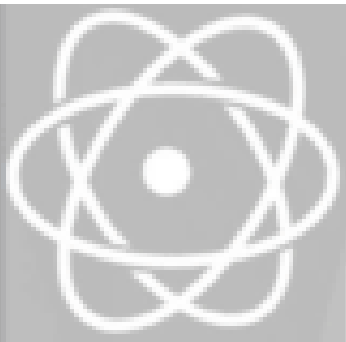


# SPCSJ

# SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL5 No2
June 2021

ISSN 2587-4667

**Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 1-11 ISSN 2587-4667**
**Scientific Cyber Security Association (SCSA)**

# NOVEL SYSTEM FOR HARDWARE-BASED VULNERABILITIES RECOGNITION

# აპარატურულ უზრუნველყოფაზე დაფუძნებული სისტემებში უსაფრთხოების პრობლემების გამოვნელის ნაივური სისტემა

**გიორგი იაშვილი კავკასიის უნივერსიტეტი, პაატა საკაძის ქ.1, 0102, თბილისი, საქართველო**
**Giorgi Iashvili Caucasus University, Paata Saakadze st.1, 0102, Tbilisi, Georgia**

**ABSTRACT.** Hardware-based security mechanisms are becoming increasingly popular, but implementing these mechanisms correctly has proved difficult, thus undermining the root of security. This work introduces an effective way to formally verify important properties of such hardware security mechanisms and, consequently, determine the optimal mitigation strategies for each particular use case.The goal of the research that is reported in this paper was to understand the weaknesses of hardware-based devices and related software systems, in order to improve the necessary security mechanisms. The goal of the work is the creation of modern recognition system to identify hardware-based vulnerabilities and provide users with corresponding recommendations. This paper describes an integrated software system that analyzes the potential security threats that may affect a certain hardware-based system, and consequently suggests the optimal solutions. The result of our research is prototype of the system, which is able to collect information about modern hardware-based vulnerabilities and provide user with corresponding recommendations according to concrete scenario. Controlled test of the system was made in the frame of the research. Furthermore, in order to optimize the usability of the reports that the system generate, and the end users overall experience, the algorithmic core will be complemented with relevant machine learning elements. Thus, dedicated analysis routines will analyze the data that is stored in the database, also considering the newly entered data, will combine the available data and eventually add the required supplementary data to the database.

**აბსტრაქტი.** აპარატურზე დაფუძნებული უსაფრთხოების მექანიზმები სულ უფრო პოპულარული ხდება, მაგრამ ამ მექანიზმების სწორად რეალიზაცია რთული ამოცანაა. ეს ნამუშევარი წარმოადგენს ეფექტური ტექნიკის უსაფრთხოების ამგვარი მექანიზმების მნიშვნელოვანი თვისებების ოფიციალურად გადამოწმების ეფექტურ გზას და, შესაბამისად, თითოეული კონკრეტული სცენარ შემთხვევაში შემსუბუქების ოპტიმალური სტრატეგიების შემუშავებას. კვლევის მიზანი იყო აპარატურული უზრუნველყოფის სისუსტეების გაგება და მასთან დაკავშირებული პროგრამული სისტემების უსაფრთხოების აუცილებელი მექანიზმების გაუმჯობესება. სამუშაოების მიზანია თანამედროვე სისტემის შექმნა, აპარატურაზე დაფუძნებული სისუსტეების დასადგენად და მომხმარებლებისთვის შესაბამისი რეკომენდაციების მიწოდება. ამ ნაშრომში აღწერილია ინტეგრირებული პროგრამული სისტემა, რომელიც აანალიზებს უსაფრთხოების პოტენციურ საფრთხეებს, რომლებმაც შეიძლება გავლენა მოახდინონ გარკვეულ აპარატურულ სისტემაზე დაფუძნებულ მექანიზმებზე და, შესაბამისად, გვთავაზობს ოპტიმალურ გადაწყვეტილებებს. კვლევის შედეგია სისტემის პროტოტიპი, რომელსაც შეუძლია შეაგროვოს ინფორმაცია თანამედროვე აპარატურული მოწყვლადობის შესახებ და მომხმარებელს მიაწოდოს შესაბამისი რეკომენდაციები კონკრეტული სცენარის შესაბამისად. კვლევის ფარგლებში გაკეთდა სისტემის კონტროლირებადი ტესტი. გარდა ამისა, სისტემის მიერ წარმოქმნილი ანგარიშების გამოყენებასა და საბოლოო მომხმარებლების საერთო გამოცდილების ოპტიმიზაციის მიზნით, ალგორითმული ბირთვი დაკომპლექტდება შესაბამისი მანქანური სწავლების ელემენტებით. ამრიგად, სპეციალური ანალიზის სქემები დამუშავებენ

