105 |
| 110100000 | 255 | 250 | 254 | 243 | 233 | 281 | 249 | 256 | 8.049145 | 0.428684 | SUCCESS 106 |
| 110100010 | 235 | 240 | 231 | 252 | 274 | 256 | 244 | 234 | 6.230554 | 0.621424 | SUCCESS 107 |
| 110100100 | 249 | 242 | 246 | 261 | 249 | 238 | 247 | 251 | 1.836067 | 0.985632 | SUCCESS 108 |
| 110101000 | 259 | 231 | 236 | 244 | 275 | 227 | 232 | 235 | 8.203783 | 0.413822 | SUCCESS 109 |
| 110101010 | 267 | 214 | 236 | 256 | 260 | 234 | 275 | 232 | 13.102434 | 0.108373 | SUCCESS 110 |
| 110101100 | 207 | 250 | 246 | 261 | 260 | 250 | 254 | 250 | 8.980153 | 0.343973 | SUCCESS 111 |
| 110110000 | 248 | 249 | 252 | 233 | 229 | 262 | 230 | 255 | 4.620619 | 0.797248 | SUCCESS 112 |
| 110110010 | 273 | 230 | 268 | 246 | 229 | 242 | 248 | 224 | 9.575405 | 0.296100 | SUCCESS 113 |
| 110110100 | 247 | 282 | 218 | 238 | 230 | 254 | 275 | 231 | 15.190053 | 0.055554 | SUCCESS 114 |
| 110111000 | 241 | 253 | 259 | 245 | 266 | 252 | 264 | 217 | 8.396552 | 0.395723 | SUCCESS 115 |
| 110111010 | 265 | 255 | 239 | 228 | 232 | 243 | 238 | 274 | 8.128582 | 0.421012 | SUCCESS 116 |
| 110111100 | 250 | 251 | 218 | 241 | 255 | 216 | 253 | 257 | 8.167772 | 0.417256 | SUCCESS 117 |
| 111000000 | 243 | 254 | 251 | 246 | 237 | 244 | 302 | 233 | 15.563939 | 0.049064 | SUCCESS 118 |
| 111000010 | 249 | 248 | 231 | 220 | 269 | 226 | 255 | 242 | 7.893447 | 0.443947 | SUCCESS 119 |
| 111000100 | 232 | 209 | 256 | 255 | 245 | 238 | 214 | 219 | 13.629899 | 0.091937 | SUCCESS 120 |
| 111000110 | 242 | 251 | 270 | 248 | 240 | 267 | 211 | 261 | 11.263719 | 0.187200 | SUCCESS 121 |
| 111001000 | 271 | 243 | 270 | 265 | 225 | 263 | 250 | 224 | 12.669234 | 0.123748 | SUCCESS 122 |
| 111001010 | 237 | 258 | 228 | 235 | 276 | 254 | 243 | 228 | 8.309700 | 0.403817 | SUCCESS 123 |
| 111001100 | 217 | 240 | 212 | 264 | 226 | 255 | 257 | 265 | 13.676503 | 0.090597 | SUCCESS 124 |
| 111010000 | 253 | 261 | 258 | 232 | 235 | 243 | 230 | 259 | 5.119487 | 0.744732 | SUCCESS 125 |
| 111010010 | 238 | 240 | 234 | 264 | 256 | 255 | 223 | 245 | 5.331321 | 0.721648 | SUCCESS 126 |
| 111010100 | 255 | 213 | 249 | 213 | 258 | 226 | 228 | 266 | 14.146773 | 0.078019 | SUCCESS 127 |
| 111010110 | 207 | 267 | 248 | 266 | 233 | 250 | 231 | 238 | 11.706451 | 0.164790 | SUCCESS 128 |
| 111011000 | 270 | 256 | 255 | 234 | 225 | 239 | 239 | 261 | 7.347976 | 0.499596 | SUCCESS 129 |
| 111011010 | 263 | 248 | 222 | 229 | 245 | 253 | 244 | 243 | 4.958493 | 0.762003 | SUCCESS 130 |
| 111011100 | 260 | 254 | 276 | 240 | 276 | 235 | 267 | 227 | 13.974129 | 0.082442 | SUCCESS 131 |
| 111100000 | 226 | 244 | 219 | 259 | 254 | 223 | 268 | 223 | 11.613244 | 0.169312 | SUCCESS 132 |
| 111100010 | 248 | 234 | 246 | 259 | 237 | 241 | 236 | 243 | 1.991765 | 0.981263 | SUCCESS 133 |
| 111100100 | 257 | 265 | 247 | 244 | 229 | 258 | 251 | 222 | 6.642570 | 0.575641 | SUCCESS 134 |
| 111100110 | 242 | 241 | 232 | 279 | 223 | 235 | 239 | 261 | 9.397465 | 0.309883 | SUCCESS 135 |
| 111101000 | 232 | 262 | 248 | 249 | 273 | 262 | 233 | 247 | 7.586288 | 0.474888 | SUCCESS 136 |
| 111101010 | 239 | 210 | 252 | 246 | 240 | 234 | 242 | 241 | 5.889502 | 0.659608 | SUCCESS 137 |
| 111101100 | 264 | 231 | 275 | 226 | 234 | 254 | 236 | 236 | 9.240708 | 0.322399 | SUCCESS 138 |
| 111101110 | 254 | 274 | 261 | 212 | 255 | 237 | 226 | 258 | 12.696773 | 0.122717 | SUCCESS 139 |
| 111110000 | 237 | 217 | 214 | 235 | 252 | 237 | 252 | 233 | 8.794799 | 0.359901 | SUCCESS 140 |
| 111110010 | 247 | 247 | 242 | 221 | 250 | 235 | 255 | 237 | 3.569925 | 0.893696 | SUCCESS 141 |

```
111110100  208  234  243  272  253  266  249  227 12.964742 0.113069 SUCCESS 142
111110110  256  229  230  249  232  278  246  231  8.741840 0.364540 SUCCESS 143
111111000  240  229  233  239  250  248  244  259  2.824271 0.944897 SUCCESS 144
111111010  222  221  240  279  253  246  253  230 11.092133 0.196533 SUCCESS 145
111111100  256  248  219  243  267  255  237  258  7.089539 0.527004 SUCCESS 146
111111110  257  225  234  247  257  240  235  227  5.090889 0.747819 SUCCESS 147
```

***Комментарий.*** Тест на совпадение неперекрывающихся шаблонов. Проверяется соответствие числа повторений некоторой фиксированной подпоследовательности (ее называют шаблоном) в исследуемой последовательности ожидаемому. При этом для поиска шаблона длины *t* применяется скользящее окно: если шаблон не обнаружен, то окно сдвигается на одну позицию, а если обнаружен - на *t* позиций.

***Тест 9.***

```
     OVERLAPPING TEMPLATE OF ALL ONES TEST
---------------------------------------------
COMPUTATIONAL INFORMATION:
---------------------------------------------
(a) n (sequence_length)      = 1000000
(b) m (block length of 1s)   = 9
(c) M (length of substring)  = 1032
(d) N (number of substrings) = 968
(e) lambda [(M-m+1)/2^m]     = 2.000000
(f) eta                      = 1.000000
---------------------------------------------
   FREQUENCY
  0   1   2   3   4 >=5   Chi^2   P-value  Assignment
---------------------------------------------
363 205 126  82  58 134  8.224142 0.144308 SUCCESS
```

***Комментарий.*** Тест на совпадение перекрывающихся шаблонов. Аналогичен тесту на совпадение неперекрывающихся шаблонов, за исключением того, что окно всегда сдвигается на одну позицию.

***Тест 10.***

```
            RANDOM EXCURSIONS TEST
-----------------------------------------
COMPUTATIONAL INFORMATION:
-----------------------------------------
(a) Number Of Cycles (J) = 1113
(b) Sequence Length (n)  = 1000000
(c) Rejection Constraint = 500.000000
-----------------------------------------
SUCCESS             x = -4 chi^2 =  7.503211 p_value = 0.185824
SUCCESS             x = -3 chi^2 =  3.402113 p_value = 0.638248
SUCCESS             x = -2 chi^2 =  6.049749 p_value = 0.301408
SUCCESS             x = -1 chi^2 =  5.398922 p_value = 0.369157
SUCCESS             x =  1 chi^2 =  2.525606 p_value = 0.772634
SUCCESS             x =  2 chi^2 =  2.581156 p_value = 0.764226
SUCCESS             x =  3 chi^2 =  8.989443 p_value = 0.109486
SUCCESS             x =  4 chi^2 =  1.801423 p_value = 0.875883
```

***Комментарий.*** В тесте на произвольные отклонения биты исследуемой последовательности трактуются как целые числа, причем все нули заменяются на -1. Далее полагается $S_t$ – сумма первых *t* членов последовательности для $t=1,2,...n$. Множество всех различных значений $S_t$ рассматривается как множество вершин графа, а последовательность значений $S_t$ как блуждание по этому графу. Тестом оценивается соответствие распределения количества циклов в этой последовательности (под циклом в тесте понимается последовательность вершин, начинающаяся и заканчивающаяся нулем), в которых присутствуют определенные вершины определенное число раз к ожидаемому.

***Тест 11.***

```
       RANDOM EXCURSIONS VARIANT TEST
-----------------------------------------
COMPUTATIONAL INFORMATION:
```

```
                -----------------------------------------
                (a) Number Of Cycles (J) = 1113
                (b) Sequence Length (n)  = 1000000
                -----------------------------------------
SUCCESS               (x = -9) Total visits = 1326; p-value = 0.273540
SUCCESS               (x = -8) Total visits = 1323; p-value = 0.250457
SUCCESS               (x = -7) Total visits = 1262; p-value = 0.381087
SUCCESS               (x = -6) Total visits = 1224; p-value = 0.478104
SUCCESS               (x = -5) Total visits = 1147; p-value = 0.810166
SUCCESS               (x = -4) Total visits = 1082; p-value = 0.803870
SUCCESS               (x = -3) Total visits = 1098; p-value = 0.886936
SUCCESS               (x = -2) Total visits = 1121; p-value = 0.922015
SUCCESS               (x = -1) Total visits = 1103; p-value = 0.832145
SUCCESS               (x =  1) Total visits = 1100; p-value = 0.782903
SUCCESS               (x =  2) Total visits = 1035; p-value = 0.339836
SUCCESS               (x =  3) Total visits =  989; p-value = 0.239847
SUCCESS               (x =  4) Total visits = 1008; p-value = 0.400259
SUCCESS               (x =  5) Total visits =  995; p-value = 0.404463
SUCCESS               (x =  6) Total visits =  864; p-value = 0.111552
SUCCESS               (x =  7) Total visits =  784; p-value = 0.053110
SUCCESS               (x =  8) Total visits =  763; p-value = 0.055441
SUCCESS               (x =  9) Total visits =  866; p-value = 0.204182
```

***Комментарий.*** Вариант теста на произвольные отклонения, где рассматривается тот же граф, что и в предыдущем тесте, однако проверяется соответствие распределения числа проходов блуждания через каждую вершину и ожидаемого.

***Тест 12.***

```
                                RANK TEST
                -----------------------------------------
                COMPUTATIONAL INFORMATION:
                -----------------------------------------
                (a) Probability P_32 = 0.288788
                (b)             P_31 = 0.577576
                (c)             P_30 = 0.133636
                (d) Frequency   F_32 = 284
                (e)             F_31 = 574
                (f)             F_30 = 118
                (g) # of matrices    = 976
                (h) Chi^2            = 1.388266
                (i) NOTE: 576 BITS WERE DISCARDED.
                -----------------------------------------
SUCCESS               p_value = 0.499507
```

***Комментарий.*** Тест рангов бинарных матриц (Binary Matrix Rank Test). Исследуемая последовательность разбивается на подпоследовательности некоторой длины, из которых составляется двоичная матрица. Тест проверяет соответствие количеств матриц максимального ранга и матриц ранга на единицу меньше максимального ожидаемым для случайной последовательности.

***Тест 13.***

```
                                RUNS TEST
                -----------------------------------------
                COMPUTATIONAL INFORMATION:
                -----------------------------------------
                (a) Pi                          = 0.500085
                (b) V_n_obs (Total # of runs)   = 499739
                (c) V_n_obs - 2 n pi (1-pi)
                    ----------------------      = 0.369089
                      2 sqrt(2n) pi (1-pi)
                -----------------------------------------
SUCCESS               p_value = 0.601690
```

***Комментарий.*** Тест на последовательность одинаковых битов. Анализирует отклонения числа непрерывных серий от ожидаемого для случайной последовательности (под непрерывной

серией длины *t* понимается последовательность из *t* единиц, ограниченная нулями, либо последовательность из *t* нулей, ограниченная единицами).

***Тест 14.***

```
                    SERIAL TEST
              ----------------------------------------------
               COMPUTATIONAL INFORMATION:
              ----------------------------------------------
              (a) Block length    (m) = 16
              (b) Sequence length (n) = 1000000
              (c) Psi_m               = 65807.249408
              (d) Psi_m-1             = 32810.201088
              (e) Psi_m-2             = 16211.177472
              (f) Del_1               = 32997.048320
              (g) Del_2               = 16398.024704
              ----------------------------------------------
SUCCESS             p_value1 = 0.185328
SUCCESS             p_value2 = 0.467667
```

***Комментарий.*** Тест на подпоследовательности определяет, соответствует ли ожидаемому количество вхождений каждого из $2^t$ шаблонов длины *t* (в случайной последовательности такие шаблоны равновероятны).

***Тест 15.***

```
                UNIVERSAL STATISTICAL TEST
              ---------------------------------------------
              COMPUTATIONAL INFORMATION:
              ---------------------------------------------
              (a) L         = 7
              (b) Q         = 1280
              (c) K         = 141577
              (d) sum       = 876774.744346
              (e) sigma     = 0.002768
              (f) variance  = 3.125000
              (g) exp_value = 6.196251
              (h) phi       = 6.192918
              (i) WARNING:  1 bits were discarded.
              ---------------------------------------
SUCCESS             p_value = 0.228651
```

***Комментарий.*** Универсальный статистический тест Маурера вычисляет сумму логарифмов расстояний между одинаковыми шаблонами в исследуемой последовательности и проверяет ее близость к ожидаемой для случайной последовательности. Фактически тест проверяет невозможность сжатия последовательности. Тест позволяет выявлять широкий класс статистических дефектов, поэтому называется универсальным.

**Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 56 – 60 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# REVIEW OF MODERN QUANTUM KEY DISTRIBUTION PROTOCOLS

Sergiy Gnatyuk[1], Tetiana Okhrimenko[1], Sergiy Dorozhynskyy[1], Andriy Fesenko[2]
[1]National Aviation University, Kyiv, Ukraine
[2]Taras Shevchenko Kyiv National University, Kyiv, Ukraine

**ABSTRACT:** Modern quantum technologies of information security consist of following direction: quantum key distribution, quantum secure direct communication, quantum steganography, quantum secret sharing, quantum stream cipher quantum digital signature etc. In practice quantum key distribution is the most real technology for existed ICT and infrastructures. From this viewpoint, in the paper up-to-date quantum key distribution protocols were carried out as well as analysis of their strengths and weaknesses, prospects and difficulties of implementation in ICT was fulfilled. Also the modern commercial quantum key distribution systems were analyzed in accordance to used protocols of key distribution and encryption.

**KEYWORDS:** Quantum Cryptography, Quantum Key Distribution, Protocol, Data Confidentiality, Encryption, Commercial Systems, Information Communication Technologies.

## I. Introduction

One of the most effective ways to ensure data confidentiality and integrity in information communication technologies (ICT) and systems is cryptographic methods and systems. The purpose of them is to provide key distribution, authentication, legitimate users authorisation, and encryption. Key distribution is one of the most important problems of cryptography. This problem can be solved with the help of quantum key distribution (QKD), that provides information-theoretic security and it can also be used as a scheme for increase in key length [1].

In recent years, QKD has attracted considerable interest [2]. The overwhelming majority of theoretic and practical research projects in quantum cryptography are related to the development of QKD protocols. The number of different quantum technologies is increasing, but there is no comprehensive information about classification of these technologies in scientific literature (there are only a few works concerning different classifications of QKD protocols. This makes it difficult to estimate the level of the latest achievements and does not allow using quantum technologies with full efficiency. The main purpose of this paper is the review of up-to-date QKD protocols, analysis of their strengths and weaknesses, prospects and difficulties of implementation in ICT.

## II. QKD Protocols Review

Up-to-date QKD includes the following protocols [3-5]:

- using single (non-entangled) qubits (two-level quantum systems) and qudits ($d$-level quantum systems, $d>2$);
- using phase coding;
- using entangled states;
- decoy states protocols and others.

Let's analyse various QKD protocols based on different quantum technologies:

**1) BB84 Protocol.** The main task of QKD protocols is encryption key generation and distribution between two users connecting via quantum and classical channels. In 1984 Ch. Bennett from IBM and G. Brassard from Montreal University introduced the first QKD protocol, which has become an alternative solution for the problem of key distribution. This protocol is called BB84 and it refers to QKD protocols using single qubits. The states of these qubits are the polarisation states of

single photons. The BB84 protocol uses four polarisation states of photons ($0^\circ$, $45^\circ$, $90^\circ$, $135^\circ$). These states refer to two mutually unbiased bases. Error searching and correcting is performed using classical public channel, which need not be confidential but only authenticated. For the detection of intruder actions in the BB84 protocol, an error control procedure is used, and for providing unconditionally security a privacy amplification procedure is used. The efficiency of the BB84 protocol equals 50%. Efficiency means the ratio of the photons number which is used for key generation to the general number of transmitted photons.

**2) Six-State Protocol** requires the usage of four states, which are the same as in the BB84 protocol, and two additional directions of polarization: right circular and left circular. Such changes decrease the amount of information, which can be intercepted. But on the other hand, the efficiency of the protocol decreases to 33%.

**3) 4+2 Protocol** is intermediate between the BB84 and B92 protocol. There are four different states used in this protocol for encryption: "0" and "1" in two bases. States in each base are selected non-orthogonal. Moreover, states in different bases must also be pairwise non-orthogonal. This protocol has a higher information security level than the BB84 protocol, when weak coherent pulses, but not a single photon source, are used by sender. But the efficiency of the 4+2 protocol is lower than efficiency of BB84 protocol.

**4) Goldenberg-Vaidman Protocol**. In this protocol, encryption of "0" and "1" is performed using two orthogonal states. Each of these two states is the superposition of two localised normalised wave packets. For protection against intercept-resend attack, packets are sent at random times.

**5) Koashi-Imoto Protocol.** A modified type of Goldenberg-Vaidman protocol is called the Koashi-Imoto protocol. This protocol does not use a random time for sending packets, but it uses an interferometer's non-symmetrisation (the light is broken in equal proportions between both long and short interferometer arms).

**6) B92 Protocol.** Another type of QKD protocol is a protocol using phase coding: for example, the B92 protocol using strong reference pulses. An eavesdropper can obtain more information about the encryption key in the B92 protocol than in the BB84 protocol for the given error level, however. Thus, the security of the B92 protocol is lower than the security of the BB84 protocol. The efficiency of the B92 protocol is 25%.

**7) Ekert Protocol (E91)** refers to QKD protocols using entangled states. Entangled pairs of qubits that are in a singlet state $\left|\psi^-\right\rangle = 1/\sqrt{2}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$ are used in this protocol. Qubit interception between Alice to Bob does not give Eve any information because no coded information is there. Information appears only after legitimate users make measurements and communicate via classical public authenticated channel. But attacks with additional quantum systems (ancillas) are nevertheless possible on this protocol. Kaszlikowski et al. carried out the generalisation of the Ekert scheme for three-level quantum systems and Durt et al. carried out the generalisation for *d*-level quantum systems: this increases the information capacity of the protocol a lot. Thus, from all contemporary QKD protocols using qudits, the most effective and secure against non-coherent attack is the protocol using single qudits and two bases (BB84 for qubits).

The aforementioned protocols with qubits are vulnerable to photon number splitting attack. This attack cannot be applied when the photon source emits exactly one photon. But there are still no such photon sources. Therefore, sources with Poisson distribution of photon number are used in practice. The part of pulses of this source has more than one photon. That is why Eve can intercept one photon from pulse (which contains two or more photons) and store it in quantum memory until Alice transfers Bob the sequence of bases used. Then Eve can measure stored states in correct basis and get the cryptographic key while remaining invisible. It should be noted that there are more advanced strategies of photon number splitting attack which allow Bob to get the correct statistics of the photon number in pulses if Bob is controlling these statistics.

In practice for realisation of BB84 and six-state protocols weak coherent pulses with average photon number about 0.1 are used. This allows avoiding small probability of two- and multi-photon pulses, but this also considerably reduces the key rate.

**8) SARG04 protocol** does not differ much from the original BB84 protocol. The main difference does not refer to the "quantum" part of the protocol; it refers to the "classical" procedure of key sifting, which goes after quantum transfer. Such improvement allows increasing security against photon number splitting attack. The SARG04 protocol in practice has a higher key rate than the BB84 protocol.

**9) Decoy states protocol.** Another way of protecting against photon number splitting attack is the use of decoy states QKD protocols, which are also advanced types of BB84 protocol. In such protocols, besides information signals Alice's source also emits additional pulses (decoys) in which the average photon number differs from the average photon number in the information signal. Eve's attack will modify the statistical characteristics of the decoy states and/or signal state and will be detected. As practical experiments have shown for these protocols (as for the SARG04 protocol), the key rate and practical length of the channel is bigger than for BB84 protocols. Nevertheless, it is necessary to notice that using these protocols, as well as the others considered above, it is also impossible without users pre-authentication to construct the complete high-grade solution of the problem of key distribution.

## III. Advantages and Disadvantages of QKD Protocols

After the analysis of the first and scale quantum method, we must sum up and highlight the following advantages of QKD protocols:

- These protocols always allow eavesdropping to be detected because Eve's connection brings much more error level (compared with natural error level) to the quantum channel. The laws of quantum mechanics allow eavesdropping to be detected and the dependence between error level and intercepted information to be set. This allows applying privacy amplification procedure, which decreases the quantity of information about the key, which can be intercepted by Eve. Thus, QKD protocols have unconditional (information-theoretic) security.
- The information-theoretic security of QKD allows using an absolutely secret key for further encryption using well-known classical symmetrical algorithms. Thus, the entire information security level increases. It is also possible to synthesize QKD protocols with Vernam cipher (One-Time Pad) which in complex with unconditionally secured authenticated schemes gives a totally secured system for transferring information.

The disadvantages of QKD protocols are:

- A system based only on QKD protocols cannot serve as a complete solution for key distribution in open networks (additional tools for authentication are needed).
- The limitation of quantum channel length which is caused by the fact that there is no possibility of amplification without quantum properties being lost. However, the technology of quantum repeaters could overcome this limitation in the near future.
- Need for using weak coherent pulses instead of single photon pulses. This decreases the efficiency of protocol in practice. But this technology limitation might be defeated in the nearest future.
- The data transfer rate decreases rapidly with the increase in the channel length.
- Photon registration problem which leads to key rate decreasing in practice.
- Photon depolarization in the quantum channel. This leads to errors during data transfer. Now the typical error level equals a few percent, which is much greater than the error level in classical telecommunication systems.
- Difficulty of the practical realisation of QKD protocols for *d*-level quantum systems.

## IV. Commercial QKD Systems

The world's first commercial quantum cryptography solution was QPN Security Gateway (QPN-8505) proposed by MagiQ Technologies (USA). This system is a cost-effective information security solution for governmental and financial organisations. It proposes VPN protection using

QKD (up to 100 256-bit keys per second, up to 140 km) and integrated encryption. The QPN-8505 system uses BB84, 3DES and AES protocols.

The Swiss company ID Quantique offers systems called Clavis and Cerberis. Clavis uses a proprietary auto-compensating optical platform, which features outstanding stability and interference contrast, guaranteeing low quantum bit error rate. Secure key exchange becomes possible up to 100 km. This optical platform is well documented in scientific publications and has been extensively tested and characterized. Cerberis is a server with automatic creation and secret key exchange over a fibre channel (FC-1G, FC-2G and FC-4G). This system can transmit cryptographic keys up to 50 km and carries out 12 parallel cryptographic calculations. The latter substantially improves the system's performance. The Cerberis system uses AES (256-bits) for encryption and BB84 and SARG04 protocols for quantum key distribution. Main features of Cerberis system are:

- Future-proof security.
- Scalability: encryptors can be added when network grows.
- Versatility: encryptors for different protocols can be mixed.
- Cost-effectiveness: one quantum key server can distribute keys to several encryptors.

Toshiba Research Europe Ltd (Great Britain) recently presented another QKD system named Quantum Key Server. This system delivers digital keys for cryptographic applications on fibre optic based computer networks. Based on quantum cryptography it provides a failsafe method of distributing verifiably secret digital keys, with significant cost and key management advantages. The system provides world-leading performance. In particular, it allows key distribution over standard telecom fibre links exceeding 100 km in length and bit rates sufficient to generate 1 Megabit per second of key material over a distance of 50 km – sufficiently long for metropolitan coverage. Toshiba's system uses a simple "one-way" architecture, in which the photons travel from sender to receiver. This design has been rigorously proven as secure from most types of eavesdropping attack. Toshiba has pioneered active stabilisation technology that allows the system to distribute key material continuously, even in the most challenging operating conditions, without any user intervention. This avoids the need for recalibration of the system due to temperature-induced changes in the fibre lengths. Initiation of the system is also managed automatically, allowing simple turn-key operation. It has been shown to work successfully in several network field trials. The system can be used for a wide range of cryptographic applications, e.g., encryption or authentication of sensitive documents, messages or transactions. A programming interface gives the user access to the key material.

Another British company, QinetiQ, realised the world's first network using quantum cryptography – Quantum Net (Qnet). The maximum length of telecommunication lines in this network is 120 km. Moreover, it is a very important fact that Qnet is the first QKD system using more than two servers. This system has six servers integrated to the Internet.

## V. Conclusions

Today the most developed direction of quantum cryptography is QKD protocols. In research institutes, laboratories and centres, quantum cryptographic systems for secret key distribution for distant legitimate users are being developed. This paper presents a systematization of modern QKD protocols. Analysis of the advantages and disadvantages of various QKD protocols is made. Their advantage is a high level of security and some properties, which classical means of information security do not have. One of these properties is the ability always to detect eavesdropping.

Modern commercial QKD systems were analyzed in accordance to used protocols of key distribution and encryption. QKD systems can be combined with any classical cryptographic (encryption) scheme [6-7], which provides information-theoretic security, and the entire cryptographic scheme will have information-theoretic security also.

Quantum technologies therefore represent an important step towards improving the security of ICT against cyberattacks. But many theoretical and practical problems must be solved for wide practical use of QKD in ICT and information infrastructures.

**REFERENCES**

1. Nielsen M.A., Chuang I.L. (2010) Quantum computation an quantum information, Cambrige, Cambrige University Press, 708 p.

2. Advanced Technologies of Quantum Key Distribution, Monograph [edited by Sergiy Gnatyuk], London, Great Britain : InTech, 227 p. (2018).

3. S. Gnatyuk, T. Zhmurko, P. Falat, Efficiency Increasing Method for Quantum Secure Direct Communication Protocols, Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015), Warsaw, Poland, September 24-26, Vol. 1, 2015, pp. 468-472.

4. Zh. Hu, S. Gnatyuk, T. Okhrimenko (Zhmurko), V. Kinzeryavyy, M. Iavich, Kh. Yubuzova, High-Speed Privacy Amplification Method for Deterministic Quantum Cryptography Protocols Using Pairs of Entangled Qutrits, CEUR Workshop Proceedings, Vol. 2393, pp. 810-821, 2019.

5. Qoussini A.E., Daradkeh Y.I., Al Tabib S.M., Gnatyuk S., Okhrimenko T., Kinzeryavyy V. Improved model of quantum deterministic protocol implementation in channel with noise, Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 2019), 2019, pp. 572-578.

6. S. Gnatyuk, V. Kinzeryavyy, M. Iavich, D. Prysiazhnyi, Kh. Yubuzova, High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks, CEUR Workshop Proceedings, Vol. 2104, pp. 657-668, 2018.

7. Gnatyuk S., Akhmetov B., Kozlovskyi V., Kinzeryavyy V., Aleksander M., Prysiazhnyi D. New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis, Advances in Intelligent Systems and Computing, Vol. 1126, pp. 93-104, 2020.

**Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 61 – 64 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# GEOPOLITICS AND INFORMATION WARFARE

***V. Khoroshko [1], V. Artemov [1], I. Ivanchenko [1], M. Brailovskyi [2]***

[1]National Aviation University, Kyiv, Ukraine,
[2]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

**ABSTRACT**: The emergence of an information society has led to a revision of old positions in politics in general and geopolitics in particular. The article is devoted to the analysis of the basic qualitative changes reflecting the new conditions and the content of geopolitical competition in the information society. The main reasons why the threat of information and psychological confrontation in the geopolitical space should be taken seriously.

**Keywords:** *geopolitics, information expansion, information aggression, information warfare.*

For any state, the state of its political relations with other states is a determining factor for internal stability and security. Politics as a line of work is an important mean of external influence that can take the form of aggression and lead to a political undermining of the power of the aggrieved state, the destruction of its military and economic potential, and even to the complete or partial separation of the entities and territories, its constituents. The standardization of architectural principles of construction, equipment and software of personal computers, high mobility of software and several other features determine the relatively easy access of a professional to the information contained in the information system. If the information resources are used by a group of users, it may be necessary to restrict access to the information of different users.

Since information technologies are developing rapidly and spreading in all spheres of human life, so information is increasingly becoming a strategic resource of the state, productive power and expensive goods. This causes the desire of states, organizations and individuals to gain benefits of taking possession of information that is not available to their opponents, as well as damaging the opponent's information resources and protecting their own [1,2,3].

In terms of intensity, scale and means used, the following terms should be distinguished: information expansion, information aggression and information warfare.

The severity of interstate information warfare can be observed in the defense matters, the highest form of which is information wars nowadays. We observe it ourselves in our country. The issue of information confrontation at the level of organizations and individual citizens is equally distressing. This is evidenced by numerous attempts by cybercriminals to gain control over computer technology and information for material benefit [1, p. 258].

The confrontation of the state in the field of information technology, the desire of the attackers to misuse information resources, the need to ensure the rights of citizens in the information sphere, the presence of many accidental threats cause the urgent need to protect information in computer systems, which are the material basis of informatization of society.

It can be argued that in the information sphere, aggression escalates into war if one of the parties of the conflict begins to use information weapons against its opponents. This criterion makes it possible to distinguish from all the diversity of processes and phenomena occurring in the information society.

Information warfare is the highest level of information warfare aimed at outbreaking socio-political, ideological, as well as national, territorial, and other conflicts between states, peoples, nations, classes, and social groups through the widespread use of information violence tools and methods.

With the advent of the information society era, the geopolitical picture of the world has changed dramatically. First and foremost, information and information technologies have become a major resource in the information society, which have displaced or reduced the importance of strategic resources such as natural resources, populations, territories, etc.

With the advent of global telecommunication networks, the factor of relative openness or closedness of continental and maritime powers has changed, as well as the factor of remoteness and

reach. Information can now be transmitted over open telecommunications systems almost instantaneously, thus, in an information society, territories with underdeveloped network infrastructure may be more distant from public life and civilization than islands in the Pacific equipped with satellite systems. The level of development of network technologies, their integration into different spheres of public life, the concentration of nodes of network infrastructure and other network resources in one area and their lack in others always leads to industrial, economic, cultural backwardness and general regression of territories and states located away from information flows.

Studying who actually controls information flows and network infrastructures by channeling them across different territories may suggest the idea of dividing all states in the information space into those with information and network technologies and those without communication in in this area and dependent on the orientation of the information policy of the dominant states in the information space, which inevitably leads to the infringement of the national interests of the states with less information potential. Such states in the information and psychological sphere are almost colonially dependent on the states-owners of networks and technologies, which allows to speak about the origin in the information society of the processes of division of territories into colonies and metropolises, the processes of modern information neo-colonialism [2, p. 315].

With the emergence of information and telecommunication networks, borders between states have become transparent for the main resource of the information society that is information. The emergence of transnational provider corporations has transformed their relationship from traditional to geopolitical. The emergence, along with the traditional types of political, economic and armed confrontation of information and psychological wars, markedly changed the military-strategic balance that had developed in the post-World War II world and led to a reassessment of the damage caused by conventional weapons, and, consequently, to the reassessment of military-political potential, which is an important geopolitical category [3,4].

The formation of the information society has led to a revision of the old positions in politics in general and in geopolitics in particular. The main qualitative changes reflecting the new conditions and the content of geopolitical competition in the information society are the following [3,4,5]:

1. Expansion of the concept of geopolitical space and space of geopolitical competition itself. In the information society, the geopolitical space is taking on a full dimension, including the space of information and psychological relations of modern society.

The struggle of geopolitical actors, their alliances and coalitions to achieve the informational advantage of acquiring more advanced information resources, which open up better opportunities to control the information resources of rivals in this struggle, becomes the main focus of geopolitical competition and significantly changes its nature.

2. Changes in the evaluation of strategically important resources. Information resources of the information society, including information flows, information and telecommunication networks and objects of their infrastructure, as well as sources that generate information or provide it with new quality in the process of analysis and processing (e.g. research portals centers with high intellectual potential), is the most important strategic resource for any subject of geopolitical competition, for the possession of which the geopolitical struggle, which results in gaining benefit be one subject and loss for the others, which affects the state of their safety.

3. Changes in the selection and evaluation of traditional allies and opponents in the geopolitical struggle. As a result of a change in the hierarchy of strategically important resources for the possession (or the right to influence their production, distribution and use) of which between particular geopolitical entities. Moreover, competition for the priority of information resources in assessing the power of the subject of geopolitical relations is unfolding, and the role of the geographical position of the states in relation to transport communications and mineral resources is emerging, as well as the interests and strategies of their achievement in the "maritime" and "continental" states that were pursued in the former the geopolitical picture of the world is the opposite of goals, converging and becoming virtually identical, enabling them to successfully overcome these differences and join alliances and coalitions. In an information society, the choice of traditional allies and opponents in the geopolitical struggle depends not on their island or continental location and the predominant role of maritime or land communications in the movement of human resources and material assets, but on the level of development of information resources and their compatibility (opportunities common goals), as well as the compatibility of national ideologies with their improvement and further development. At the same

time different states can act as a coalition in the information and psychological struggle, pursuing common geopolitical goals.

4. New subjects of geopolitical competition (virtual coalitions). In addition to the traditional subjects of geopolitical competition, that are acting at the global and regional levels of states and various international coalitions in the information and psychological space, fundamentally new centers are involved in the geopolitical struggle – virtual alliances and coalitions, that consist of states, transnational corporations, media holdings participating on the equal basis, whose scope of activity is global (covers large territories), and the results of the activities may affect the policies of states and their coalitions at the international level. However, state sovereignty, its own territory and population is not a prerequisite for the subject to participate in geopolitical competition, and this significantly differentiates the information society from the industrial one.

5. The possibility of a conflict-free combination of cooperation and confrontation in geopolitical relations. Geopolitical competition was carried out within a single geographical space and resources distributed within it. In these circumstances, it was practically impossible to combine allied relations and competitive struggle between allies without internal contradictions. As a result of competition, they were carried out secretly, often leading to the collapse of the union (coalition).

The information (informational and psychological) sphere with its intensively developing processes, in which some states increase their information potential and others lose it (as information, as well as money, has high mobility and concentrates where its turnover and implementation creates the most favorable conditions), creates many independent directions and varieties of social relations. For geopolitical subjects, the desire to control these social relations and processes (which is a prerequisite for achieving excellence in ϕ part of the information and psychological sphere) may cause geopolitical competition to emerge on this basis [5,6].

The nature of information space allows different subjects of geopolitical relations to be allies and competitors (opponents) at the same time. Geopolitical entities may at the same time conflict with other entities of geopolitical competition over the influence on one or another part of the information and psychological sphere and in the coalition over the influence on the other part.

6. Changes in the system of assess the strength of the subjects of geopolitical competition in the information-psychological sphere. The aggregate power of objects of geopolitical relations in the informational and psychological sphere is estimated by the following categories:

- ability to control own segment of information space;
- the ability to effectively compete within the information field;
- the ability to expand the sphere of its influence in the information space.

The ability to control one's own segment of the information space is conditioned by the presence of enough information (intellectual and scientific-technical) potential, which ensures the independence and sustainable development of the national segment of the information space for the subject.

In the past, geopolitical conflicts have been arising around the physical and military-political division and redistribution of the world and its individual regions and, accordingly, have been gaining a form of armed, military-political, or ideological, with military preparations for confrontation. Nowadays the main battle for the spheres of influence is conducted in the informational and psychological sphere by special latent methods and means. The power of a geopolitical subject, in addition to its information resources, possession of information weapons, and practical experience of its use, includes the potential to reflect information-psychological aggression, which includes the mental health of society and factors that link the information society into a single socio-cultural whole – national awareness, national ideology and a clear, consistent and effective information policy.

7. Information and psychological influence as a way to ensure geopolitical balance. Informational confrontation implemented in the form of informational and psychological operations. The main tool of ensuring a geopolitical balance in the modern multipolar world that has reached the stage of building an information society.

8. Information expansion. Traditionally, expansion in geopolitics has been understood primarily as territorial acquisitions and establishment of military-political spheres of influence, as well as activities in this area (expansion policy). Today, expansion is a continuous political process aimed at many objects and, as a result, conflicts of interest give rise to a complex set of diverse conflicts. The so-called "peaceful" expansion is carried out by many states and their groups in relation to each other, so we can talk about their "interpenetration" or, in other words, the formation of a complex of

interdependencies and contradictions (for example, providing information supremacy). The intra-coalition expansion is periodically accompanied by "voluntary" mutual concessions of the parties, although their overall balance, of course, contributes to the strongest of them.

9. Neo-colonialism of the information society. An important feature of information and psychological expansion of the subjects of geopolitical competition is the so-called information and psychological neo-colonialism, which divides all countries and regions of the world into subjects, dominant in the information and psychological space and are sources of expansion, and subjects, who do not possess the necessary information resources, technologies and developed information and telecommunications infrastructure and are therefore information dependent on the dominant entities. [7,8]

It is seen that the concept of information confrontation in the geopolitical space includes the whole spectrum of conflict situations in the information and psychological sphere - from interpersonal conflicts to open confrontation of social systems. Information psychological warfare is definitely one of the types of information warfare. There are several main reasons why the threats of information and psychological confrontation in the geopolitical space should be taken seriously and their laws and conditions of development carefully studied [9, p. 198]:

- first, modern wars are increasingly becoming psychological and reminiscent of a large-scale PR company, and their own military operations are gradually sidelined and play a well-defined and limited role, given to them in the overall scenario of a military company;
- secondly, modern technologies of psychological combat can inflict no less damage on the enemy than an armed attack, and information weapons built on the basis of technology of psychological influence have a much greater penetrating and selective ability than modern systems of precision weapons;
- thirdly, in international politics they are displaced from political practice or replaced in it by other, more influential forms of political regulation than war in general and military actions in general;
- fourth, there is a need to emphasize the high social dangers of some contemporary organizational forums and technologies of information and psychological influence that are used for political purposes.