მონაცემთა ბაზაში შენახულ ინფორმაციას, და ასევე მიაქცევენ ყურადღებას ახლად შეყვანილი მონაცემების ნაკადებს. სისტემა მოახდენს ახალი მონაცემების დამატებას ბაზაში და შედეგად მივიღებთ რეკომენდაციების უკეთეს და უფრო დეტალურ ვარიანტს რაც დადებითად იმოქმედებს მომხმარებლის უსაფრთხოების დონეზე.

**KEYWORDS***: hardware-based attacks, side-channel, hardware security, modern system, hardware vulnerabilities.*

**საკვანძო სიტყვები:** *აპარატურული, აპარატურული დაცვა, გვერდითი არხი, თანამედროვე სისტემა, აპარატურული სისუსტეები*

## შესავალი

თანამედროვე კიბერ სამყაროში სარეკომენდაციო სისტემები ხელოვნური ინტელექტის მექანიზმების ყველაზე თვალსაჩინო მაგალითია. ჩვეულებრივ, ასეთი პროგრამები იქმნება მომხმარებლისთვის უკეთესი გამოცდილებისთვის სხვადასხვა სისტემებში. მაგალითად Facebook, რომელიც შეიცავს „ადამიანები, რომელბსაც შეიძლება იცნობდეთ" მოდული და YouTube, რომელიც გთავაზობთ
შესაბამის ვიდეოს ინტერესების მიხედვით, რაც დგინდება დათვალიერების წინა ისტორიის საფუძველზე. ეს ყველაფერი შეიძლება ჩაითვალოს მომხმარებელზე ორიენტირებული სარეკომენდაციო სისტემების საკმაოდ კარგ მაგალითებად. ვებ პლატფორმები მომხმარებლებს საშუალებას აძლევს მიიღოს რეკომენდაციები სხვადასხვა კრიტერიუმების საფუძველზე. ალგორითმებს, რომლებიც გამოიყენება
ასეთი პროგრამებს მიერ უწოდებენ სარეკომენდაციო სისტემებს. დღეს ალგორითმები გამოიყენება სხვადასხვა სარეკომენდაციო სისტემა, მაგრამ შინაარსზე დაფუძნებული შემოთავაზებების მეთოდი ერთ-ერთი ყველაზე ორიენტირებულია მომხმარებელზე. სარეკომენდაციო სისტემები ფართოდ
გამოიყენება შინაარსის ფილტრაციისთვის სხვადასხვა ვებ პლატფორმებში, როგორიცაა ონლაინ მაღაზიები, ფილმების ან მოგზაურობის მონაცემთა ბაზა, საგანმანათლებლო მიმართულებები და მრავალი სხვა. შინაარსის ფილტრაციის სისტემები (content filtering systems) მომხმარებლებს ეხმარება მაქსიმალურად კარგად იპოვონ შესაბამისი შინაარსი, მათი საჭიროებებიდან და ინტერესებიდან
გამომდინარე. დღეს ნებისმიერი თანამედროვე სისტემისთვის მომხმარებლის უსაფრთხოებაა უაღრესად მნიშვნელოვანია. ჰაკერები ასრულებენ შეტევას სხვადასხვა ტექნიკისა და მიდგომის გამოყენებით. აპარატურულ უზრუნველყოფაზე დაფუძნებული სისტემები ხშირად ხდება სხვადასხვა
თავდასხმების სამიზნეები. გვერდითი არხი (side-channel), ცენტრალურ პროცესორზე ორიენტირებული (central processor unit) და ფიზიკური შეტევები გარჩევის ან კრიტიკული ინფორმაციის მიღების დღეს თავდასხმის მოდელის ერთ-ერთი ყველაზე პოპულარული მეთოდია. აღსანიშნავია, რომ სხვადასხვა პროგრამული მექანიზმები სამუშაოდ დღეს იყენებენ აპარატურულ სისტემას. ასეთი სისტემების უსაფრთხოების ხარვეზებმა შეიძლება სერიოზული პრობლემები შეუქმნას მთლიანობაში მექანიზმებს. სისტემა უზრუნველყოფს მომხმარებელს რეკომენდაციებს შესაბამის ინტერესებზე და პარამეტრებზე