**REFERENCES**

1. Bukharin, S. N. (2007) Metody i tekhnologii informatsionnykh voyn. “Methods and Techniques of Information Warfare”. M: Academic project. 382 p. [in Russian].

2. Makarenko, S. I. (2017) Informatsionnoye protivoborstvo i radio- elektronnaya bor'ba v setetsentricheskikh voynakh nachala XXI veka. “Information Warfare and Radioelectronic Struggle in the Network-Centric Wars of the Early Twenty-First Century”. SPB: High Tech. 546 p. [in Russian].

3. Pirtskhalava, L. G., Khoroshko, A.V., Khokhlacheva, J. E. and others (2019). Informatsionnoye protivoborstvo v sovremennykh usloviyakh. “Information Warfare in Modern Conditions”. "Komprint". 226 p. [in Russian].

4. Panarin, N. N. (2011) Informatsionnaya voyna i geopolitika. “Information Warfare and Geopolitics”. M: Peace and Security. 719 p. [in Russian].

5. Rastorguiev, S. P. (2003) Filosofiya informatsionnoy voyny. “Philosophy of Information War”. M: Psychological Socialogical Institute. 496 p. [in Russian].

6. Pocheptsov, G. G. (1999) Teoriya i praktika informatsionnykh voyn. “Theory and Practice of Information Wars”. Rovno: "Volynsk Charms".124 p. [in Russian].

7. Tolubko ,V. B. (2003) Informaciina borotba (kontseptual′ni, teoretychni, tekhnolohichni aspekty). “Information Struggle (conceptual, theoretical, technological aspects)”. Kyiv. 320 p. [in Ukrainian].

8. Manoilo, A.V. (2008) Tekhnologii nesilovogo razresheniya sovremennykh konfliktov. “Technology of Non-Coercive Resolution of Contemporary Conflicts”. M: Hotline –Telecom. 392 p. [in Russian].

9. Metody i priyemy psikhologicheskoy voyny. “Methods and Techniques of Psychological War” / compiler S.T. Taras. M: AST-Minsk: Harvey, 2006. 420 p. [in Russian].

**Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 65 – 70 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# HIGH-SPEED AND SECURE HASH FUNCTION FOR BLOCKCHAIN SECURITY MECHANISMS

Anatoliy Hrytsak[1], Vasyl Kinzeryavyy[2], Dmytro Prysiazhnyi[1], Yuliia Burmak[3], Yevhen Samoylik[2]
[1]Vinnytsia National Technical University, Vinnytsia, Ukraine
[2]National Aviation University, Kyiv, Ukraine
[2]Kyiv College of Communication, Kyiv, Ukraine

**ABSTRACT:** Information communication technologies development and the emergence of new attack types leads to increasing the amount of existing hash functions vulnerabilities and other disadvantages. In every blockchain security mechanisms each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. New hash function development is very actual and value research task. Thus, in this paper a new hash function was proposed, which was based on well-known hash function. Improvements involved a number of changes: increased the size of words and an increase in the message digest; at the pre-processing stage, the incoming message is supplemented by a pseudo-random sequence; the numbers of nonlinear functions are increased. The proposed changes allow reducing the number of rounds in the compression function, which will guarantee at least similar security indicators with simultaneous increase in data processing speed.

**KEYWORDS:** Information Communication Technologies, Cybersecurity, Blockchain Security, High-Speed, Hash Function, Data Processing, Confidentiality and Integrity.

## I. Introduction

Every year the level of information security is increasing in organizations of different forms ownership. First of all, this is due to an increase in the flow of information that is provided in real time with the help of Internet resources. Through the web-portals of the organization highlight results of its activities, provide online services and financial services, conduct financial transactions and etc. The lion's share of the information circulating in the above-mentioned processes needs to be adequately protected. According to this, another important task is to ensure the proper protection of information during the exchanging data at the expense of Internet resources. One of the most common methods of such protection is the using of cryptographic certificates – digital certificates that ensure the confidential exchange of data between the client and using public key encryption. However, the certificate is not only an open key with information, but also a digital signature of a server or a web portal that is implemented using hash function. But, the number of cyberattacks, especially on web portals, has increased in geometric loopholes: blocking access, stealing confidential data, monitoring traffic, etc. At the intelligence stage, hackers monitor the network to identify weaknesses, where you can get the access to users working machines and ultimately penetrate into the network. Improvement of efficiency of digital certificates, as one of the most common methods of protecting information in the process of exchange and connection, is relevant and needs improvement. Such cyberattacks as DROWN (a vulnerability that allows decrypting ciphertext without a private key) [1], FREAK (vulnerability that allows you to penetrate into the installed encrypted connection and analyze a traffic) [2], LOGJAM (vulnerability that allows reading and modification of data transmitted over a secure communications channel [3]) caused large losses to many web resource owners, including such giants as Google, Mozilla, Yahoo, etc. and put under the question reliability of digital certificates. Besides, in every blockchain security mechanisms each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Therefore, increasing the reliability of digital certificates, as the most common methods for protecting the exchange of data through communication channels, is relevant and needs to be improved. The purpose of this work is high-speed and secure hash function development for using the information security systems and blockchain technologies.

## 2. Related papers

One of the most common cryptographic algorithms is hash function. They are necessary for "compressing" information into message digest that represent a bit combinations of fixed length. Hash functions of SHA-2 are very popular in applications related to the systematization, search and protection of information. Digital protocols use public key encryption to authenticate the client and server. At the confirmation stage, the hash function plays the role of the identification mark and is used to ensure the integrity of the data during transmission. That is, the hash function has to make it impossible to fake the certificate, while leaving the same signature of the verification center. Till recently, the SHA-1 hash function was used in digital certificates. In connection with the detection of numerous collisions in SHA-1 [4,5] and in the most digital certificates [5-7], Microsoft, Google and others initiated a decision to replace the hash function [8]. Starting in 2016 the SHA-2 hash function is used in the SSL certificate. However, technologies continue to improve, the power of technology is increasing, and today many works are devoted to the investigation of cryptographic strength of SHA-2, in particular, the following shortcomings were identified in works [9-10]: collisions for truncated variants SHA-512; finding the first and second prototypes; a birthday attack. The paper proposes a new method for constructing a hash function; it is the prototype of SHA-512. In our opinion, this hash function can allow to improve the efficiency of cryptographic protection of digital certificates when it is applied.

## 3. High-speed and secure hash function development

*Pre-processing step.* At the pre-processing step, an incoming message $M$ ($M \in V_N$, $V_N \in \{0,1\}^N$, $N$ is message length $M$ in bits, $N \in Z$, $N < 2^{128}$) are complemented by additional sequence $D_l$ (message length $M$) and pseudorandom sequence $salt$ (is determined on the basis of $M$), so that the resulting message length is a multiple of the length data blocks $L$ ($L = 1024 \cdot t'$ bits, $t' \in N$):

$$M_{rez} = \left( M,\ D_l, salt \right) \tag{1}$$

where $M_{rez} \in V_{NN}$, $V_{NN} = N + 128 + N_{salt}$, $D_l = H_{Dl}(M)$, $D_l \in V_{128}$, $salt = H_{Gen}(M)$, $salt \in V_{Nsalt}$, $N_{salt} = 2L - \left( (N + 128) \bmod L \right)$, as a function $H_{Gen}$ could be any function of generating a pseudorandom sequence which is based on $M$, $H_{Dl}$ is function of length $M$. Based on the completed message $M_{rez}$ will determine the hash value of the message $M$.

Message $M_{rez}$, $M_{rez} \in V_{NN}$, broken into $k$ $L$ - bit blocks: $M_{rez} = (m_1, m_2 .... m_k)$ where $m_i \in V_L$, $i = \overline{1,k}$, $k = (NN)/L$.

*Determination step of a hash.* The digest of the message is iteratively calculated, processing each one $m_i$ block messages $M_{rez}$, $m_i \in V_L$, $i = \overline{1,k}$ compression function $F_g$ (2), to get the resulting hash (3):

$$h_i = F_g\left(h_{i-1}, m_i\right),\ i = \overline{1,k} \tag{2}$$

$$H\left(IV, M_{rez}\right) = h_k \tag{3}$$

where $h_0 = IV$, $IV$ is initialization vector, $IV \in V_{L/2}$, $h_i$ is intermediate values of the messages digest $h_i \in V_{L/2}, i = \overline{1,k}$; $H$ is resulting hash, $H \in V_{L/2}$; $F_g$ is the compression function uses in the hash function.

The compression function $F_g$ is performed in three stages: splitting blocks into words (1), initialization of variables (2), compression (3).

<u>*Step 1*</u>. Each $m_i$ data block $M_{rez}$, $m_i \in V_L$, $i = \overline{1,k}$, decomposes into 16 words (4):

$$m_i = \left( W_0^i, ..., W_{15}^i \right) \tag{4}$$

where $W_j^i \in V_{L/16}$, $j = \overline{0,15}$.

On the basis of words which are received $W_j^i$, $j=\overline{0,15}$, words are calculated $W_u^i(5)$ $W_u^i \in V_{L/16}$, $u=\overline{16,63}$:

$$W_u = W_{u-16} + Delta0(W_{u-15}) + W_{u-7} + Delta1(W_{u-2}), \quad (5)$$

where $Delta0(W_u) = Rotr(W_u,1) \oplus Rotr(W_u,8) \oplus SHR(W_u,7)$,
$Delta1(W_u) = Rotr(W_u,19) \oplus Rotr(W_u,61) \oplus SHR(W_u,6)$, $Rotr(x,l)$ is right bitwise cyclic shift of argument $x$ for $l-$bits; $SHR(x,l)$ is left shift argument $x$ for $l-$bits.

Step 2. Re-initialization of internal state vectors is performed $T$ (6), $T=(T_1,...,T_8)$, $T_z \in V_{L/16}$, $z=\overline{1,8}$:

$$T_z = h_{i-1}^z \quad (6)$$

where $h_{i-1}=(h_{i-1}^1,...,h_{i-1}^8)$, $h_{i-1}$ is the previous value of the digest, which is fed to the input of the function $F_g$, $h_{i-1}^z \in V_{L/16}$, $z=\overline{1,8}$.

Step 3. At this step, there is a direct compression of the data block $m_i \in V_L$, $i=\overline{1,k}$, $k = NN/L$, the value of the vectors of the internal state will change each 64 rounds $T=(T_1,...,T_8)$, $T_z \in V_{L/16}$, $z=\overline{1,8}$, through their mixing with vectors $W_j$ and constants $K_j$ $j=\overline{0,63}$.

For each $j$ round, the mathematical actions given in the formulas will be executed (7) - (11), $j=\overline{0,63}$:

$$F_{g_1} = T_8 \oplus Sigma1(T_5) \oplus Ch(T_5,T_6,T_7) + W_j + K_j \quad (7)$$

$$F_{g_2} = Sigma0(T_1) \oplus Maj(T_1,T_2,T_3) \quad (8)$$

$$F_{g3} = JQ(T_3,T_6) \oplus Maj(T_2,T_3) \quad (9)$$

$$F_{g_4} = SH(T_8,T_7) \oplus Sigma(T_8) \quad (10)$$

$$T_8 = T_7 + F_{g_4};\ T_7 = T_6;\ T_6 = T_5;\ T_5 = T_4 + F_{g_1};\ T_4 = T_3;\ T_3 = T_2 + F_{g_3};\ T_2 = T_1;\ T_1 = F_{g_1} + F_{g_2} \quad (11)$$

where $T_z$ are vectors of the internal state, $T_z \in V_{L/16}$, $z=\overline{1,8}$; $W_j$ are words which are broken from $m_i$ block; $K_j$ are predetermined constants (if necessary, may change), $K_j \in V_{L/16}$;
$Ch(x,y,z)$, $Maj(x,y,z)$, $Sigma0(x)$, $Sigma1(x)$, $Delta0(x)$, $Delta1(x)$, $JQ(x,y)$ and $SH(x,y)$ are nonlinear functions that are described in (12) - (19):

$$Sigma0(x) = Rotr(x,28) \oplus Rotr(x,34) \oplus Rotr(x,39) \quad (12)$$

$$Sigma1(x) = Rotr(x,14) \oplus Rotr(x,18) \oplus Rotr(x,41) \quad (13)$$

$$Ch(x,y,z) = (x+y) \oplus (\bar{x}+z) \quad (14)$$

$$Maj(x,y,z) = (x+y) \oplus (x+z) \oplus (y+z) \quad (15)$$

$$Delta0(x) = Rotr(x,1) \oplus Rotr(x,8) \oplus SHR(x,7) \quad (16)$$

$$Delta1(x) = Rotr(x,19) \oplus Rotr(x,61) \oplus SHR(x,6) \quad (17)$$

$$JQ(x,y) = (\bar{x}+y) \oplus Rotr(x,13) \oplus SHR(\bar{y},17) \quad (18)$$

$$SH(x,y) = SHR(x,7) \oplus Rotr(y,8) \oplus Rotr(\bar{x},y) \quad (19)$$

where $F_g$ is intermediate compression function value, $F_{g_o} \in V_{L/16}$, $o = \overline{1,4}$, $Ch(x,y,z)$, $Maj(x,y,z)$, $Sigma0(x)$, $Sigma1(x)$, $Delta0(x)$, $Delta1(x)$, nonlinear functions that were used in the original SHA-2. $JQ(x,y)$ and $SH(x,y)$ are new nonlinear functions that were proposed in this hash function.

After completing the last round, the values of the vectors of the internal state $T = (T_1,...,T_8)$, $T_z \in V_{L/16}$, $z = \overline{1,8}$, completely changed as follows:

$$T_z = T_z \oplus h_{i-1}^z, \tag{20}$$

where $h_{i-1}$ is the previous value of the digest, which is fed to the input of the function $F_g$ $h_{i-1} = (h_{i-1}^1,...,h_{i-1}^8)$, $h_{i-1}^z \in V_{L/16}$, $z = \overline{1,8}$. The output of the function will be given to the final values of the internal state vectors.

In our opinion, the method for constructing a hash function is developed by adding a pseudorandom sequence $salt$ to an incoming message at the pre-processing and non-linear operations $JQ(x,y)$ and $SH(x,y)$ at the step of determining the hash values. It is possible to reduce the total number of rounds in the compression function with similar or better performance and security indicators data in the aspect of resistance to various attacks and neutralization of known vulnerabilities compared with the SHA-2. Theoretical and experimental researches will be conducted for verification of this statement and cryptanalysis performing in the further works.

## 4. Experiments and discussion

For the experimental study on the basis of the proposed method, three hash functions with such parameters were constructed: $t' = 1$, $L = 1024 \cdot t' = 1024$, $H \in V_{L/2} = V_{512}$ for $BK_1$; $t' = 2$, $L = 1024 \cdot t' = 2048$, $H \in V_{L/2} = V_{1024}$ for $BK_2$; $t' = 3$, $L = 1024 \cdot t' = 3072$, $H \in V_{L/2} = V_{1536}$ for $BK_3$. As a function $H_{Gen}$ for $BK_i$, $i = \overline{1,3}$ cryptographic algorithm SNOW 2.0 was selected. The software implementation of proposed hash functions was carried out as console tool using the programming language C++. Development environment was Microsoft Visual Studio 2013 (Release Version).

Therefore, to study the statistical characteristics of hash functions, these were investigated in the statistical test NIST STS [11]. Also proposed hash functions were compared with the results of the benchmark generator of pseudo-random sequences BBS and some block symmetric ciphers (Kalyna, Luna, Neptun), which worked in counter mode. Note that for this research, based on the developed hash functions and the SHA-512 function, stream ciphers were constructed to generate required length files for NIST STS statistical tests.

In Fig. 1 the statistical portrait of the passage of statistical tests is given for $BK_1$ (similar portraits can be built for $BK_2$ and $BK_3$), and in Table 1 the results of the study was showed. It showed that the proposed functions of healing passed a comprehensive control in accordance to NIST STS.

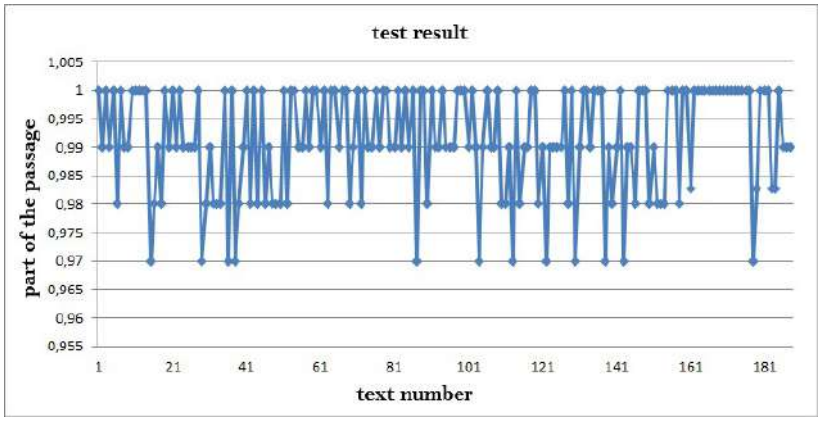


Fig. 1. The statistical portrait of the stream cipher on the basis of $BK_1$

Table 1. Sequence testing results

| Generator | The number of tests in which the testing was completed | |
|---|---|---|
| | 99% | 96% sequence |
| BBS | 133 | 188 (100%) |
| Kalyna | 136 | 188 (100%) |
| Luna | 141 | 188 (100%) |
| Neptun | 140 | 188 (100%) |
| SHA-512 | 137 | 188 (100%) |
| $BK_1$ | 141 | 188 (100%) |
| $BK_2$ | 140 | 188 (100%) |
| $BK_3$ | 142 | 188 (100%) |

Also, the study of the rate characteristics for developed hash functions $BK_i$, $i=\overline{1,3}$ was carried out. To do this randomly selected several files of different sizes and for each file was scanned hash code, while measuring the time hash code, see Table 2.

All experiments were performed using the system with following characteristics: Intel (R) Core (TM) i3-6100 processor, 3.7 GHz processor, and a 4 GB RAM based on the 64-bit Windows 7 Service Pack 1.

Table. 2 Results of the study for the speed characteristics of the hash functions

| Hash function | File 1, 1 MB | | File 2, 10 MB | | File 2, 100 MB | |
|---|---|---|---|---|---|---|
| | $t$, s | $v$, MB /s | $t$, s | $v$, MB /s | $t$, s | $v$, MB /s |
| SHA-512 | 0.015 | 68,26 | 0,145 | 70,62 | 1,38 | 74,20 |
| $BK_1$ | 0,012 | 85,33 | 0,101 | 101,38 | 0,926 | 110,58 |
| $BK_2$ | 0,011 | 93,09 | 0,098 | 104,48 | 0,902 | 113, 52 |
| $BK_3$ | 0,011 | 93,09 | 0,094 | 108,93 | 0,879 | 116,49 |

According to the obtained results of the developed hash functions' speed characteristics $BK_i$, $i=\overline{1,3}$, are better than well-known and widely used SHA-512 hash function.

## 5. Conclusions

The paper proposes a new method for secure hash function constructing, which can be used to improve the effectiveness of cryptographic protection of digital certificates in the future. It will provide a more reliable exchange of confidential information on the network. The method requires further research to test the performance on different platforms, the resistance to common methods of cryptanalysis. In the following works, it is planned to conduct the above-mentioned studies and compare them with the parameters of the hash functions of the SHA-2 series.

## REFERENCES

1. N. Aviram, S. Schinzel, J. Somorovsky, "DROWN: Breaking TLS using SSLv2, Proceedings of the 25th USENIX Security Symposium", pp.18, 2016. [Online]. Available: https://drownattack.com/drown-attack-paper.pdf

2. M. Green, "Attack of the week: FREAK (or 'factoring the NSA for fun and profit')" [Online]. Available: https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa/ | Date accesses: april 2018|.

3. B. Duncan, "Weak Diffie-Hellman and the Logjam Attack", [Online]. Available: (https://weakdh.org/ | Date accesses: april 2018|.

4. P. Karpman, T. Peyrin, M. Stevens, “Practical Free-Start Collision Attacks on 76-step SHA-1”, [Online]. Available: https://eprint.iacr.org/2015/530

5. S. Sanadhya, P. Sarkar, “22-Step Collisions for SHA-2” [Online]. Available: http://arxiv.org/abs/0803.1220

6. F. Kohlar, S. Schage, “On the Security of TLS-DH and TLS-RSA in the Standard Model1”, pp.50, 2013 [Online]. Available: http://eprint.iacr.org/2013/367.pdf

7. C. Meyer, J. Schwenk, “Chair for Network and Data Security Ruhr-University Bochum. Lessons Learned From Previous SSL/TLS Attacks A Brief Chronology Of Attacks And Weaknesses”, pp.15 [Online]. Available: http://eprint.iacr.org/2013/049.pdf

8. C. Castelluccia, E. Mykletun, “Improving Secure Server Performance by Re-balancing SSL/TLS Handshakes”. pp.11 (Published in “Proceeding ASIACCS '06 Proceedings of the 2006 ACM Symposium on Information, computer and communications security. pp 26-34”).

9. F. Mendel “Improving Local Collisions: New Attacks on Reduced SHA-256”, p.17 [Online]. Available: https://eprint.iacr.org/2015/350.pdf

10. C.Dobraunig, M. Eichlseder, “Analysis of SHA-512/224 and SHA-512/256”, p.30 [Online]. Available: https://eprint.iacr.org/2016/374.pdf

11. NIST Special Publication 800-22 “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications” [Online]. Available:https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf

**Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 71 – 74 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# „GozNym“-ი ტრანსნაციონალური კიბერდანაშაულისთვის”
# “GozNym” for transnational cybercrime“

ნათია ფილაშვილი
ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, III კურსის სოციოლოგიის მიმართულების სტუდენტი
მარიამ კიკლიაშვილი
ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, III კურსის სოციოლოგიის მიმართულების სტუდენტი.

Natia Pilashvili
Ivane Javakhishvili Tbilisi State University, Sociology_Junior;
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. მაშინ, როდესაც კიბერდანაშაული და ტანსნაციონალური დანაშაული ერთად მოქმედებს, საქმე გვაქვს მასშტაბურ, გლობალურ დანაშაულთან, რომელთან ბრძოლაც გაცილებით რთულია. სწორედ, ერთ-ერთი ასეთი ტრანსნაციონალური კიბერდანაშაულის იარაღს წარმოადგენდა „GozNym“-ის მავნე პროგრამა, რომლის საშუალებითაც 41 000 ათასზე მეტი ადამიანი ფინანსურად დაზარალდა.

**Annotation:** In the 21st century, in parallel with rapid technological progress, the increasing trend of unsolved and inexcusable crimes is marked by cybercrime, often referred to as "the crime of the future." Malicious software, one of the key mechanisms of cybercrime, makes it easy for us to be victims of it. While cybercrime and transnational crime work together, we are dealing with large-scale, global crime that is far more difficult to combat. One of these transnational cybercrime weapons was „GozNym’s” malicious program that has affected more than 41,000 people financially.

**საკვანძო სიტყვები:** კიბერდანაშაული, დისტანციური მართვის მექნიზმი(RAT), „ტროიანი“,

„GozNym”, „ტრანსნაციონალური დანაშაული“.

# „GozNym“-ი ტრანსნაციონალური კიბერდანაშაულისთვის”

დღეს ტრანსნაციონალური დანაშაული მსოფლიოს წინაშე მდგარი უდიდესი გამოწვევაა. ის ორგანიზებული დანაშაულის ერთ-ერთ ფორმას წარმოადგენს, რაც თავის მხრივ გულისხმობს მართლსაწინააღმდეგო ქმედებას, რომელიც ადამიანთა ჯგუფის მიერ ხორციელდება არა ერთჯერადად, არამედ დროის გარკვეული პერიოდის განმავლობაში. დანაშაულის ჩადენა წარმოადგენს მუდმივ საერთო საქმეს ორგანიზებული სუბიექტებისთვის, რომელთა შორის თითოეულს გააჩნია საკუთარი ფუნქციონალური ვალდებულებები, „უფლებები და მოვალეობები“. ტრანსნაციონალურ დანაშაულს 4 ძირითადი თვისება ახასიათებს, რომელთაგან მეოთხე, სახელმწიფო საზღვრების იგნორირება, მას სხვა სახის ორგანიზებული დანაშაულებისგან გამოარჩევს. ეს თვისებებია:

1) ორგანიზაციის არსებობა ან მასში მონაწილეობა

2) უწყვეტობა

3) საქმიანობის მიზნად მოგების მიღების დასახვა

4) მისი მიღწევის ხერხები, რომლებიც ეყრდნობა სახელმწიფო საზღვრების იგნორირებას.

იმ დროს, როდესაც ხდება ტრანსნაციონალურ და კიბერდამნაშავეთა ურთიერთგადაკვეთა, საქმე გვაქვს გლობალურ მასშტაბზე გათვლილ დანაშაულებრივ სქემასთან.

სწორედ, ერთ-ერთი ასეთი კომპლექსური ტრანსნაციონალური კიბერდანაშაულის შემთხვევაა „GozNym“-ის მავნე პროგრამის გამოყენება აშშ-სა და მსოფლიოს სხვადასხვა ქვეყანაში მცხოვრები ადამიანებისთვის საბანკო ანგარიშებიდან 100 მლნ. აშშ დოლარის მოსაპარად. „GozNym“-ი მიეკუთვნება ეგრეთ წოდებული „ტროიანის“, იგივე „ტროას ცხენის“ მავნე პროგრამას. „ტროიანი“ ისეთი მავნე კომპიუტერული პროგრამაა, რომელიც ერთი შეხედვით უვნებლად გამოიყურება, ან თავს ინიღბავს ყველასთვის კარგად ცნობილ პროგრამად; რამდენადაც მომხმარებლები ცნობილი პროგრამების ინსტალირებას არ ერიდებიან, ისინი საკუთარი ნებით საშუალებას აძლევენ „ტროას ცხენს“ მათ კომპიუტერულ სისტემაში შესვლის. აღსანიშნავია, რომ მის მიზანი არაა საკუთარი თავის რეპლიკაცია, არამედ ჰაკერები მას იყენებენ, როგორც კომპიუტერული სისტემის დისტანციურ მართვის მექანიზმს (RAT -Remote Administration Tool).

„GozNym“-ი ორი მავნე პროგრამის ერთობლიობაა: „Gozi ISFB“ (ასევე ცნობილია, როგორც Ursnif) და „Nymaim“. „GozNym“–ს ჰაკერები იყენებენ ბანკების, ელექტრონული კომერციის პლატფორმების, საკრედიტო კავშირებისა და სხვა ბიზნეს ანგარიშებიდან ფულის მოსაპარად. ეს მავნე პროგრამა განსაკუთრებით საშიშია, რადგან მას შეუძლია თავიდან აიცილოს ანტივირუსული პროგრამების ეფექტი. უამრავი ადამიანი იყენებს ერთი და იგივე პაროლს მრავალი ანგარიშისთვის. ამიტომ, საბანკო ანგარიშის გატაცებისა და მთელი პროფილის

შემოწმების შემდეგ, კიბერ დამნაშავეებმა შესაძლოა ასევე მიიღონ წვდომა მსხვერპლთა ელ. ფოსტის მისამართებზე და საბოლოოდ, სხვა პირად ანგარიშებზე.

აღნიშნული დანაშაულებრივი ქსელი და მისი ლიდერი, ზედმეტსახელად „None"-ი, რომელიც პროკურატურის ცნობით ეროვნებით ქართველია, ახორციელებდა ათასამდე კომპანიის კომპიუტერულ სისტემაში უნებართვო შეღწევას, კომპიუტერული სისტემიდან კომპიუტერული მონაცემების უნებართვოდ მოპოვებასა და მათი უკანონოდ შენახვა-გავრცელებას, კომპიუტერული მონაცემისა და კომპიუტერული სისტემის უკანონოდ გამოყენებას. აღნიშნული გლობალური დანაშაულებრივი ქსელის მსხვერპლი 41 000-ზე მეტი კომპანია გახდა.

დაჯგუფებამ მომხმარებლების კომპიუტერი „GozNym"-ის ვირუსით დააინფიცირა, რითაც მათ წვდომა მოიპოვეს ინტერნეტ ბანკის მონაცემებზე, შემდეგ კი მოპარული თანხების ლეგალიზებას უცხოურ ბენეფიციარ ბანკებში არსებული ანგარიშების საშუალებით ახორციელებდნენ. დანაშაულებრივი ქსელის ფორმირება იატაკქვეშა რუსულენოვან ინტერნეტ ფორუმებზე მოხდა, სადაც ჰაკერებმა ჯგუფში მოსახვედრად საკუთარი ტექნიკური შესაძლებლობები გამოიყენეს. დაზარალებულები ფიქრობდნენ, რომ ინტერნეტში მარტივ ოპერაციას ახორციელებდნენ, რა დროსაც კიბერ დამნაშავეები მათ სენსიტიურ და პირად ინფორმაციაზე წვდომას იღებდნენ. დაზარალებულთა შორის სხვადასხვა ქვეყნის არაერთი იურიდიული თუ საქველმოქმედო ორგანიზაციაა.

შეერთებული შტატების ხელმძღვანელობით ჩატარებულ საერთაშორისო ოპერაციაში საქართველოს, უკრაინის, მოლდოვის, გერმანიისა და ბულგარეთის პროკურატურები მონაწილეობდნენ. საქმეში აქტიურად ჩაერთნენ საერთაშორისო ორგანიზაციები - „ევროჯასტი" და „ევროპოლი", რომელთა ინიციატივით არაერთი შეხვედრა დაიგეგმა და შედგა ჰააგაში. საერთაშორისო გამოძიების ფარგლებში ბრალი 10 პიროვნებას წარედგინა. საქმის გამოძიება 2 წლის განმავლობაში მიმდინარეობდა და მხოლოდ 2019 წლის მაისში გაიხსნა. პირი, რომელმაც ვირუსი ისე დაშიფრა, რომ ის ქსელში შესამჩნევი არ ყოფილიყო, მართლმსაჯულების წინაშე მოლდოვაში წარდგა. თუმცა დღემდე ქსელის რამდენიმე წევრი კვლავ ძებნაშია.

ნებისმიერი კიბერდანაშაულის შემთხვევა განსაკუთრებით კი გლობალური, ტრანსნაციონალური კიბერდანაშაულები, კარგად გვიჩვენებს, თუ როგორი საფრთხის წინაშე დგას ნებისმიერი ჩვენგანი ციფრულ ტექნოლოგიასთან და სოციალურ ქსელებთან გადაჯაჭვული ცხოვრების გამო, რაც დღევანდელობის განუყოფელი ნაწილია. ყოველი ახალი შემთხვევა საჭიროა იყოს ჩვენთვის მაგალითი იმისთვის, რომ გამოვიჩინოთ უფრო მეტი სიფრთხილე ინტერნეტ სივრცეში ყოფნის დროს, რათა არ გავხდეთ უნებლიედ თუ „ჩვენივე ნებით" ჰაკერებისა და მავნე პროგრამების მორიგი მსხვერპლი.

## ბიბლიოგრაფია


1. „GozNym virus removal guide“ Written by Tomas Meskauskas on 03 September 2019
2. „GOZNYM MALWARE: CYBERCRIMINAL NETWORK DISMANTLED IN INTERNATIONAL OPERATION“ 16 MAY 2019
3. „Cybercrime Gang Behind GozNym Banking Malware Dismantled“ May 16, 2019
4. “კრიმინოლოგია და სამართლებრივი სისტემა საქართველოში” მთავარი რედაქტორი: გიორგი ღლონტი; თინათინ წერეთლის სახელმწიფოსა და სამართლის ინსტიტუტი 2008წ.

**Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 75 – 79 ISSN 2587-4667**
**Scientific Cyber Security Association (SCSA)**

# BLOCKCHAIN TECHNOLOGY AND PERSONAL PRIVACY ISSUES

Iryna Dmytrieva[1], Oleksandr Oksiiuk[2]
[1]Taras Shevchenko University of Kyiv, Faculty of Information Technology, [2]Taras Shevchenko University of Kyiv, Faculty of Information Technology

**ABSTRACT:** Blockchain technology has gone from prominence in a narrow circle of enthusiasts to mass insanity and frustration. The time has come to take a look at the trends in the development of technology and soberly assess the capabilities of the blockchain after the hype has stopped. Now blockchain finds application in areas such as financial transactions, user identification, or the creation of cybersecurity technologies. Despite the fact that blockchain technology is reliable and supportive, the privacy issues and challenges of this technology cannot be left out.

**KEYWORDS***: privacy, blockchain technology, data security, zk-SNARK, online threats*

## 1. The brief introduction to blockchain

Back in 1991, research scientists S. Haber and W. Scott Stornett described blockchain technologies for solving the security of digital documents with a timestamp so that they could not be faked or framed retroactively.

The system used a cryptographically secured chain of blocks to store documents with a time stamp, and in 1992 Merkle trees were included, and thus, this made the chain of blocks more efficient. However, this technology was not used, and the patent was lost in 2004 [1].

Nevertheless, in 2009, the concept of blockchain again made itself felt, not only as a bitcoin but also expanding its use in other areas. Blockchain, as a distributed database, turned out to be not only an excellent platform for cryptocurrency management, but also interested specialists from other fields, and especially the information security sphere, since this technology allows for more secure transactions, eliminates certain hacker attacks, and in some cases even eliminates the need for passwords [2].

## 2. Positive side of blockchain technology

Blockchain has become an almost ideal tool for ensuring security, storage, and confirmation of data. This technology is the result of many years of achievements in cryptography and information security. The already implemented use of the blockchain is its use in cryptography since this technology allows you to transfer information in a safe way. Blockchain is also used to prevent data manipulation, because the nature of the blocks is unchanged, using sequential hashing along with cryptography in a decentralized structure, it becomes possible to build a system that is almost impossible to manipulate [3].

Among the undeniable advantages of this technology stands out:

- resolving an intermediary attack,
- immunity to data manipulation,
- immunity to DDoS attacks.

### 2.1 Resolving an intermediary attack

Intermediary attack (Man-in-the-Middle (MITM)) is the name of the attack when users are fraudulently offered through the certification authority (CA) fake public keys, the use of which can lead to the disclosure of confidential data. One solution to this problem is the ability to put the

public key in the published block, which will make the key unchanged. As a result, it will be very difficult for potential attackers to publish fake keys and prove their authenticity. In addition, the certification authority will also be distributed, and disabling the service will become virtually impossible.

### 2.2 Immunity to data manipulation

Each blockchain-based transaction is distributed between nodes. In other words, each node that confirms the transaction receives a copy of the confirmed information. This means that no one can change the data and go unnoticed.

This prevents many problems, including data manipulation, which can be crucial in some industries, such as healthcare. Using the blockchain, it became almost impossible to engage in fraud in medical insurance or fake records.

### 2.3 Immunity to DDoS attacks

In recent years, DDoS attacks have become one of the largest online threats from which numerous websites and systems have suffered. However, if domain name systems (DNS) were based on blockchain technology, it would be much more difficult to carry out such attacks. The system would receive additional protection, become more transparent, and the DNS infrastructure would be distributed.

## 3. Blockchain technology and personal privacy issues

One of the main distinguishing features of blockchain technology is transparency. It is necessary for conducting online transactions without hiding any details, for which crypto aesthetes praise this technology. However, as soon as alternative options for using the blockchain appeared, it became clear that transparency was not always useful, especially when exchanging data.

Transactions on the blockchain are conducted publicly, everyone can view them at any time. This means that the data is not encrypted and accessible to everyone. This is not always convenient - in particular when it comes to confidentiality, be it financial information or medical records.

Of course, such solutions as storing exclusively encrypted data were proposed, but there are drawbacks. For example, the loss of a decryption key can lead to a complete loss of data. Finding it is also a problem: data can again be made available to everyone if the key is published on the Internet.

Confidentiality in blockchain technology is an aspect that still needs a lot of refinement. Despite the fact that the security of the blockchain is significantly improved compared to other systems, with respect to confidentiality, it is significantly lame. However, there is a solution. One of them - zk-SNARK (evidence with zero disclosure), which has already been used by Ethereum and Zcash - gives users the ability to make anonymous payments, vote anonymously, and also has a number of other advantages.

### 3.1 zk-SNARK technology

When people in the cryptocurrency sphere say “evidence of zero knowledge”, they usually refer to a certain type of evidence - zk-SNARKs. With it you can completely hide all the data: from

which address the payment went, where it came from and how much money was transferred. It also allows you to prove that the transaction has really passed and that the correct amount is on the account of the recipient [4].

When you hear about zero-knowledge proofs, most likely, we are talking about their one specific kind - zk-SNARKs. The basis of these protocols is a complex mathematical apparatus, but you cannot go into it if you do not implement this solution yourself.

Zk stands for zero-knowledge. SNARK – succinct non-interactive adaptive argument of knowledge [5].

Succinct means effective enough to be calculated in a short period of time. This is extremely important when conducting verification.

Non-interactive means that SNARKs do not require Verifier to directly poll Prover. The last one can publish his evidence in advance, and the verifier will verify its authenticity. Imagine that your teacher is asking you an arithmetic problem. After you have solved it, you do not submit the work. Instead, zk-SNARKs prove to the teacher that your result is correct. So far, everything looks very simple, but it's worth a couple of reservations [9].

SNARKs require large computing power. Often they lack the resources of mobile devices. Recently, however, some promising advances have been observed in this regard.

There is also the problem of losing access to the hash function, on the basis of which authentication is verified. SNARK technology allows the user to prove that he has access to a certain secret, but that must ensure its safety and accessibility.

The biggest drawback of SNARKs is the so-called installation phase.

### 3.2 Installation phase

This step is a necessary part of introducing SNARK protocols into any task. The authenticity of the calculation is fixed on it (the so-called circuit), the result of which you want to prove. Due to this limitation, SNARK protocols are poorly suited for arbitrary Turing-complete smart contracts - each new contract will require a new installation. Each of the tasks set by your teacher will require its own installation phase [6]. For example, one phase will be required for the operation of addition or multiplication.

The installation phase has another important aspect. It is at this stage that a secret is created, the existence of which allows the publication of fake proofs. In a system with two participants (teacher-student) this is permissible - the verifier (your teacher) creates a secret, and security is ensured until he shares the secret with you.

If you want to use some circuit publicly, that is, with more than one verifier, you must have a "trusted setup". In this case, the secret will be generated not by one person (which, incidentally, is obliged to destroy it immediately), but by a group of users. If all members of the group adhere to the rules (delete sensitive data), the security of the exchange is guaranteed [10].

### 3.3 How does it work?

The math underlying zk-SNARKs is hard to understand. Only a couple hundred people actually understand how this protocol works, but let's try to give analogies to understand how this system works.

Imagine that you meet someone on the street, and he claims to know your cat - she is stuck in a tree yard, and you need to urgently go with him to save her. You worry about your cat, but at the

same time you feel some kind of distrust. You need to make sure that this stranger is, in fact, a neighbor whom you can trust. Therefore, you ask questions to which he must know the answer, if you really saw your cat. Assuming you are asking the right questions, the protocol you just came up with is an example of proof of zero knowledge. You, the verifier, verify that the stranger or prover really saw your cat. You do this interactively, coming up with questions that are difficult to prepare in advance, and as much as is necessary to confirm the event. That's all. The proof of zero knowledge is when the prover convinces the verifier that he has secret knowledge without revealing this knowledge directly to the verifier.