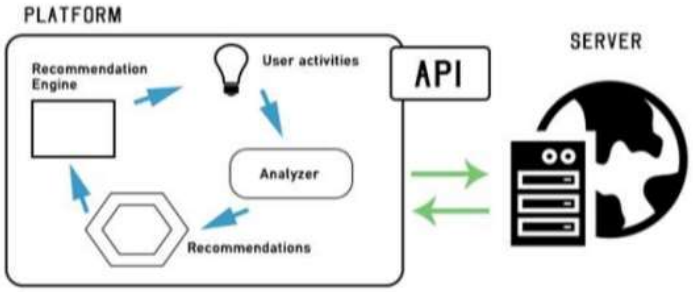
დაყრდნობით. სარეკომენდაციო სისტემის პირველი ვერსია ეყრდნობა ცნობილ ღია წყაროებს, მოწყვლადობის მონაცემთა ბაზებს და მუშაობს თითოეული მომხმარებლის შეყვანისთვის ნდივიდუალურად. მანქანური სწავლების მექანიზმების გამოყენებით, რომლებიც ჩაწერილია არსებულ რეკომენდაციების სისტემაში უკეთესი შედეგების მისაღწევად. ასეთი მიდგომა მნიშვნელოვნად გაიზრდის უსაფრთხოების დონის აპარატურულ სისტემებში.

## ლიტერატურის მიმოხილვა

აპარატურულ უზრუნველყოფაზე ორიენტირებული თავდასხმები ძალიან პოპულარულია დღეისთვის. არსებობს წარმატებული ჩატარებული თავდასხმების მთლი რიგი, რომელიც ორიენტირებულია კიბერ უსაფრთხოების ამ კონკრეტულ მიმართლებაზე [1-3]. ასევე, აპარატურაზე ხშირად ფიქსირდება ე.წ. side-channel თავდასხმები, რომელიც ხორციელდება მათ შორის პროგრამულ რეალიზაციაზე და ზოგ კრიპტოგრაფიულ ალგორითმზე [4-7]. ამ პერიოდისთვის პოპულარული სისტემებიც კი შეიძლება იყოს მოწყვლადი აპარატურაზე ორიენტირებული თავდასხმების წინაშე [8-10]. აღსანიშნავია, რომ არსებობს ე.წ. კომბინირებული თავდასხმების მიდგომები, რომელიც წარმატებით ხორციელდება არსებულ უსაფრთხოების მექანიზმებზე [11-13]. განხორციელებულია ამ მიმართულებით ახალი უსაფრთხოების მექანიზმების შემუშავება და ავტორები სთავაზობენ არსებული სისტემების გაუმჯობესებულ ვარიანტებს [14-16]. ერთ-ერთი მნიშვნელოვანი მიმართულება კიბერ უსაფრთხოებაში გახლავთ IoT (ნივთების ინტერნეტი) და ე.წ. ჭკვიანი მოწყობილობები, რაც იმას ნიშნავს, რომ მუდმივად იქმნება თავდასხმების ახალი ვექტორები [17-19].

## შინაარსზე დაფუძნებული სისტემების მუშაობა

უსაფრთხოების სცენარის ანალიზისთვის შინაარსზე (content-based) დაფუძნებული რეკომენდაციების სისტემას სჭირდება მომხმარებლის მიერ მოწოდებული მონაცემები და სპეციალური ჩარჩოები, რომელიც ინახება მონაცემთა ბაზაში, მაგალითად შინაარსზე დაფუძნებული პარამეტრები, შეფასება, უკუკავშირი და
მომხმარებლის სხვა აქტივობები. ამ შემთხვევაში კიბერ უსაფრთხოებაზე და ტექნიკაზე დაფუძნებულ სისტემებში, მონაცემები კონკრეტული რეკომენდაციით გაანალიზებულია სისტემის მიერ. მონაცემების შეყვანა ხდება სპეციალური ინტერაქტიული ჩაშენებული ფორმის გამოყენებით. ამ მონაცემებზე დაყრდნობით, სისტემა ქმნის მომხმარებლის პროფილს, რომელიც გამოიყენება შესაბამისი უსაფრთხოების რეკომენდაციების შესაქმნელად. ეს პროცესი ხდება მომხმარებლის მხრიდან დამატებითი ინფორმაციის შეყვანის საშუალებით. სისტემას შეუძლია ამ დამატებითი ინფორმაციის დამუშავება, რის შედეგადაც ეს მექანიზმი ხდება უფრო ზუსტი.