### 3.4 Anonymity and Authenticity Elections

The decision-making process has always been one of the most important components of the development of any community. One form of finding an option that suits everyone is voting. It is acceptable to most people under the following basic conditions: votes must be counted impartially. Most often, uninterested parties are involved for this, or it is possible to check the correctness of the calculation on individual samples [7]. Another important characteristic of voting is the anonymity of the participants.

At first glance, it seems that these are conflicting concepts. There is some truth to this: compliance with anonymity complicates the provision of verification. This is where Zero Knowledge Proof will help us [8]. It allows you to verify the correctness of the calculation without disclosing personal information.

## Conclusions

Now that online threats continue to emerge almost daily, it’s important to develop a strong and secure system, such as blockchain. Of course, the blockchain will not become a panacea, since there is no universal solution. Especially if you consider this technology from the side of personal safety.

## REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

[2] G. Zyskind, O. Nathan et al., Decentralizing privacy: Using blockchain to protect personal data, in Security and Privacy Workshops (SPW), 2015 IEEE, IEEE, 2015, 180–184.

[3] O. J. Onyigwang, Y. Shestak and A. Oksiuk, "Information protection of data processing center against cyber attacks," *2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP)*, Lviv, 2016, pp. 397-400. doi: 10.1109/DSMP.2016.7583586

[4] Jens Groth. “Short pairing-based non-interactive zero-knowledge arguments”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2010, pp. 321–340.

[5] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, Madars Virza. *Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture*. Cryptology ePrint Archive, Report 2013/879. https://eprint.iacr.org/2013/879. 2013.

[6] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. *Quadratic Span Programs and Succinct NIZKs without PCPs*. Cryptology ePrint Archive, Report 2012/215. https://eprint.iacr.org/2012/215. 2012.

[7] Jens Groth, Markulf Kohlweiss, Mary Maller, Sarah Meiklejohn, and Ian Miers. *Updatable and Universal Common Reference Strings with Applications to zk-SNARKs*. Cryptology ePrint Archive, Report 2018/280. https://eprint.iacr.org/2018/280. 2018.

[8] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. *Scalable, transparent, and post-quantum secure computational integrity*. Cryptology ePrint Archive, Report 2018/046. https://eprint.iacr.org/2018/046. 2018.

[9] Mary Maller, Sean Bowe, Markulf Kohlweiss, and Sarah Meiklejohn. *Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updateable Structured Reference Strings*. Cryptology ePrint Archive, Report 2019/099. https://eprint.iacr.org/2019/099. 2019.

[10] O. Oksiiuk, L. Tereikovska and I. Tereikovskiy, "Adaptation of the neural network model to the identification of the cyberattacks type "denial of service"," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 502-505. doi: 10.1109/TCSET.2018.8336251

**Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 80 – 86 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# МЕТОДИКА ПРОВЕДЕНИЯ ДИАГНОСТИРОВАНИЯ КИБЕРНЕТИЧЕСКОЙ СТОЙКОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

**д.т.н., профессор Забара Станислав Сергеевич,**
Институт компьютерных технологий Открытого международного университета развития человека «Украина», г. Киев, Украина
**д.т.н., профессор Хлапонин Юрий Иванович,**
Киевский национальный университет строительства и архитектуры, г. Киев, Украина
**Козубцова Леся Михайловна,**
Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина

**АННОТАЦИЯ.** В статье проанализированы известные попытки решений научной задачи расчета кибернетической стойкости информационной системы специального назначения. Установлено, что на данное время существующие решения не учитывают при расчете кибернетической стойкости активное действий деструктивных информационных влияний, а результат носит статический характер, который отображает состояние составных системы политике безопасности. Безусловно этого недостаточно для оценки реального состояния. В результате этого возникла необходимость в разработке методики диагностирования, которая бы обеспечивала расчет кибернетической стойкости информационной системы специального назначения по результатам активных кибернетических действий. Предложен математический аппарат методики обеспечивает расчет кибернетической стойкости информационной системы специального назначения для модели наихудшего варианта, для так называемого наступления события угрозы нулевого дня.

**Практическое значение и применение** заключается в практичной возможности определения уровня кибернетической стойкости информационной системы специального назначения с учетом активных действий деструктивных информационных влияний на стадии проектирования и эксплуатации системы.

**Научная новизна.** Научная новизна полученного результата заключается в том, что предложено решение научно-практической задачи расчета кибернетической стойкости информационной системы специального назначения с учетом активных действий деструктивных информационных влияний угрозы нулевого дня.

**КЛЮЧЕВЫЕ СЛОВА**: методика, оценка, кибернетическая стойкость, защищенность, надежность, живучесть, информационная система специального назначения, деструктивное информационное влияние.

# METHODS FOR DIAGNOSING CYBERNETIC STABILITY OF A SPECIAL PURPOSE INFORMATION SYSTEM

**doctor of technical Sciences, Professor Stanislav Zabara,**
Institute of computer technologies of the Open international University of human development "Ukraine", Kiev, Ukraine
**doctor of technical Sciences, Professor Yuri Khlaponin,**
Kiev national University of construction and architecture, Kiev, Ukraine
**Lesya Kozubtsova,**
Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine

**ABSTRACT.** The article analyzes well-known attempts to solve the scientific problem of calculating the cybernetic stability of a special-purpose information system. It is established that at this time, existing solutions do not take into account the active actions of destructive information influences when calculating cybernetic stability, and the result is static, which reflects the state of the components of the security policy

system. Of course, this is not enough to assess the real state. As a result, it became necessary to develop a diagnostic technique that would provide a calculation of the cybernetic stability of a special-purpose information system based on the results of active cybernetic actions. The mathematical apparatus of the method provides calculation of cybernetic stability of a special-purpose information system for the worst-case scenario model, for the so-called zero-day threat event.

The practical significance and application lies in the practical possibility of determining the level of cybernetic stability of a special-purpose information system, taking into account the active actions of destructive information influences at the stage of design and operation of the system.

Scientific novelty. The scientific novelty of the result is that a solution to the scientific and practical problem of calculating the cybernetic stability of a special-purpose information system is proposed, taking into account the active actions of destructive information influences of the zero-day threat.

**KEYWORDS**: methodology, assessment, cybernetic stability, security, reliability, survivability, special-purpose information system, destructive information influence.

**ВВЕДЕНИЕ.** Информационные системы (ИС) применяются для решения широкого спектра научных и производственных задач сбора, обработки, накопления и хранения информации, управления критическими объектами в реальном масштабе времени. Эти задачи имеют актуальное значение в повседневной деятельности специальных пользователей. Для таких пользователей, которые решают эти задачи, информационные системы начали именовать, как информационные системы специального назначения (ИС СН) (рис. 1).

Функционирование ИС СН в новой среде – киберпространстве, порождает новые уязвимости и угрозы. Отсюда высокий уровень требований, предъявляемых к надежности информационных систем [1 – 4]: адекватность, оптимальность, оперативность, устойчивость, непрерывность, скрытность (рис. 2). Из множества перечисленных свойств процесса управления в диссертационном исследовании ограничимся рассмотрением устойчивостью. И как следствие, необходимо разработать новый инструментарий обеспечения безопасности ИС, под которой понимается состояние ее защищенности, что обеспечивает устойчивое функционирование в условиях действий деструктивных информационных воздействий (ДИВ).

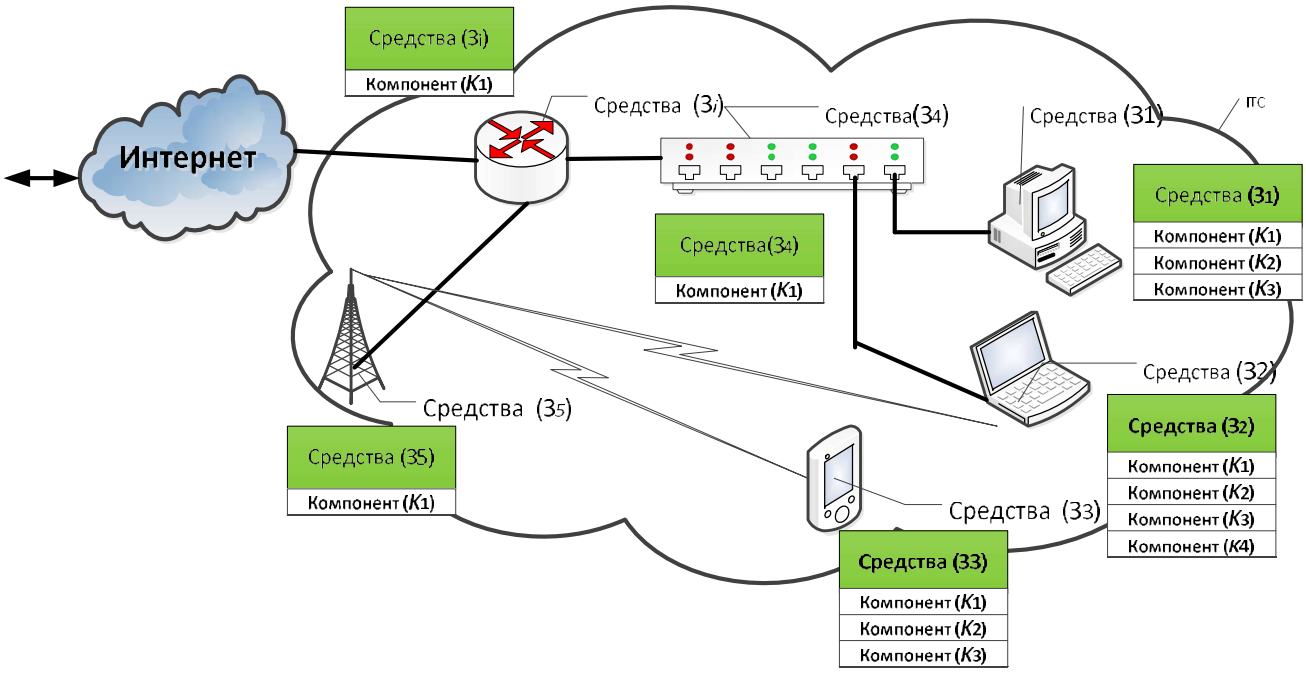


Рис. 1. Фрагмент информационной системы специального назначения

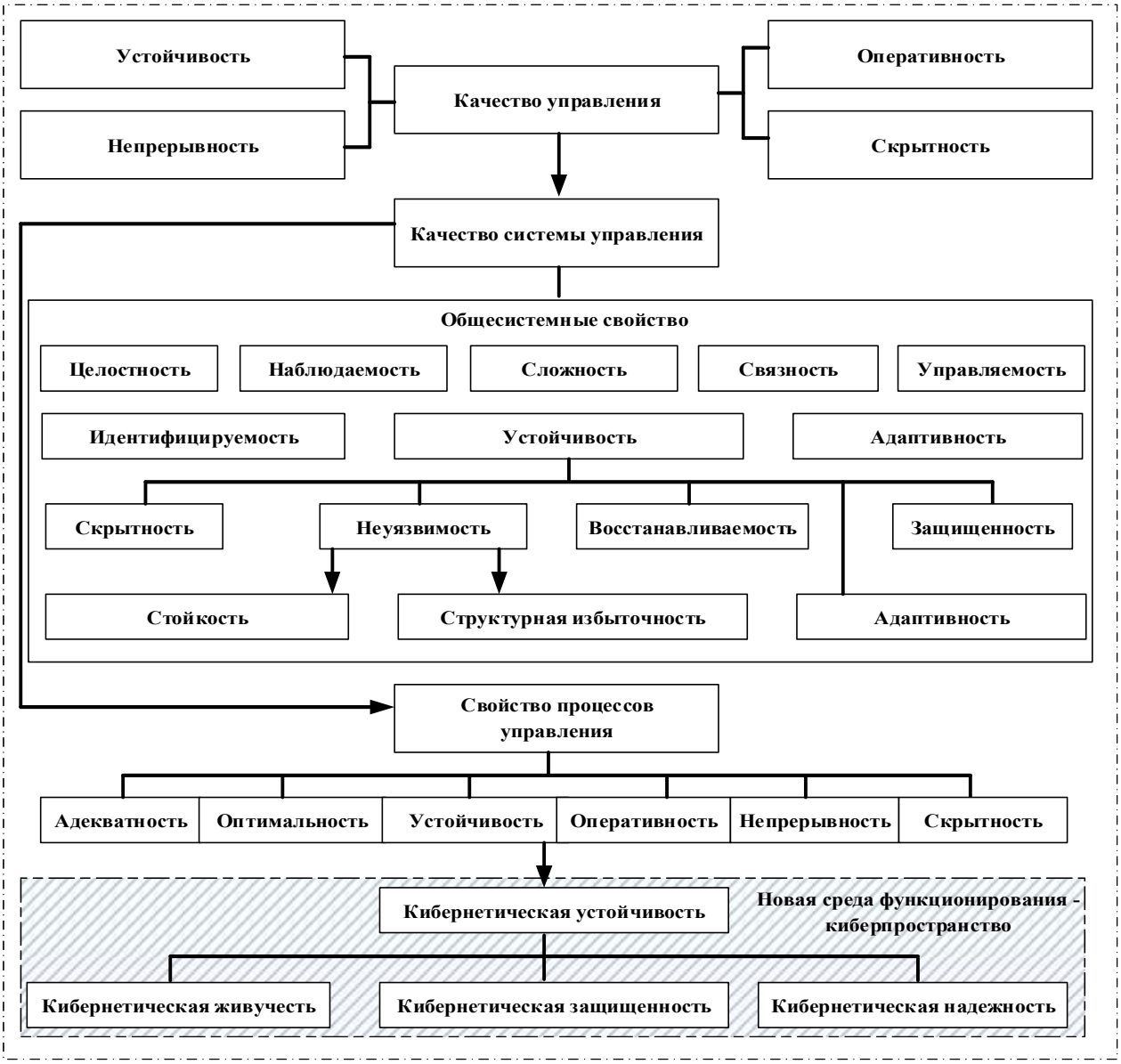



Рис. 2. Место понятия «кибернетическая устойчивость» в классификации

Согласно цели, объекта, предмета и определенного научного задания диссертационного исследования необходимо разработать методику диагностирования кибернетической устойчивости функционирования информационной системы специального назначения (ИС СН) в кибернетическом пространстве.

**Анализ последних исследований и публикаций по данному направлению.** Поиск в открытых источниках информации по ключевому слову «кибернетическая устойчивости ИС СН» дал возможность найти только понятие «кибернетическая устойчивости ИС», которое на первый взгляд тождественные «ИС СН», но это совсем не так.

В исследованиях [5 – 7] введено в употребление понятие киберустойчивости объекта критической информационной инфраструктуры (КИИ). В коллективной работе [8, с. 46] обосновано понятие «киберустойчивость объекта критической инфраструктуры (КИ).

В целом мы согласны с классификацией (рис. 2) предложенной в работах [5 – 8], тогда «кибернетическая устойчивость $P_{КС(S)}$ ИС СН» по классике состоит из следующих компонентов (1):

$$P_{КС(S)} = P_{КЖ(S)} \text{ x } P_{КН(S)} \text{ x } P_{КЗ(S)} \quad (1)$$

Где $P_{КЖ(S)}$ – кибернетическая живучесть, это вероятность сохранения ее работоспособности (выживания) в условиях выхода из строя технических средств обработки информации; $P_{КЗ(S)}$ – кибернетическая защищенность ИС СН, это вероятность обеспечения выполнения целевой функции ИС СН с заданным качеством в условиях применения «общих» и целенаправленных деструктивных информационных воздействий; $P_{КН(S)}$ – кибернетическая надежность ИС СН, это вероятность обеспечения выполнения целевой функции ИС СН на протяжении определенного временного интервала в условиях возникновения программных ошибок, технических сбоев и непреднамеренных ошибочных действий технического персонала и должностных лиц.

**Цель статьи.** Апробировать структуру методики диагностирования устойчивого функционирования кибернетической ИС СП в кибернетическом пространстве и зону ответственности участников эксперимента.

## ОСНОВНОЙ РЕЗУЛЬТАТ

**Методика диагностирования устойчивого функционирования кибернетической ИС СН в кибернетическом пространстве** включает следующие этапы:

Этап 1. Реализация мероприятий по категорированию и декомпозиции ИС СН на средства и компоненты (элементы) относительно уязвимых к деструктивных информационных воздействий.

Этап 2. Выбор мер кибербезопасности для каждого средства и компоненты (элемента) составляющих ИС СН.

Этап 3. Процедуры по реализации мер кибербезопасности на каждом средстве и компоненте (элементы) составляющих ИС СН.

Этап 4. Диагностирование уровня достижения реализуемости процедур кибербезопасности на каждом средстве и компоненте (элементы) составляющих ИС СН в соответствии с мероприятий.

Этап 5. Расчет показателя устойчивости функционирования кибернетической ИС СН в кибернетическом пространстве. (**Методика расчета составляющих показателя кибернетической устойчивости функционирования ИС СН в кибернетическом пространстве).**

Для наглядности единства разработанных уточняющих методик, которые позволяют рассчитать необходимые компоненты кибернетической устойчивости функционирования ИС СН по результатам диагностирования, представлено в виде блок-схемы (см. рис. 3).

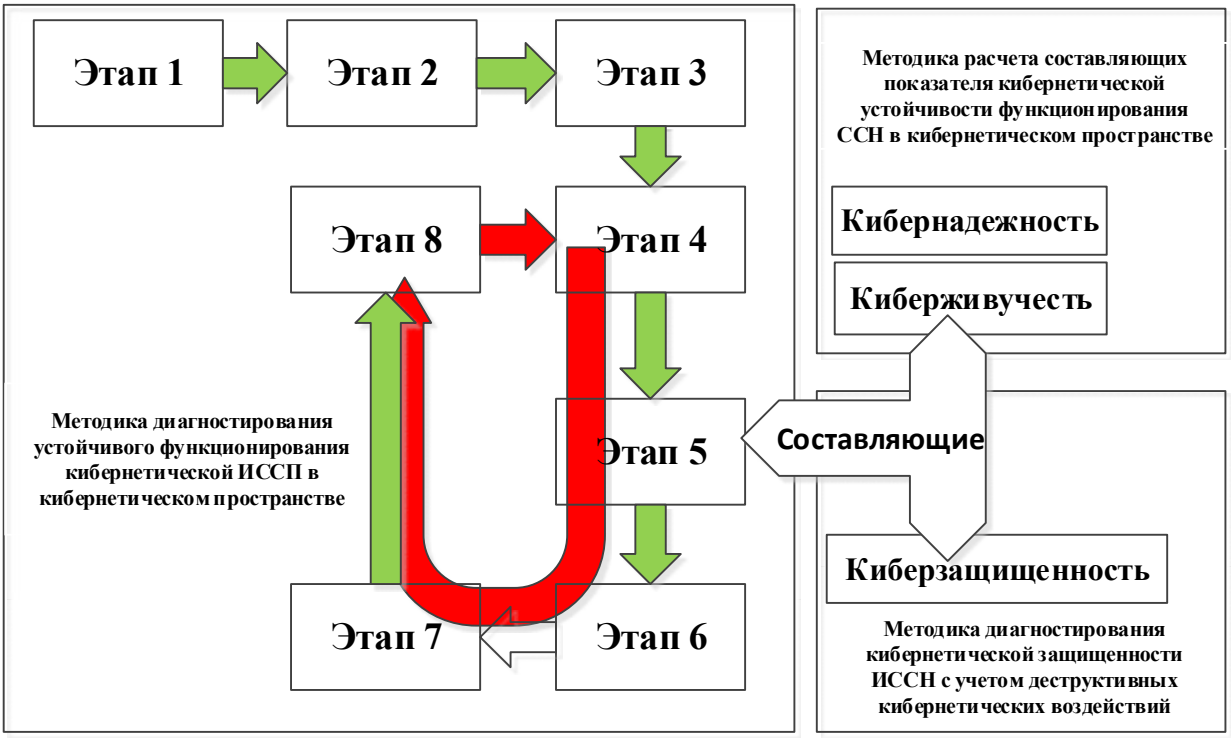


Рис. 3. Бока-схема методики диагностирования кибернетической устойчивого функционирования ИС СН в кибернетическом пространстве

Вычисление основывается на методике расчета составляющих показателя устойчивости функционирования кибернетической ИС СН в кибернетическом пространстве и в общем виде методика представлена следующими этапами:

Этап 5.1. Диагностирование и расчет кибернетической защищенности $P_{КЗ(S)}$ ИС СН [9; 10].