**სურ.1.** კონტენტზე დაფუძნებული სისტემის მუშაობის პრინციპი

როგორც ნაჩვენებია გრაფიკულ გამოსახულება 1-ზე, პლატფორმის შიგნით სისტემა მიუთითებს მომხმარებლის საქმიანობაზე - მონაცემებსა და პრეფერენციებზე, აანალიზებს მათ და გარდაქმნის მათ რეკომენდაციებად. მიღებული რეკომენდაციები კი იგზავნება სარეკომენდაციო ძრავასთან. პლატფორმა ქმნის კავშირი სერვერთან და გაცვლის მონაცემებს სპეციალური არხით ან სპეციალური API - თ. ყოველი ახალი იტერაცია გვაძლევს უფრო ზუსტ და მომხმარებელზე მორგებულ შედეგს, გამომდინარე იქიდან, რომ ხდება მომხმარებლის უფრო მეტი მონაცემების მოგროვება და ხდება ცნობილი მისი პრეფერენციები და სხვა აქტივობა სისტემასთან მიმართებაში.

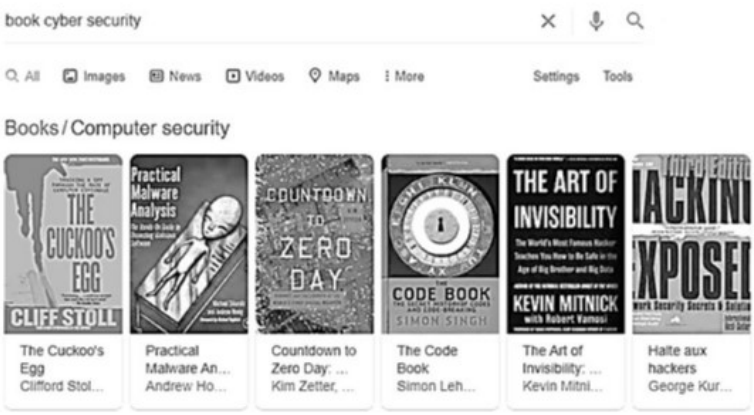
## კონტენტზე დაყრდნობილ სისტემებში გამოყენებული კონცეფცია

შინაარსზე დაფუძნებულ მექანიზმებში გამოყენებული ცნებები ხშირად ეყრდნობა ინფორმაციის აღდგენის სისტემებს. ინფორმაციის მოძიების ეს სისტემები მომხმარებელს უზრუნველყოფს შესაბამისი ძიების შედეგებითა და ამავე დროს ისინი აანალიზებენ მომხმარებლის ქცევას. ეს აძლევს ამ სისტემებს შესაძლებლობას დაადგინონ, არის თუ არა მომხმარებლის ძებნის მოთხოვნა სასარგებლო. ეს პროცესი ემყარება განსხვავებული კომბინაციის ალგორითმებს, რომლებიც ხელს უწყობენ თითოეული მომხმარებლის მოთხოვნის ძიების პროცესს. ჩვენ ვხედავთ აღნიშნული ალგორითმების მუშაობას პრაქტიკაზე, როდესაც ვიყენებთ ძებნას ისეთი ძრავები, როგორიცაა Google ან Yahoo. ასეთი ტიპის საძიებო სისტემებში, ინფორმაცია აღდგენის სისტემები უფრო რთულია და მუშაობს უზარმაზარ მონაცემებთან, რაც ეყრდნობა ინტერნეტის მომხმარებლების მოთხოვნებს. საძიებო სისტემების მუშაობა შეიძლება ნათლად ჩანს, თუ შევადარებთ სხვადასხვა ძიების შედეგების შედეგებს (სურათი 2):

- Cyber security news;
- News on cyber security;


**სურ2.** საძიები სისტემის შედეგების დემონსტრაცია

როგორც ვხედავთ ორივე საძიებო მოთხოვნის (სურათი 2) შედეგები საკმაოდ მსგავსია. ასევე უნდა აღინიშნოს, რომ თუ ჩვენ შევასრულებთ ისეთ საძიებო მოთხოვნას, როგორიცაა მაგალითად „წიგნები კიბერ უსაფრთხოება", ჩვენ სულ სხვა შედეგს ვიღებთ. საძიებო სისტემა გვთავაზობს უსაფრთხოებასთან დაკავშირებული სხვადასხვა წიგნებს ინტერნეტში. და ასეთი შედეგი უკვე განსხვავებულია, მაგრამ საინტერესო ისაა, თუ როგორ შეუძლია საძიებო სისტემას ამოიცნოს საძიებო მოთხოვნა და მიაწოდოს მომხმარებელს შესაბამისი ინფორმაცია. საძიებო ძრავები აგროვებენ ინფორმაციას, რომელსაც მომხმარებლები აწვდიან საძიებო მოთხოვნების დროს და ამ შედეგის საშუალებით საძეობი სისტემას შეუძლია ანალიზი და შესატყვისი შინაარსში სხვადასხვა საძიებო ობიექტების პოვნა. შედეგი მიიღწევა ტექსტის მოპოვების ტექნიკის გამოყენებით. თანამედროვე საძიებო სისტემები განსხვავებული ტექსტის მოპოვების ტექნიკას იყენებენ. ყველაზე აშკარა ტექნიკა ტექსტის მოპოვებისთვის არის TF მატრიცა (ტერმინის სიხშირის მატრიცა). ამ ტექნიკის საფუძველზე კონტექსტში ყველაზე ხშირად გავრცელებულ სიტყვას უფრო მეტი აქტუალობა აქვს. საძიებო სისტემა იყენებს TF- ს მატრიცას, რომ გააანალიზოს თითოეული სიტყვის სიხშირე საძიებო სისტემაში, რომელსაც ითხოვს მომხმარებელი.




**სურ 3.** საძიები სისტემის შედეგების დემონსტრაცია წიგნების მაგალითზე

შინაარსობრივი ტერმინების წონა

სარეკომენდაციო სისტემებში გამოიყენება ორი ძირითადი მექანიზმი. ეს არის მექანიზმები ტერმინის სიხშირისთვის (TF) და ინვერსიული დოკუმენტის სიხშირისთვის (IDF). ჩვენ შეგვიძლია გამოვყოთ სხვადასხვა შინაარსის ვებსაიტებისთვის გამოყენებული სიტყვების სიხშირე. ჩემი კვლევის ფარგლებში დამუშავდა შემდეგი ორგანიზაციების ვებ – გვერდები:

1. სამეცნიერო კიბერ უსაფრთხოების ასოციაციის ოფიციალური ვებგვერდი;
2. Utoweb სტუდიის ოფიციალური ვებ – გვერდი;
3. საბავშვო კიბერ უსაფრთხოების უნივერსიტეტის ოფიციალური ვებ – გვერდი.

გამოსახულება 4 ასახავს თითოეული სიტყვის სხვადასხვა სიხშირის დათვლის შედეგებს ვებსაიტის შინაარსი:

| | Frequency of the word | | | | | |
|---|---|---|---|---|---|---|
| **Website** | security | website | student | team | university | design |
| 1 | 120 | 28 | 15 | 17 | 9 | 1 |
| 2 | 25 | 85 | 0 | 5 | 0 | 75 |
| 3 | 85 | 105 | 55 | 0 | 1 | 1 |

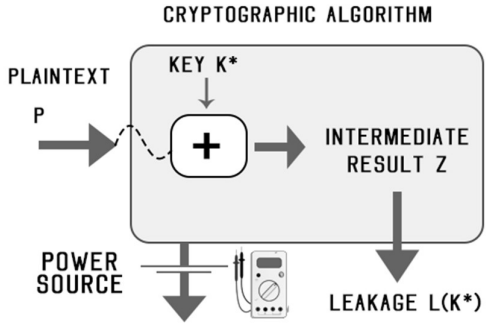
**სურ 4.** ტერმინების სიხშირე

ტერმინების სიხშირის შესამოწმებლად, ზემოთ აღნიშნულ ვებ – გვერდებზე უნდა დაითვალოს სიტყვების წარმოქმნის რაოდენობა. მაგალითად, ის ფაქტი, რომ კონკრეტული სიტყვა "X" პირველ ვებ – გვერდზე გვხვდება 20 – ჯერ, ხოლო მეორე ვებ – გვერდზე ოთხჯერ, არ ნიშნავს რომ სიტყვა „X“ პირველ ვებგვერდზე ხუთჯერ უფრო აქტუალურია, ვიდრე მეორეში. სხვაობა ამ შემთხვევაში გაცილებით ნაკლებია. "ტერმინი სიხშირე" - სთან ერთად უნდა გავითვალისწინოთ ”ინვერსიული დოკუმენტის სიხშირე” (IDF), რომელიც ზომავს რამდენად მნიშვნელოვანია კონკრეტული ტერმინი დოკუმენტში. ტერმინის სიხშირე (TF) ჩვეულებრივ იყოფა დოკუმენტის ზომაზე და გვიჩვენებს შინაარსის კონკრეტული პირობების საერთო რაოდენობას:

TF (A) = რამდენჯერ გამოჩნდება ტერმინი A დოკუმენტში და იყოფა ჯამზე ამ დოკუმენტის ტერმინების რაოდენობა. რადგან ინვერსიული დოკუმენტის სიხშირე (IDF) ზომავს ტერმინის მნიშვნელობას გასათვალისწინებელია, რომ ისეთი შემთხვევები, როგორიცაა "the", "of", "or", "is" შეიძლება აღმოჩნდეს ბევრი შინაარსში, მაგრამ ნაკლები წონა ექნება. ბალანსის მიღება შესაძლებელია შემდეგი ფორმულით:

IDF (A) = log_e (ყველა დოკუმენტის რიცხვი გაყოფილი დოკუმენტების რაოდენობაზე შინაარსით A). მაგალითად, ჩვენ გვაქვს ტერმინი A, რომელიც 3-ჯერ გვხვდება D დოკუმენტში, რომელიც ჯამში შეიცავს 100 სიტყვას, TF ტერმინისთვის გამოითვლება (3/100) = 0,03.

**გვერდითი არხის თავდასხმა პრაქტიკაზე** - დღეისთვის გვერდითი არხის თავდასხმები მიკროკონტროლერებზე არის ძალიან გავრცელებული სურათი 5 ახდენს ამ თავდასხმის პროცესის დემონსტრაციას. მაგალითში ნაჩვენებია თავდასხმა AES - ის პროგრამულ




რეალიზაციაზე.

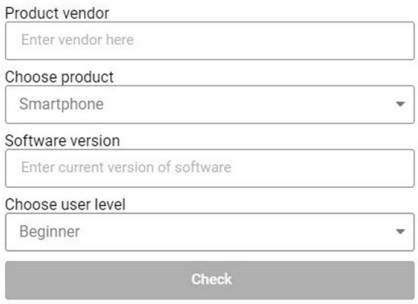
**სურ 5**. გვერდითი არხის თავდასხმა

ამ თავდასხმის მიზანია კრიპტოგრაფიული ალგორითმის ფარული $k^*$ გასაღების მიღება. თავდამსხმელს შეუძლია შეყვანილი $p$ მონაცემების და მიკროკონტროლერის ელექტრომოხმარების გაანალიზება. შიფრაციის ალგორითმი ამ შემთხვევაში უკვე ცნობილია. ერთადერთი რამ, რაც არ არის ცნობილი ფარული გასაღები $k^*$-ია. თავდამსხმელს შეყვანილი $p$-ს მიხედვით შეუძლია შუალედური z შედეგის მიღება. შუალედური შედეგი z ეფუძნება შეყვანილ $p$ მონაცემებს და $k^*$ ფარულ გასაღებს. გვერდითი არხის გაჟონვის გაანალიზებით ხდება ცნობილი შუალედური $z$ და შეიძლება გაკეთდეს ჰიპოტეზური ტესტი $k^*$-ზე. გაჟონილი ინფორმაცია რომელიც გამოწვეულია $z$ - ით შეიძლება იყოს წარმოდგენილი ფუნქციით გასაღების მნიშვნელობით $k^*$.

$$L(k^*) = f_{k^*}(p) + \varepsilon \qquad (1)$$

ფუნქცია $f_{k^*}$ დამოკიდებულია კრიპტოგრაფიულ ალგორითმზე და რეალიზაციის მეთოდებზე პროგრამულ და აპარატულ უზრუნველყოფაში. ფუნქციიდან ჩნდება შეცდომის ε რომელიც ხმაურის ცვლადს წარმოადგენს და არის დამოუკიდებელი.