Этап 5.2. Расчет кибернетической надежности $P_{КН(S)}$ ИС СН.

Этап 5.3. Расчет кибернетической живучести $P_{КЖ(S)}$ ИС СН.

Этап 5.4. Расчет кибернетической устойчивости $P_{КС(S)}$ функционирования ИС СН.

Этап 6. Обработка, анализ и оценка результатов диагностирования кибернетической устойчивости функционирования ИС СН в кибернетическом пространстве.

Этап 7. Отработка (представления) практических рекомендаций по дальнейшей безопасной эксплуатации ИС СН в кибернетическом пространстве.

Этап 8. Эпизодический (внезапный) мониторинг ИС СН в рамках этапов 4-7.

Методика апробирована в работе [11].

**Методика расчета составляющих показателя кибернетической устойчивости функционирования информационной системы специального назначения в кибернетическом пространстве** включает следующие этапы:

В общем виде методика расчета составляющих показателя кибернетической устойчивости представлена следующими этапами:

Этап 1. Сбор и анализ исходных данных необходимых для расчета кибернетической устойчивости функционирования ИС СН.

Этап 2 Расчет кибернетической устойчивости ($P_{КС(KjZi)}$) функционирования компонента ($K_j$), который есть составляющей средства ($Z_i$) ИС СН.

Этап 2.1 Диагностирование и расчет кибернетической защищенности ($P_{КЗ(KjZi)}$) компонента ($K_j$), который есть составляющей средства ($Z_i$) ИС СН в соответствии [9; 10].

Этап 2.2 Расчет надежности кибернетической ($P_{КН(KjZi)}$) компонента ($K_j$), которая есть составляющей средства ($Z_i$) ИС СН.

Этап 2.3 Расчет кибернетической живучести **(**$P_{КН(KjZi)}$**)** компонента ($K_j$), которая есть составляющей средства ($Z_i$) ИС СН. Этап 2.4 Расчет кибернетической устойчивости ($P_{КС(KjZi)}$) функционирования компоненты ($K_j$) со склада средства ($Z_i$) ИС СН.

Этап 3 Расчет кибернетической устойчивости ($P_{КС(Zi)}$) функционирования средств ($Z_i$) ИС СН.

Этап 3.1 Диагностирование и расчет кибернетической защищенности ($P_{КЗ(Zi)}$) каждого средства ($Z_i$) ИС СН рассчитывается в соответствии [9; 10].

Этап 3.2 Расчет кибернетической надежности ($P_{КН(Zi)}$) каждого средства ($Z_i$) ИС СН.

Этап 3.3 Расчет кибернетической живучести ($P_{КЖ(Zi)}$) в пределы состояний каждого средства ($Z_i$) ИС СН.

Этап 3.4 Расчет кибернетической устойчивости ($P_{КС(Zi)}$) функционирования средства ($Z_i$) ИС СН.

Этап 4 Расчет кибернетической устойчивости ($P_{КС(S)}$) функционирования ИС СН.

Этап 4.1 Расчет кибернетической защищенности ($P_{КЗ(S)}$) ИС СН в целом рассчитывается в соответствии [9; 10].

Этап 4.2 Расчет кибернетической надежности **(**$P_{КН(S)}$) ИС СН в целом.

Этап 4.3 Расчет кибернетической живучести ($P_{КЖ(S)}$) ИС СН в целом.

Этап 4.4 Расчет кибернетической устойчивости ($P_{КС(S)}$) ИС СН в целом.

Этап 5. Обработка, анализ и оценка результатов диагностирования кибернетической устойчивости функционирования ИС СН в кибернетическом пространстве. Формализация результатов.

Методика подготовлена и проходит предварительную апробацию, поэтому является предметом дальнейшее публикации.

**Методика диагностирования кибернетической защищенности информационной системы с учетом деструктивных кибернетических воздействий** включает следующие этапы:

Этап 1. Реализация мероприятий по категоризации и разложения ИС СН на компоненты и элементы уязвимости кибернетического воздействия

Этап 2. Расчет показателей $P_{КЗ(KjZi)}$ кибернетической защищенности каждого компонента ($K_j$),

который есть составляющей средства ($Z_i$) ИС СН.

Этап 3. Вычисления показателя $P_{КЗ(Zi)}$ каждого средства ($Z_i$) со склада ИС СН.

Этап 4. Расчет $P_{КЗ(S)}$ кибернетической защищенности ИС СН в целом.

Этап 5. Обработка, анализ и оценка результатов испытаний.

Методика многократно апробирована, а именно при оценке кибернетической защищенности системы связи организации [9] и информационно-телекоммуникационной системы [10].

**Особенности практической реализации обобщенной методики.**

1 Состав группы экспериментального диагностирования кибернетической устойчивого функционирования ИС СП в кибернетическом пространстве

1) Руководитель комиссии группы специалистов с кибербезопасности.

2) группы специалистов с кибербезопасности по направлениям и ответственности:

группа №1 фиксирования изменений состояния функционирования ИС СН;

группа №2 кибернетического влияния на ИС СН – отработки кибернетических действий в роли «хакера»;

группа №3 математического расчету кибернетической стойкости ИС СН – рассчитывают все параметры на всех этапах испытаний;

группа №4 условны пользователи (АРМ) ИС СН – осуществляют фиксирование передачи голосовых, текстовых, графических данных, потока видеоданных.

Порядок взаимодействия участников испытаний по данной методике:

специалисты контроля и фиксирования непосредственно с группой расчета;

руководитель испытаний через команду осуществления кибернетического влияния с условным хакером.

Запрещается лицам, которые осуществляют кибернетическое влияние (№2) сообщать начало наступления события кибернетического влияния группе №1.

**ВЫВОДЫ.**

Важнейшими научными и практическими результатами являются:

1. Усовершенствована методика диагностирования кибернетической устойчивости функционирования информационной системы специального назначения в кибернетическом пространстве. Методика основывается на введении отдельного этапа вычисления кибернетической устойчивости функционирования информационной системы специального назначения. В предложенной методике, в отличие от известных, предложена декомпозиция ИС СН на отдельные средства и компоненты по критериям конфиденциальности, целостности и доступности. Это позволило обеспечить более качественный отбор компонентов информационной системы специального назначения по критерию уязвимости деструктивным информационным воздействием.

2. Усовершенствована методика расчета составляющих показателя кибернетической устойчивости функционирования информационной системы специального назначения в кибернетическом пространстве. Методика основывается на расширении свойств кибернетической устойчивости, что является интегральным показателем кибернетической защищенности, надежности и живучести. Необходимость введения нового свойства вызванная новой средой функционирования информационной системы специального назначения в киберпространстве. Применение нового типа оружия – кибернетического оружия создает деструктивные информационные воздействий, которые нарушают нормальное функционирование системы.

3. Усовершенствована методика диагностирование кибернетической защищенности информационной системы специального назначения. В предложенной методике, в отличие от известных, предложено рассчитать оценку кибернетической защищенности информационной системы специального назначения на некоторый момент времени $t_{ДИВ}$, в который осуществляется активное деструктивное информационное влияние на эту систему $F_{ДИВ} = 1$ с целью прогнозирования и предотвращения потерять некоторых актив (Ак). Математический аппарат методики обеспечивает расчет кибернетической защищенности информационной системы специального назначения для модели наихудшего варианта наступления события угрозы нулевого дня.

## СПИСОК ЛИТЕРАТУРЫ

[1] Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 296 с.
[2] БоговикА.В., Игнатов В.В. Теория управления в системах военного назначения. СПб.: ВАС, 2008. 460 с.
[3] Давыдов А.Е., Савицкий О.К., Максимов Р.В. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. Москва: Воентелеком, 2015. 520 с.
[4] Шолудько В.Г., Єсаулов М.Ю., Вакуленко О.В., Гурський Т.Г., Фомін М.М. Організація військового зв'язку : навчальний посібник. К.: ВІТІ, 2017. 282 с.
[5] Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. №2. С. 52 – 61.
[6] Минаев В.А., Крупенин А.В., Королев И.Д., Бондарь К.М., Захарченко Р.И. Оценка устойчивости функционирования критической информационной инфраструктуры // «Вестник РосНОУ», серия «Сложные системы: модели, анализ и управление». 2018. Вып. 4. Информатика и вычислительная техника. С. 129 – 138.
[7] Критическая информационная инфраструктура: оценка устойчивости функционирования / В.А. Минаев, И.Д. Королев, Е.В. Зеленцова, Р.И. Захарченко // Радиопромышленность, 2018. Т. 28. №4. С. 59 – 67.
[8] Гончар С.Ф., Герасимов Р.П., Ткаченко В.В. Дослідження проблеми кіберживучості Об'єднаної енергосистеми України // Міжнародний науково-теоретичний журнал «Електронне моделювання», 2019. Т.41. №1. С. 43 – 54.
[9] Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П Методика оцінки кібернетичної захищеності системи зв'язку організації // Сучасні інформаційні технології у сфері безпеки та оборони. 2018. №1(31). С. 43 – 46.
[10] Куцаєв В.В., Радченко М.М., Козубцова Л.М., Терещенко Т.П., Куцаєв В.В. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку // Збірник наукових праць ВІТІ. К.: ВІТІ, 2018. №2. С. 67 – 76.
[11] Козубцова Л.М. Апробація структури методики діагностування кібернетичної стійкості функціонування інформаційної системи спеціального призначення в кібернетичному просторі // Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" (17 березня 2020 року, м. Харків). Харків. Національна академія Національної гвардії України, 2020. С141 – 142.

**Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 87 – 92 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# ELIMINATING PRIVILAGE ESCALATION TO ROOT IN CONTAINERS RUNNING ON KUBERNETES

[1]Linetskyi Artem, [2]Babenko Tetiana, [3]Myrutenko Larysa, [4]Vialkova Vira
1-4 Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine
artem.linetskiy@gmail, babenkot@ua.fm, myrutenko.lara@gmail, veravialkova@gmail.com

**ABSTRACT:** containerization and orchestration tools like Kubernetes allow enterprises to automate many aspects of application lifecycle, especially deployment, significant business benefits. However, these new deployments are also vulnerable to attacks and introduce new exploits from hackers and insiders, making Kubernetes security a crucial component for every deployment. We perform a study analyzing privilege escalation to root in containers running on Kubernetes. Based on the results we create a solution that can eliminate this type of attack.

**KEYWORDS***: kubernetes; privilage escalation; cybersecurity*, *security layer.*

## I. INTRODUCTION

Lately, microservice based architecture has proven to be the most reliable and scalable approach to developing an application. With the popularity of small apps, the solution to maintain them was found - Kuberntes. Kubernetes is an orchestration tool that can easily manage thousands deployments and scale and container-based workload. With wide adoption by many organization and major cloud companies, it has exploded onto the technology scene over the last couple of years. Once Kubernetes has become the new industry standard, hackers and malicious organisations also did't miss the chance. Attacks for crypto mining, ransomware, service disruption and data stealing will continue to be launched in the new container based virtualized environments in both public and private clouds. In the recent days even such large company as Tesla was affected by hacker's interest to Kubernetes clusters. "The hackers had infiltrated Tesla's Kubernetes console which was not password protected," RedLock researchers wrote. "Within one Kubernetes pod, access credentials were exposed to Tesla's AWS environment which contained an Amazon S3 (Amazon Simple Storage Service) bucket that had sensitive data such as telemetry" [1,2].

## II. BACKGROUND

### *A. Kubernetes basics*

Kubernetes is tool, which automates the updates, deployment and monitors containers. Kubernetes is supported by all major container management and cloud platforms such as Red Hat OpenShift, IBM Cloud, AWS EKS and Google Cloud. Here are some of the key things to know about Kubernetes:

- **Master Node**. A server that manages the deployment of pods the Kubernetes worker node cluster.
- **Worker Node**. Servers that typically run the app containers or other Kubernetes components, they are also called slaves or minions sometimes.
- **Pods**. A single deployment and addressability unit in Kubernetes. A pod can have one or more containers and their own IP addresses.
- **Services.** A service functions as a proxy to its underlying pods and requests can be load balanced across replicated pods.
- **System Components.** Key components that are used to manage a Kubernetes cluster include the API Server, Kubelet, and etcd. Each of these components are the most likely targets for the attack.

### *B. Kubernetes Networking Basics*

Kubernetes' main concept in networking is that every pod has routable IP address (Fig. 1). Plug-ins for Kubernetes take care of routing requests internally between host machines to appropriate pods. Kubernetes pods can be accessed from outside only through a load balancer, service or ingress controller, which routes the traffic to the correct pod.

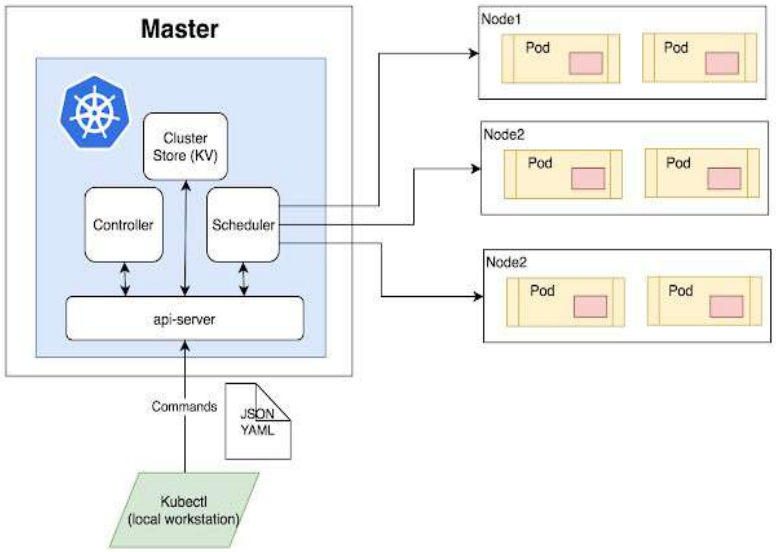



***Fig. 1.*** *Kubernetes architecture diagram*

DNAT and Load balancing help to make connections to the correct pod. Pods communicate with each other over the network overlay. Encapsulation is used for packets, where appropriate headers are added to get them to the appropriate destination, where the encapsulation is removed.

Having all that overlay, being dynamically handled by Kubernetes, it is extremely difficult to monitor network traffic, and even more difficult to secure it [3].

### *C. Container Inspection*

Attacks in containerized environments usually utilize malicious processes and privilege escalations to execute an attack or spread it. Exploits of vulnerabilities in the Linux kernel, libraries, packages, or applications can result in suspicious activity inside the container.

Each application in a container has a defined set of functions and it is built with only the needed libraries and packages, detecting suspicious file system activity and processes should be much more accurate.

Inspecting container file system activity, processes and suspicious behavior is crucial in container security. Reverse shells, port scanning or privilege escalations should all be detected at the beginning. Some of these detections should be built-in and also include a baseline behavioral learning process which can identify unusual processes based on previous activity [3].

## III. ESCALATION CAUSE ANALYSIS

Since every container running in Kubernetes is running on Docker, there's always a possibility of other libraries being compromised. Hence, "compromised container = compromised cluster" we should take seriously protection of Docker containers running on production grade environments like Kubernetes. The best and simplest security measure that could be taken is avoid running containers as root user. Let's break down why is it important.

### *A. Non-root containers*

When application is running on the host machine, it is normally understood why isolation between the root user and non-privileged users is required. If application is run as a root, if breached, it can easily wreak the system, by modifying system files, stopping or launching privileged processes and so on. A lot of Linux daemons remove privileges in the early setup stages, for example the Nginx daemon forks and runs as the unprivileged www-data user.

Containers have just simplified the privilege separation. Separate runtime is given to each container and it's isolated by Linux namespaces with a set of capabilities. Every application is run in a separate container, and can be considered to be safe to use in the container.

Therefore it has accidently become a common practice to run application with root user and most of the Docker images don't change to unprivileged user. However, a very important security layer is eliminated in such cases. It's even more true, considering that there's no real reasoning to why, such images should be run as root.

On the other hand, there are container platforms that run all their containers as unprivileged users by default. OpenShift is a great example, that only allows its users to use images with support for a random, non-root user.

Some containerized applications can remove root privilege, changing the root user to a non-privileged straight after the setup. This allows them to rely on file permissions, based on users and prevents access to sensitive information (e.g. configuration files, processes) in the containers. Such preventions, really limit the damage, that can be done to a compromised container. A great example of such design is Jenkins image. [4].

Nonetheless, using a non-root user in containers is a crucial security precaution to prevent container breakout.

In most container runtimes root user is shared between the host machine and containers. This is not a problem, because the container processes are sandboxed using Linux capabilities and Linux namespaces such as PID, net, mount and IPC. However, when kernel doesn't distinct the user or group IDs of the host and the container, vulnerabilities in the container, that exposes everything from the host to a container process, creates real trouble. Simply speaking, a container breakout is more likely to happen for processes running as root.

In this situation, any attacker's process will be able to change files on the system, without further escalating privileges to the root user. [5].

## IV. ROOT PRIVILAGES ESCALATION METHOD

Root-privilege escalation can be performed in a number of different ways. These are some of them:

- System libraries' (runC, libC) vulnerabilities exploitation
- Improper following of symbolic links
- Usage of same volumes for different containers
- Go programming language vulnerabilities
- Docker vulnerabilities
- Default unsecure configuration problem
- Natively Kubernetes security issues

In this particular case we'll look at root privilege escalation using known Kubernetes vulnerability in kubelet v1.13.6 and v1.14.2. This versions are still broadly used by both cloud providers and on-premise deployments.

### A. *So What Is Kubelet?*

**Kubelet** is an agent, that's present on every Kubernetes server. Kubelet takes a PodSpec which is a description of pod resource. PodSpec is usually described in a form of a YAML file. Kubelet makes sure that every file with pod description is successfully transformed into a healthy running pod.

### B. *Exploitation process*

Every container that is deployed in Kubernetes environment is usually created with a user that is specified in the respective Dockerfile. Hovewer, Kubernetes includes native handling for this and gives a possibility to specify a user in PodSpec file or configure the container to avoid running as root user. So the regular behavior is for Kubernetes to start the container with user in the dockerfile if nothing else was specified in PodSpec (like *runAsUser: <uid>* or *mustRunAsNonRoot:true).* But sometimes the image can be run as root instead. These are some of the scenarios:

- explicitly specified *runAsUser* pods are unaffected and continue to work properly
- *runAsUser* setting that is forced by *podSecurityPolicies* keeps containers unaffected and works properly
- If *mustRunAsNonRoot:true* is specified, the container will refuse to start as uid 0, this can affect availability
- If *runAsUser* or *mustRunAsNonRoot:true are not specified, pods* will run as uid 0 on restart or if the image was pulled to the node previously

### C. *Steps to reproduce*

In order to reproduce this issue, security analyst or malicious user needs to have access to pod resources and ability to create them in the cluster. He can have access to any given namespace. To reproduce this problem minikube will instance will be created (Fig 2)

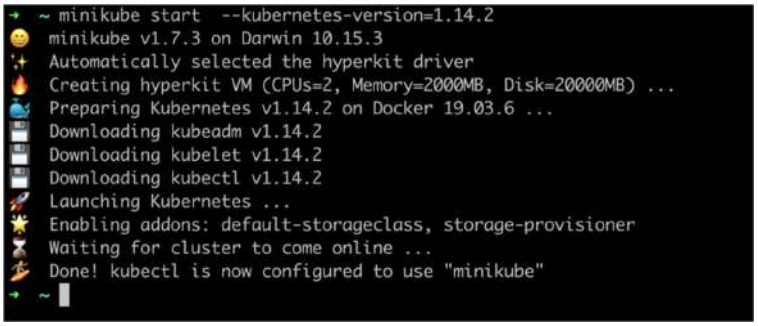



***Fig. 2.*** *Minikube instance creation process*

After environment for reproduction is ready, we need to prepare a test pod resource YAML file. Example of a YAML file (Fig 3):


***Fig. 3.*** *Example of exploit YAML file*

It's a simple pod resource that has a base image of memcached:latest, which has it's process run as memcached user. Snippets of Dockerfile confirming that (Fig 4, Fig 5):

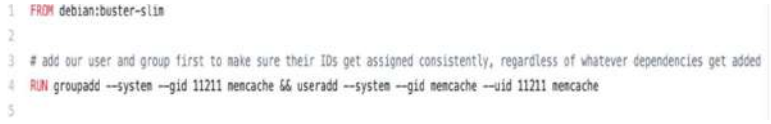



***Fig.4.*** *First snippet of memcached Dockerfile*

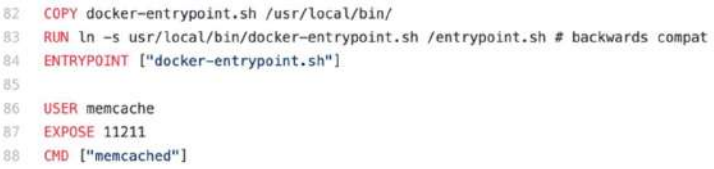



***Fig.5.*** *Second snippet of memcached Dockerfile*

So, it's clear that the container should be executed with memcache user, specified in the Dockerfile. According to the reproduction steps, if the container will restart, next time it will be executed with uid 0, the command with args in the Pod YAML file simulates just that. It displays the uid of the user that container is running under and then waits 30 seconds and restarts. After the restart it should be executed by root. The proof of this concept is available on Fig 6.

***Fig. 6.*** *Proof of exploit*

The container was restarted 2 times and according to the logs it is executed with uid 0, so we can verify that expoit works, which verifies that some security measures should be taken in order to protect any existing Kubernetes cluster.

## V. MITIGATIONS

### *A. Avoidance*

This problem exists on the level of the core Kubernetes component, so this is Kubernetes development team responsibility to patch it in the next release. However there are some security measures that can be taken before the patch version release:

- Specify *runAsUser* directives in pods to control the uid a container runs as
- Specify *mustRunAsNonRoot:true* directives in pods to prevent starting as root (note this means the attempt to start the container will fail on affected kubelet versions)
- Downgrade kubelets to v1.14.1 or v1.13.5 as instructed by your Kubernetes distribution.

## VI. CONCLUSION

Containerization brings a lot of benefits to the industry, speeds up the development and deployment processes and improves the workflow. Needless to say how Kubernetes has changed production deployment management, improved usability and scalability of various applications and became popular among small businesses and large enterprise companies like Google and Tesla.

However, all the rapid development brings new horizons for hackers and security breaches. Therefore, it's always important to treat security seriously, take minimal measures to ensure no stupid misconfiguration or mistake will result in resource loses [10].

Therefore in recently created environments, like Kubernetes, security measures have to be taken even more seriously and every plugin or configuration for a more secure environment should be inspected and enforced.

## REFERENCES

[1] "Production-Grade Container Orchestration", *Kubernetes.io*, 2019. [Online]. Available: https://kubernetes.io/. [Accessed: 30- Oct- 2019].

[2] D. Goodin, "Tesla cloud resources are hacked to run cryptocurrency-mining malware", *Ars Technica*, 2018. [Online]. Available: https://arstechnica.com/information-technology/2018/02/tesla-cloud-resources-are-hacked-to-run-cryptocurrency-mining-malware/. [Accessed: 30- Sep- 2019].

[3] F. Huang and G. Duan, "The Ultimate Guide to Kubernetes Security - Threats, Tips, and Ebook", *NeuVector*, 2018. [Online]. Available: https://neuvector.com/container-security/kubernetes-security-guide/. [Accessed: 30- Oct- 2019].

[4] C. Meléndez, "The top Kubernetes security best practices - Sqreen blog", *Sqreen Blog*, 2019. [Online]. Available: https://blog.sqreen.com/kubernetes-security-best-practices/. [Accessed: 30- Sep- 2019].

[5] A. Zelivansky, "Non-Root Containers, Kubernetes CVE-2019-11245 and Why You Should Care", *Unit42*, 2019. [Online]. Available: https://unit42.paloaltonetworks.com/non-root-containers-kubernetes-cve-2019-11245-care/. [Accessed: 11- Nov- 2019].

[6] C. Gilbert, "9 Kubernetes Security Best Practices Everyone Must Follow - Cloud Native Computing Foundation", *Cloud Native Computing Foundation*, 2019. [Online]. Available: https://www.cncf.io/blog/2019/01/14/9-kubernetes-security-best-practices-everyone-must-follow/. [Accessed: 30- Nov- 2019].

[7] Y. Avrahami, "Breaking out of Docker via runC – Explaining CVE-2019-5736", *Unit42*, 2019. [Online]. Available: https://unit42.paloaltonetworks.com/breaking-docker-via-runc-explaining-cve-2019-5736/. [Accessed: 09- Nov- 2019].

[8] A. Martin, "11 Ways (Not) to Get Hacked", *Kubernetes.io*, 2018. [Online]. Available: https://kubernetes.io/blog/2018/07/18/11-ways-not-to-get-hacked/. [Accessed: 30- Oct- 2019].

[9] "Extending your Kubernetes Cluster", *Kubernetes.io*, 2019. [Online]. Available: https://kubernetes.io/docs/concepts/extend-kubernetes/ extend-cluster/. [Accessed: 19- Oct- 2019].

[10] S. Prodan, "Scanning Kubernetes resources with Kubesec", *Stefanprodan.com*, 2018. [Online]. Available: https://stefanprodan.com/2018/scanning-kubernetes-deployments-with-kubesec/. [Accessed: 30- Sep- 2019].

**Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 93 – 102 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# ADVANTAGES AND CHALLENGES OF QRNG INTEGRATION INTO MERKLE

Maksim Iavich[1], Tamuna Kuchukhidze[2], Avtandil Gagnidze[3], Giorgi Iashvili[1]
[1]Caucasus University, Scientific Cyber Security Association, Tbilisi, Georgia
[2] Georgian Technical University, Scientific Cyber Security Association
[3]Scientific Cyber Security Association

**ABSTRACT.** Google Corporation, NASA and the Universities Space Research Association have teamed up with D-Wave, the manufacturer of quantum processors. Quantum computers will be able to break most, if not absolutely all conventional cryptosystems, that are widely used in practice, for example RSA. RSA cryptosystem is used in different products on different platforms and in different areas. To date, this cryptosystem is integrated into many commercial products, the number of which is growing every day.

Hash-based digital signature schemes offer an alternative. Like any other digital signature scheme, hash-based digital signature schemes use a cryptographic hash function. Their security relies on the collision resistance of that hash function.

In 1979 Ralph Merkle proposed Merkle signature scheme. Merkle signature scheme has efficiency problems, so it cannot be used in practice. World scientists are working on improving the scheme. One of the improvements is integrating PRNG (pseudo random number generator) not to calculate and store large amount of one-time keys pairs. This approach cannot be considered secure, because according to our research quantum computers are able to crack PRNG, which were considered safe against attacks of classical computers.

In the article it is offered to use hash based pseudo random number generator and the quantum random number generator for generating the seed. The advantages and disadvantages of the scheme are analyzed.

**Keywords:** *quantum, random number generator, pseudo-random number generator, digital signature*.

**რეზიუმე**: გუგლის კორპორაცია, NASA და Universities Space Research Association შეუერთდა D-Wave-ს, კვანტური პროცესორების მწარმოებელს. კვანტურ კომპიუტერს შეუძლია გატეხოს უმეტესობა, შესაძლოა ყველა ტრადიციული კრიპტოსისტემა, რომლებიც პრაქტიკაში ფართოდ გამოიყენება, მაგალითად RSA. RSA კრიპტოსისტემა გამოიყენება სხვადასხვა პროდუქტებში, სხვადასხვა პლატფორმასა და განსხვავებულ სფეროებში. დღესდღეობით, ეს კრიპტოსისტემა ინტეგრირებულია ბევრ კომერციულ პროდუქტში, რომელთა რიცხვი ყოველდღიურად იზრდება.

ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის სქემები გვთავაზობს ალტერნატივას. როგორც სხვა ნებისმიერი ციფრული ხელმოწერის სქემა,

ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის სქემები იყენებს კრიპტოგრაფიულ ჰეშ ფუნქციას. მათი უსაფრთხოება ეყრდნობა ჰეშ ფუნქციის შეჯახების წინაღობას.
1979 წელს Ralph Merkle-მა შემოგვთავაზა Merkle-ს ხელმოწერის სქემა. Merkle-ს ხელმოწერის სქემას ეფექტურობის პრობლემა აქვს, მისი პრაქტიკაში გამოყენება არ შეიძლება. მსოფლიოს მეცნიერები მუშაობენ ამ სქემის გაუმჯობესებაზე. ერთ-ერთია PRNG-ის (ფსევდო შემთხვევითი რიცხვების გენერატორის) ინტეგრირება, რათა არ შევინახოთ გამოთვლები და დიდი ოდენობით ერთჯერადი გასაღების წყვილები. ეს მიდგომა არ არის უსაფრთხო, რადგან ჩვენი გამოკვლევების თანახმად, კვანტურ კომპიუტერებს PRNG-ის გატეხვა შეუძლიათ, რომელიც უსაფრთხოა კლასიკური კომპიუტერებიდან შეტევების შემთხვევაში.
სტატიაში შემოთავაზებულია ჰეშირებაზე დაფუძნებული ფსევდო შემთხვევითი რიცხვების გენერატორებისა და კვანტური შემთხვევითი რიცხვების გენერატორებისთვის საწყისი მნიშვენლობების გენერაცია. გაანალიზებულია სქემის დადებითი და უარყოფითი მხარეები.

**საკვანძო სიტყვები:** კვანტური, შემთხვევითი რიცხვების გენერატორები, ფსევდო შემთხვევითი რიცხვების გენერატორები, ციფრული ხელმოწერა.

## 1. შესავალი

გუგლის კორპორაცია, NASA და Universities Space Research Association შეუერთდა D-Wave-ს, კვანტური პროცესორების მწარმოებელს. კვანტურ კომპიუტერს შეუძლია გატეხოს უმეტესობა, შესაძლოა ყველა ტრადიციული კრიპტოსისტემა, რომლებიც პრაქტიკაში ფართოდ გამოიყენება, მაგალითად RSA. RSA კრიპტოსისტემა გამოიყენება სხვადასხვა პროდუქტებში, სხვადასხვა პლატფორმებზე და განსხვავებულ სფეროებში. დღესდღეობით, ეს კრიპტოსისტემა ინტეგრირებულია ბევრ კომერციულ პროდუქტში, რომელთა რიცხვი ყოველდღიურად იზრდება. RSA სისტემა ასევე ფართოდ გამოიყენება ოპერაციულ სისტემებში: Microsoft, Apple, Sun, და Novell. ტექნიკურ მოწყობილობებში RSA ალგორითმი გამოიყენება უსაფრთხო ტელეფონებში, Ethernet-ში, ქსელურ ბარათებში, სმარტ ბარათებში, ასევე ფართოდაა გავრცელებული კრიპტოგრაფიულ აპარატურაში. ამასთან, ალგორითმი წარმოადგენს დაცული ინტერნეტ კომუნიკაციების ძირითადი პროტოკოლების ნაწილს, მათ შორის S / MIME, SSL და S / WAN. ასევე გამოიყენება ბევრ ორგანიზაციაში, მაგალითად: მთავრობა, ბანკები, კორპორაციების დიდი ნაწილი, საჯარო ლაბორატორიები და უნივერსიტეტები. RSA BSAFE დაშიფვრის ტექნილოგიას მსოფლიოში საშუალოდ 500 მილიონი მომხმარებელი იყენებს. ვინაიდან დაშიფვრის ტექნოლოგიებში ძირითადად RSA ალგორითმი გამოიყენება, ის შეგვიძლია ჩავთვალოთ ყველაზე გავრცელებულ ღია გასაღების კრიპტოსისტემად, რომელიც ინტერნეტის განვითარებასთან ერთად ვითარდება. ამის საფუძველზე, RSA-ს განადგურებით ადვილი გახდება უმეტესი პროდუქტების გატეხვა, რაც სრულ ქაოსში გადაიზრდება.

### 1.1 ციფრული ხელმოწერები

ციფრული ხელმოწერა ინტერნეტისა და სხვა IT ინფრასტრუქტურების უსაფრთხოებაში ძირითადი ტექნოლოგიაა. მისი საშუალებით უზრუნველყოფილია მონაცემების საიმედოობა, მთლიანობა და non-repudiation. ციფრული ხელმოწერა ფართოდ გამოიყენება იდენთიფიკაციისა და აუთენტიფიკაციის პროტოკოლებში. ასე რომ, უსაფრთხო ციფრული ხელმოწერის არსებობა კიბერ უსაფრთხოებისთვის აუცილებელია. ციფრული ხელმოწერის ალგორითმები, რომლებსაც პრაქტიკაში ვიყენებთ შემდეგია: RSA, DSA და ECDSA. ისინი არ არიან კვანტურად იმუნური, რადგან მათი უსაფრთხოება ეყრდნობა დიდი შედგენილი მთელი რიცხვების დაშლის სირთულესა და დისკრეტული ალგორითმების გამოთვლას. ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის სქემები გვთავაზობს სერიოზულ ალტერნატივას. როგორც სხვა ციფრული ხელმოწერის სქემა, ჰეშირებაზე დაფუძნებული სქემაც იყენებს კრიპტოგრაფიულ ჰეშ ფუნქციას. მათი უსაფრთხოება ამ ჰეშირების ფუნქციის შეჯახების წინაღობაზეა დამოკიდებული.

### 1.2 ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერები

შემოგვთავაზეს ერთჯერადი ხელმოწერის სქემა - "Lamport One-Time Signature Scheme" [1].

1.2.1 ამ სისტემის ხელმოწერის გასაღები X შეიცავს n სიგრძის 2n ხაზს, რომლებიც შემთხვევითაა შერჩეული.

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

სისტემის ვერიფიკაციის გასაღები Y შეიცავს n სიგრძის 2n ხაზს, რომლებიც შემთხვევითაა შერჩეული.

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

გასაღების გამოსათვლელად ვიყენებთ ცალმხრივ ფუნქცია f-ს:

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

$y_i[j] = f(x_i[j]), 0<=i<=n-1, j=0,1$

#### 1.2.2 დოკუმენტის ხელმოწერა:

თვითნებური ზომის m შეტყობინება, ჰეშ ფუნქციის საშუალებით n ზომად გადაიქცევა:

$h(m)=hash = (hash_{n-1}, \ldots , hash_0)$

h ფუნქცია კრიპტოგრაფიული ჰეშ ფუნქციაა:

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

ხელმოწერა შემდეგნაირად ხდება:

$sig = (x_{n-1}[hash_{n-1}], \ldots, x_0[hash_0]) \in \{0,1\}^{n,n}$

თუკი შეტყობინების i-ური ბიტი 0-ის ტოლია, სეგმენტში i-ურ სტრინგს მიენიჭება $x_i[0]$. იმ შემთხვევაში, თუკი შეტყობინების i-ური ბიტი 1-ია, მიენიჭება $x_i[1]$.

ხელმოწერის სიგრძეა $n^2$.

### 1.2.3 ხელმოწერის ვერიფიკაცია

ხელმოწერის ვერიფიკაციისთვის $sig = (sig_{n-1}, \ldots, sig_0)$, შეტყობინების ჰეში გამოითვლება.

$hash = (hash_{n-1}, \ldots, hash_0)$ და შემდეგი განტოლება უნდა შევამოწმოთ:

$(f(sig_{n-1}), \ldots, f(sig_0)) = (y_{n-1}[hash_{n-1}], \ldots, y_0[hash_0])$

თუ მართალია, ხელმოწერა სწორია.
ამ სქემის მთავარი და სერიოზული ნაკლი გასაღების დიდი ზომაა.

O ($2^{80}$) უსაფრთხოების მისაღწევად, ღია და დახურული გასაღებები უნდა იყოს 160∗2∗160 ბიტი = 51200 ბიტს, ეს 51200/1024=50-ჯერ დიდია, ვიდრე RSA-ს შემთხვევში.

ასევე უნდა ავღნიშნოთ, რომ მოცემულ სქემაში ხელმოწერის ზომა უფრო დიდია, ვიდრე RSA-ს შემთხვევაში. Winternitz-ის ერთჯერადი ხელმოწერის სქემა შემოთავაზებულია ხელმოწერის ზომის შესამცირებლად.

ერთჯერადი ხელმოწერის სქემები არაადეკვატურია უმეტესი პრაქტიკული სიტუაციებისთვის, რადგან გასაღების თითოეული წყვილის გამოყენება მხოლოდ ერთი ხელმოწერისთვისაა შესაძლებელი. 1979 წელს Ralph Merkle-მა შემოგვთავაზა ამ პრობლემის გადაწყვეტა. მისი იდეაა სრული ორობითი ჰეშის ხის გამოყენება. იდეა არის, რომ გამოვიყენოთ ბინარული ჰეშეპის ხე იმისათვის, რომ შევამციროთ ერთჯერადი ვერიფიკაციების გასაღებების რაოდენობა ერთი საჯარო გასაღებით, რომელიც იქნება ხის ფესვი.

## 2 Merkle-ს ხელმოწერის სქემა

ხის სიგრძე უნდა იყოს H>=2 და ერთი ღია გასაღებით $2^H$, დოკუმენტზე ხელის მოწერა შეიძლება. ხელმოწერისა და ვერიფიკაციის $2^H$ წყვილი გენერირდება; $X_i$, $Y_i$, 0<=i<=2H. $X_i$ არის ხელმოწერის გასაღები, $Y_i$ კი ვერიფიკაციის.
ხეს ფოთლების გასაგებად, ხელმოწერის გასაღებების ჰეშირება შემდეგი ჰეშ ფუნქციის საშუალებით უნდა მოხდეს:

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

მშობელი კვანძის მისაღებად, წინა ორი კვანძის კონკატენაციის ჰეშირება ხდება. ხის ფესვი ხელმოწერის ღია გასაღებია.

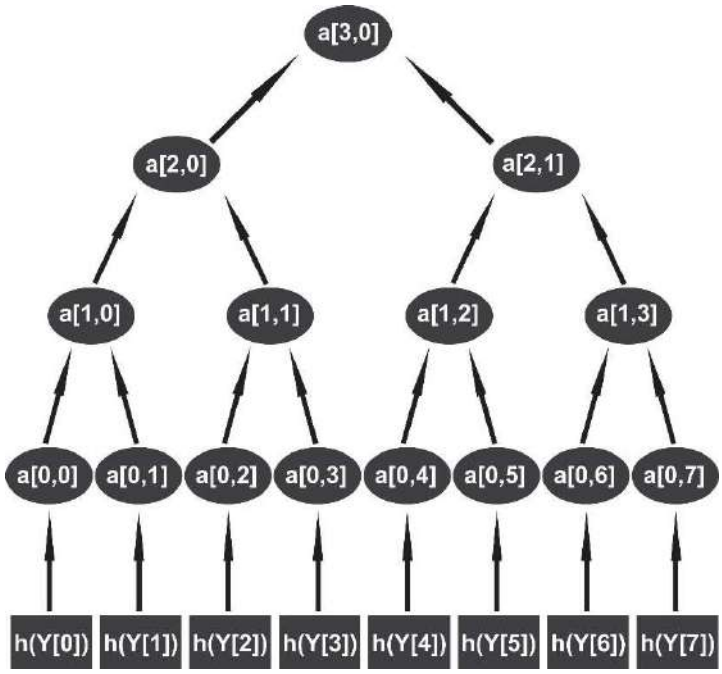



**Fig. 1.** Merkle-ს ხე, სადაც H=3

ფიგ.1 გამოსახულია ხე, სადაც H=3; a[i,j] კი ხის კვანძებია.