**შემუშავებული სისტემა**




**სურ 6.** სისტემის ინტერფეისის ნაწილი

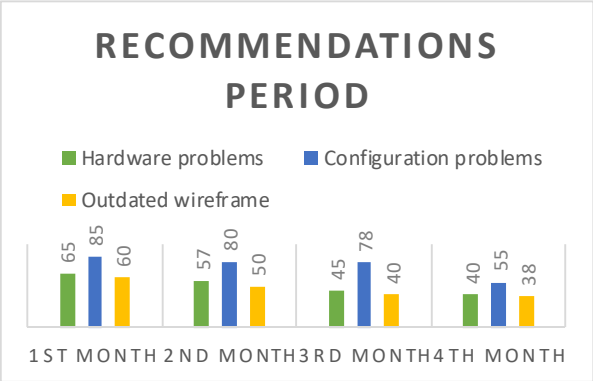
სისტემა, რომელიც შემუშავდა კვლევის ფარგლებში შეყვანილი მონაცემების საფუძველზე ახდენს აპარატურულ უზრუნველყოფაზე დაფუძნებული სქემების უსაფრთხოების დონის დადგენას. მსგავსი ტიპის შეფასება შეიძლება მოხდეს როგორც საოფისე, ასევე ინდუსტრიულ და IoT გარემოში. წარმოდგენილი სისტემა არის შექმნილი web აპლიკაციის სახით, რომელიც ვრცელდება ღია წყაროს მოდელით (open source). სისტემა თავის შეფასების მეთოდებში იყენებს სპეციალიზირებულ მონაცემთა ბაზებს, რომლებშიც ინახება ინფორმაცია თანამედროვე და აქტუალური უსაფრთხოების პრობლემების და თავდასხმების შესახებ. ამ პლატფორმებში შედის ისეთი რესურსები როგორიცაა AttackerKB, CVE MITRE და ExploitDB. სისტემაში ხდება ზემოაღნიშნული ბაზებიდან აქტუალური და განახლებადი ინფორმაციის მიღება. სისტემაში მონაცემები ნაწილდება რამდენიმე კატეგორიის მიხედვით: აპარატურული უსაფრთხოებაზე თავდასხმის ვექტორები, ახალი სისუსტეები არსებულ პროდუქტებში და მოწყვლადობა სისტემების განუახლებელ ვერსიებში. არსებული ინფორმაციის დამუშავების საფუძველზე, სისტემის მიერ ხდება შესაბამისი რეკომენდაციის გაცემა.

სისტემის სამუშაო მექანიზმი ეფუძნება ინფორმაციის მოგროვებას კონკრეტული აპარატურლი უზრუნველყოფის მიხედვით. ერთ-ერთი ყველაზე პოპულარული თავდასხმების ტიპი აპარატურულ უზრუნველყოფაზე არის ე.წ. გვერდითი არხის (side-channel) თავდასხმა. კვლევის ფარგლებში შექმნილ სისტემას აქვს შესაძლებლობა დაადგინოს გვერდითი არხის გაჟონვა საშუალო შედეგით $z$. ეს გაჟონვა შეიძლება იყოს წარმოდგენილი ფუნქციის სახით რომლის გასაღების მნიშვნელობაა $k^*$, სისტემას შეუძლია შეაფასოს გაჟონვის შესაძლებელი დონე შესაბამისი პარამეტრების გამოყენებით და ხმაურის დამოუკიდებელი $\varepsilon$ ცვლადით.

## შედეგების განხილვა

კვლევის ფარგლებში, მოხდა შექმნილი სისტემის შემოწმება სხვადასხვა მოწყობილობებზე და ტექნიკაზე ორიენტირებულ პროგრამულ პლატფორმებზე, რომლებიც სხვადასხვა ორგანიზაციას ეკუთვნის. ტესტირების პერიოდი იყო ოთხი თვე. ამრიგად, ჩართულმა ორგანიზაციებმა თვეში ერთხელ გამოსცადეს თავიანთი სისტემები, რათა მოგვაწოდონ მონაცემები, რომლებიც აუცილებელია უსაფრთხოების დონის გაუმჯობესების თვალსაზრისით. მოწყობილობები,

რომლებიც ყოველდღე გამოიყენება სხვადასხვა ორგანიზაციებში სხვადასხვა მიზნებისთვის, სადაც ტესტირება ხდება წარმოდგენილი სისტემის გამოყენებით. ამრიგად, იგი გამოიყენეს დარეგისტრირებულმა ორგანიზაციებმა და შეგროვებული მონაცემების საფუძველზე შეიქმნა რეკომენდაციების სრული სია, რომლებიც სინთეზურად არის წარმოდგენილი სურათზე 7.