ნებისმიერი ზომის შეტყობინებაზე ხელმოწერისას, ჰეშირებით ზომა შეგვიძლია n-ის ტოლად გარდავქმნათ.
*h (m) = hash*, შეტყობინების ხელმოწერისთვის, გამოიყენება თვითნებური ერთჯერადი გასაღები $X_{arb}$. ხელმოწერა არის ერთობლიბა: ერთჯერადი ხელმოწერის, ერთჯერადი ვერიფიკაციის გასაღების, გასაღების ინდექსის და ყველა ძმა კვანძების, რომლებიც შერჩეულია თვითნებური გასაღებით, რომელთა ინდექსია "*arb*".

$$Signature = (sig||arb||\ Y_{arb}||auth_{0,\dots,}auth_{H-1}) \quad .$$

ხელმოწერის შემოწმებისთვის, ერთჯერადი ხელმოწერის კონტროლი შერჩეული ვერიფიკაციის გასაღებით ხდება. თუ ვერიფიკაცია გაიარა, ყველა საჭირო კვანძი გამოითვლება "auth"-ით, "arb" ინდექსითა და $Y_{arb}$. თუ ხის ფესვი ემთხვევა ღია გასაღებს, მაშინ ხელმოწერა სწორია.

ამ კრიპტოსისტემას ეფექტურობის პრობლემა აქვს, მისი გამოყენება პრაქტიკაში მიუღებელია [2-4].

ერთჯერადი გასაღებების $2^H$ წყვილი უნდა გამოვთვალოთ ღია გასაღების გენერირებისთვის. გასაღების ასეთი დიდი რიცხვის შენახვა პრაქტიკაში პრობლემურია.

## 3. Merkle ინტეგრირებული PRNG -ით

მსოფლიოს მეცნიერები მუშაობენ ამ სქემის გაუმჯობესებაზე. ერთ-ერთია PRNG-ს (ფსევდო შემთხვევითი რიცხვების გენერატორის) ინტეგრირება, რათა არ შევინახოთ გამოთვლები და დიდი ოდენობით ერთჯერადი გასაღების წყვილები [5,6].

ზოგიერთი PRNGs, რომლებიც ითვლებოდა უსაფრთხოდ შეგვიძლია კვანტური კომპიუტერით გავტეხოთ, ამიტომ ფრთხილად უნდა ვიყოთ PRNG-ის შერჩევისას.

Merkle-ში CSPRNG გვთავაზობს ჰეშ ფუნქციაზე დაფუძნებულ ალგორითმს, რადგან მასზე მთელი ალგორითმია დაფუძნებული. NIST-ის რეკომენდაციაა PRNGs-ზე დაფუძნებული ორი უწყვეტი ჰეში: HASH_DBRG და HMAC_DBRG. უკეთესია HASH_DBRG, რადგან უფრო ეფექტურია.

ჩვენ გთავაზობთ HASH_DBRG საწყისი მნიშვნელობების, თესლის, გენერაციისთვის ფიზიკური კვანტური შემთხვევითი რიცხვების (QRNG) გამოყენებას.

## 4. კვანტური შემთხვევითი რიცხვების გენერატორები

მე-20 საუკუნის მეორე ნახევარში კომპიუტერული სიმულაციის ზრდასთან ერთად, ელექტრონულ შემთხვევითი რიცხვების გენერატორებზე მოთხოვნაც გაიზარდა. იმ დროს, ჩვეულებრივი მოვლენა იყო შემთხვევითი რიცხვების ცხრილები. რადიოაქტიური დაშლა ხელმისაწვდომი წყაროა ჭეშმარიტი შემთხვევითობისთვის. Geiger-M¨uller-ის მილები მგრძნობიარეა α, β და γ რადიაციის აღმოჩენისა და გაძლიერებისთვის. მისი საშუალებით მივიღეთ საიმედო, კარგი რადიოაქტიული ნიმუშები. სიმარტივისთვის, რადიოაქტიურობაზე დაფუძნებული შემთხვევითი რიცხვების გენერატორები დაფუძნებული იყოს β რადიაციის აღმოჩენაზე.

Geiger-M¨uller, GM - ში ერთი ნაწილაკის დეტექტორი წარმოქმნის იონიზაციის მოვლენას, რომელიც Townsend avalanche-ში გაფართოვდება. შედეგად გვაქვს მოწყობილობა, რომელიც სწორად კონფიგურირების შემთხვევაში, თითოეული აღმოჩენილი ნაწილაკისთვის წარმოქმნის პულსს. ნებისმიერი ატომის დაშლის ალბათობა კონკრეტული დროის ინტერვალიში (t, t + dt) არის ექსპონენციალური შემთხვევითი ცვლადი, $P(t)dt = \lambda_m e^{\wedge}(-\lambda_m t)dt$ , $\lambda_m$ დაშლის მუდმივისთვის.

ეს QRNGs წარმოადგენს დღევანდელი ოპტიკური QRNG-ის წინამორბედს. გამოიყენება მსგავსი ცნებები და სქემები, მაგრამ რადიოაქტიური წყარო და GM მთვლელი, ფოტონის წყაროებითა და დეტექტორებითაა ჩანაცვლებული.

რადიოაქტიურ დაშლაზე დაფუძნებული პირველი კვანტური შემთხვევითი რიცხვების გენერატორები ბევრ საერთო ელემენტს იზიარებს. უმეტესობა იყენებს ციფრულ მთვლელს, დეტექტორიდან პულსების შემთხვევით ბიტებში კონვერტაციისთვის. ციფრული მრიცხველი ზრდის მის გამომავალ მნიშვნელობას 1-ით, როდესაც მნიშვნელობად მიიღებს პულსს და შეუძლია გადატვირთოს - დაიწყოს თვლა ნულიდან. კიდევ ერთი მნიშვნელოვანი ელემენტია ციფრულ საათთან სინქრონიზაცია. ამ QRNGs უკეთესად განვმარტავთ თუ აღვწერთ საათებს, სწრაფი და ნელი საათის ტერმინით, ν სიხშირით, რომელიც აღმოჩენის საშუალო მაჩვენებელს მნიშვნელოვნად აღემატება ან გაცილებით მცირეა. სწრაფი საათი, სადაც $\nu > \lambda$, აგენერირებს ბევრ პულსს, Geiger-ის მთვლელებს შორის. ნელ საათში, სადაც $\nu < \lambda$, უნდა იყოს გასული საკმარისი დრო, GM დეტექტორმა უნდა დაარეგისტრიროს საკმარისი ოდენობის პულსები.

ამ ელემენტებით, აღმოჩენის დროის შემთხვევითობა შეიძლება გარდავქმნათ რამდენიმე გზით შემთხვევით ციფრებში. გენერატორები Isida და Ikeda, ასევე Vincent იყენებს სწრაფ საათიან მრიცხველს, სადაც ყოველი აღმოჩენილი მნიშვნელობა იკითხება და შემდეგ ნულდება (ყოველ ჯერზე, როცა დეტექტორზე მნიშვნელობას ვიღებთ). აღმოჩენის მომენტში მრიცხველის მნიშვნელობა გამოიყენება შემთხვევითი რიცხვის წარმოსაქმნელად. მნიშვნელობების განაწილება არ არის თანაბარი, საჭიროებს შესწორებას. თუ წარმოვქმნით ათობით ციფრს, შეგვიძლია ავიღოთ ყველაზე ნაკლებად მნიშვნელოვანი ფიგურა. ოროობითი მიმდევრობისთვის ექვივალენტური მეთოდია მრიცხველის მნიშვნელობის ტოლობის შემოწმება, დათვლილი პულსების მნიშვნელობა კენტია თუ ლუწი.

მეორე ვარიანტია, ნელი საათის გამოყენება, რათა დავადგინოთ როდის წავიკითხოთ მრიცხველი. Schmidt-ის გენერატორში GM-ის დეტექტორის პულსები მრიცხველის მნიშვნელობას ზრდის. როდესაც ნელი საათი წარმოქმნის ახალ პულსს, მრიცხველის მნიშვნელობა გამოიყენება, როგორც შემთხვევითი ციფრი და ათვლა კვლავ იწყება 0-დან. გამომავალი მნიშვნელობა შეესაბამება თითოეული საათის პერიოდში ნაწილაკების ოდენობას. ჩვენ ვზღუდავთ მრიცხველს, რომელიც აგენერირებს 0 დან M−1-მდე მნიშვნელობებს. ეს არის მოდულით M მრიცხველი. როდესაც M = 2, გვაქვს ოროობითი შემთხვევითი რიცხვების გენერატორი. შერჩეული ციფრების განაწილება არ არის თანაბარი, მაგრამ თუ ავიღებთ M მოდულით და მრავალჯერ გამოვიტანთ მნიშვნელობებს, მივიღებთ მიკერძოებას სასურველად მცირე განაწილებით. ამ პროცესს ეწოდება "შეკუმშვა ". რადიოაქტიური დაშლა ასევე გამოიყენება ანალოგური კომპიუტერებისთვის თეთრი ხმაურის შესაქმნელად. შემთხვევითი ხმაურის გენერატორებს მნიშვნელოვანი როლი ჰქონდათ თვითმფრინავის დიზაინის სიმულაციაში, ანალოგურ გამოთვლებში. ის ასევე გამოიყენება, როგორც სატესტო სიგნალი, ზოგადად ისეთ კომუნიკაციისა და სიმულაციის პრობლემებში სადაც მაღალგამტარი სიგნალია საჭირო. ამ შემთხვევაში, GM გამტარიდან პულსები იწვევს ძაბვის სიგნალის შეცვლას. როდესაც ნაწილაკი გამოვლინდება, სიგნალი მაღალიდან დაბალი ძაბვიდან გადადის დაბალიდან მაღალში. შედეგად მიღებულ შემთხვევით სიგნალს შემთხვევით ტელეგრაფიულ ხმაურს უწოდებენ. ამ დროს არ გვინდა ოროობითი სიგნალი, არამედ Gaussian-ის ხმაური.

## 5. გამოწვევები

მიუხედავად იმისა, რომ რადიოაქტიურ დაშლაზე დაფუძნებული QRNGs გვაძლევს კარგი ხარისხის ჭეშმარიტ შემთხვევით რიცხვებს, აქვთ ნაკლოვანებები, რომლებიც ზღუდავს მათ პრაქტიკულ გამოყენებას. მნიშვნელოვანი ბარიერია ბიტების სიჩქარე, ჩვეულებრივ, რამდენიმე ასეული კილობიტი წამში.

პირველი პრობლემა რადიოაქტიური წყაროს საჭიროებაა. პრინციპში, ყველა დაშლაზე დაფუძნებული QRNGs მუშაობს ფონურ რადიაციაზე. თუ დეტექტორი იზილირებული არ არის, შეუძლია დაითვალოს მოხეტიალე კოსმოსური სხივები, რადიაცია რადიუმიდან, თორიუმიდან და სხვა რადიოაქტიური მასალებიდან, რომლებიც დედამიწის ქერქში ან ჰაერშია. თუმცა, ბუნებრივი იშვიათად წარმოქმნის საჭირო ნაწილაკებს, რომლებიც ერთ წამში რამდენიმეზე მეტი იქნება. ეს არის ფუნდამენტური პრობლემა, რომელიც რადიოაქტიური დაშლის QRNGs ფართოდ გამოყენებას ხელს უშლის. სწრაფი ტემპის მისაღწევად, QRNG-ს სჭირდება ძალიან რადიოაქტიური წყარო. მაგალითად გენერატორები იყენებენ Cobalt-60, Strontium-90, Caesium-137, Americium-241 ან Nickel-63. ეს მოუხერხებელია და მოითხოვს უსაფრთხოების გაუმჯობესებას. მიუხედავად იმისა, რომ α წყარო, როგორიცაა Americium ადვილად იზოლირებადია და გავრცელებულია კვამლის სიგნალებში, დამატებითი სიფრთხილის ზომები ხელს უშლის კომპიუტერთან ინტეგრაციას. ეს მიდგომა კარგად მუშაობს მხოლოდ ისეთ სპეციალურ სერვერებთან, როგორიცაა HotBits.

გენერირებული ბიტების სისწრაფის მეორე შეზღუდვაა დეტექტორების მკვდარი დრო. Geiger-ის მთვლელში avalanche, რომელიც ზრდის თითოეულ დათვლას, GM მილში ხდება გაზის იონიზაცია. avalanche ჩერდება, როდესაც დადებითი იონები შემოერტყმება cathode მილში. ეს იონები გვიცავს უფრო მეტი avalanche-დან, სანამ ნორმალურ მდგომარეობაში დაბრუნდებიან. მკვდარი დრო არის, GM მილის მინიმალური დრო, რომელიც საჭიროა სრულ აღმოჩენის უნარის დაბრუნებამდე. ეს დრო შეიძლება იყოს ათეულობით ნანოწამიდან რამდენიმე მიკროწამამდე. ეს ზღუდავს დათვლის სიჩქარეს MHz დიაპაზონში. ნახევრადგამტარ გამტარებს ასევე სჭირდებათ მკვდარი დრო თითოეული აღმოჩენის შემდეგ, რომელიც მიკროწამის დიაპაზონშია.

მკვდარ დროს და სხვა არაერთგვაროვან წყაროებს სჭირდებათ დამუშავება, როდესაც შემთხვევითი ბიტების გენერაცია ხდება. ზოგადად, დაგენერირებული ბიტების ხარისხი კარგი იქნება და როდესაც არის დარჩენილი რაღაც მიკერძოება, არსებობს მარტივი დამუშავების მეთოდები, რომლებიც აღადგენენ შემთხვევით მიღებულ მნიშვნელობებს.

საბოლოო პრობლემა ნახევარგამტარ დეტექტორებს ეხება. მათზე მოქმედებს რადიაცია. Geiger მილებიც დროთა განმავლობაში იცვითება, მაგრამ მათზე რადიაციის ეფექტი უკვე შესწავლილია, ხოლო კონკრეტულად რადიაციის დეტექტორებისთვის ნახევარგამტარები ახალია. საჭიროა ამ საკითხის დროის განმავლობაში შესწავლა.

ამ შეზღუდვების მიუხედავად, რადიოაქტიური დაშლა შემთხვევითობის შესაფერისი წყაროა, დაბალი სიჩქარის მოწყობილობებისთვის. მაგალითად, მას შეუძლია მოგვაწოდოს ენტროფია ფსევდო შემთხვევითი რიცხვების გენერატორების საწყისი მნიშვნელობებისთვის. უფრო

მომთხოვნი სისტემებისთვის, რომლებიც ბიტების მაღალ სიხშირეს მოითხოვენ ან როცა გვინდა თავი ავარიდოთ რადიოაქტიურ წყაროებს, უახლესი QRNGs კარგი ჩანაცვლებაა.

## 6. სქემა

ხის ზომა უნდა იყოს H>=2 და დოკუმენტზე ხელმოწერა შეიძლებოდეს ერთი $2^H$ ღია გასაღებით. კვანტური შემთხვევითი რიცხვების გენერატორებით წარმოვქმნით საწყის მნიშვენლობებს. PRNG HASH_DBRG იღებს ამ საწყის მნიშვნელობას, როგორც შემავალ მნიშვნელობად და აგენერირებს ხელმოწერისა და ვერიფიკაციის გასაღებებს; $X_i$, $Y_i$, 0<=i<=2H. $X_i$ არის ხელმოწერის გასაღები, $Y_i$ - ვერიფიკაციის გასაღები. ხეზე ფოთლების მისაღებად, ჰეშ ფუნქციით ხელმოწერის გასაღებების ჰეშირება ხდება:

$$h:\{0,1\}^* \rightarrow \{0,1\}^n \quad .$$

მშობელი კვანძის გასაგებად, წინა ორი კვანძის კონკატენაციის ჰეშირებაა საჭირო. ხის ფესვი არის ხელმოწერის ღია გასაღები.

ნებისმიერი ზომის შეტყობინებაზე ხელმოწერისას, ჰეშირებით ზომა შეგვიძლია n-ის ტოლად გარდავქმნათ.

*h (m) = hash*, შეტყობინების ხელმოწერისთვის, გამოიყენება თვითნებური ერთჯერადი გასაღები $X_{arb}$. ხელმოწერა არის ერთობლიბა: ერთჯერადი ხელმოწერის, ერთჯერადი ვერიფიკაციის გასაღების, გასაღების ინდექსის და ყველა ძმა კვანძების, რომლებიც შერჩეულია თვითნებური გასაღებით, რომელთა ინდექსია "*arb*".

$$Signature= (sig||arb|| Y_{arb}||auth_0,\ldots,auth_{H-1})$$

ხელმოწერის შემოწმებისთვის, ერთჯერადი ხელმოწერის კონტროლი შერჩეული ვერიფიკაციის გასაღებით ხდება. თუ ვერიფიკაცია გაიარა, ყველა საჭირო კვანძი გამოითვლება "auth"-ით, "arb" ინდექსითა და $Y_{arb}$. თუ ხის ფესვი ემთხვევა ღია გასაღებს, მაშინ ხელმოწერა სწორია.

## 7. დასკვნა

მიღებული სქემა საკმაოდ ეფექტურია, რადგან არ ინახავს ხელმოწერის ყველა გასაღებს. იყენებს კვანტურად მდგრად ფსევდო შემთხვევითი რიცხვების გენერატორს, რომელიც იყენებს ჰეშ ფუნქციებს და არის NIST სტანდარტი. ის გენერატორი საწყის მნიშვნელობებს იღებს კვანტური შემთხვევითი რიცხვების გენერატორიდან. გაანალიზებულია კვანტური შემთხვევითი რიცხვების გენერატორების გამოყენების გამოწვევები.

**ACKNOWLEDGEMENT**

The work was conducted as a part of PHDF-19-519 and the grant financed by Caucasus University

## ბიბლიოგრაფია


1. Ajtai, M.: Generating hard instances of lattice problems. In Complexity of computations and proofs, volume 13 of Quad. Mat., pages 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 (1986).
2. A Gagnidze, M Iavich, G Iashvili, Novel Version of Merkle Cryptosystem - Bull. Georg. Natl. Acad. Sci, 2017
3. Buldas A., Firsov D., Laanoja R., Lakk H., Truu A. (2019) A New Approach to Constructing Digital Signature Schemes. In: Attrapadung N., Yagi T. (eds) Advances in Information and Computer Security. IWSEC 2019. Lecture Notes in Computer Science, vol 11689. Springer, Cham
4. Post-quantum cryptosystems // Modern scientific researches and innovations. 2016. № 5 [Electronic journal]. URL: http://web.snauka.ru/en/issues/2016/05/67264
5. A.Gagnidze, M.Iavich, G. Iashvili, MERKLE WITH QUANTUM TRNG, Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):14-20, 2017
6. Buchmann J., García L.C.C., Dahmen E., Döring M., Klintsevich E. (2006) CMSS – An Improved Merkle Signature Scheme. In: Barua R., Lange T. (eds) Progress in Cryptology - INDOCRYPT 2006. INDOCRYPT 2006. Lecture Notes in Computer Science, vol 4329. Springer, Berlin, Heidelberg