**სურ 7.** სარეკომენდაციო პერიოდი

შეგროვებული მონაცემები ეხება კიბერუსაფრთხოებასთან დაკავშირებული სამი კატეგორიის პრობლემას: აპარატურის პრობლემებს, კონფიგურაციის პრობლემებს და მოძველებულ ქსელურ სტრუქტურებს. ამრიგად, აღმოჩნდა, რომ უსაფრთხოების ყველაზე გავრცელებული საკითხი ეხებოდა აპარატურის არასწორ კონფიგურაციას, რამაც შეიძლება მომავალში სერიოზული პრობლემები გამოიწვიოს. შესაბამისად, ჩართულ ორგანიზაციებს მიეწოდათ შესაბამისი რეკომენდაციები.

დღეს კომპიუტერული მეცნიერების თეორიასა და პრაქტიკაში სტანდარტული კრიპტოგრაფიული ალგორითმები უსაფრთხოდ ითვლება კლასიკური კომპიუტერების შეტევისგან. ხაზგასმით უნდა აღინიშნოს, რომ აპარატურაზე დაფუძნებულ გვერდითი არხების შეტევებმა შეიძლება გაჟონოს ინფორმაცია შიფრის შესახებ. ეს დღეს კომპიუტერულ მეცნიერებაში დიდი პრობლემაა. სისტემით, რომელსაც ამ კვლევის ფარგლებში ვთავაზობ, ამ პრობლემის მოგვარება შეიძლება. თანამედროვე ტექნიკაზე დაფუძნებული სისუსტეების ამოცნობის სისტემა იყენებს ახალ მიდგომას პრობლემის გასაანალიზებლად კონკრეტული სცენარის საფუძველზე. ახალი მიდგომა იყენებს ცნობილ ტექნიკურ მოწყვლადობის მონაცემთა ბაზებს, გაანალიზებული სისტემის მდგომარეობის გათვალისწინებით. ტექნიკურ ბაზაზე დაფუძნებული სხვადასხვა შეტევები წარმატებით ხორციელდება ბიზნესის, განათლებისა და ფინანსური სფეროების ცნობილ სისტემებზეც კი. ეს ფაქტი თანამედროვე რეკომენდაციების სისტემას უნიკალურ და არსებულ სიტუაციასთან შესაბამისობაში აქცევს. ეს ნიშნავს, რომ გათვალისწინებული მიდგომის საფუძველზე, მრავალ ორგანიზაციას, რომელიც მუშაობს სხვადასხვა მიმართულებით, შეუძლია შეავსოს უსაფრთხოების ხარვეზები ტექნიკურ სისტემებზე და, შესაბამისად, გაზრდის მათ უსაფრთხოების დონეს.

რეკომენდაციების სისტემაში გამოყენებული მეთოდები ემყარება პრაქტიკულ ანალიზის მიდგომებსა და პოპულარულ მონაცემთა ბაზებს. ეს ფაქტი რეკომენდაციებს შესაბამის და სასარგებლოს ხდის როგორც საბოლოო მომხმარებლებისთვის, აგრეთვე ორგანიზაციებისათვის.

**ACKNOWLEDGEMENTS**

ნამუშევარი შესრულებულია შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის მიერ დაფინანსებული PHDF-19-519 პროექტის ფარგლებში.

## ბიბლიოგრაფია

1. Taehyun K. Reinforcing Meltdown Attack by using a Return Stack Buffer / K.Taehyun, S. Youngjoo // IEEE Access - 2019 - P. 186065 – 186077. DOI: 10.1109/ACCESS.2019.2961158
2. ZombieLoad: Cross-Privilege-Boundary Data Sampling / [M. Schwarz, M. Lipp, D. Moghimi, et al.] // ACM SIGSAC Conference on Computer and Communications Security, London, 11-15 November 2019: proceedings. ACM CCS 2019 - P. 753–768.
3. Clavier C. Differential power analysis in the presence of hardware countermeasures / C. Clavier, J-S Coron, N Dabbous // CHES – 2000, Worcester 17-18 August, 2000 - P. 252–263.
4. Schaumont P. Masking and dual-rail logic don't add up / P Schaumont, K Tiri // Cryptographic hardware and embedded systems, Vienna 10-13 September 2007: proceedings. CHES 2007 – P. 95–106.
5. Abomhara M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks / M. Abomhara, Geir M. Køien // Journal of Cyber Security and Mobility – 2015 – Vol. 4, Issue 1. - P. 65-68.
6. Ishai Y. Private Circuits: Securing Hardware against Probing Attacks / Y. Ishai, A.Sahai, D. Wagner. // Advances in Cryptology, Santa Barbara 17-21 August 2003: proceedings. CRYPTO 2003 - Vol. 2729 – P. 463-481.
7. Dan P. Theoretical Use of Cache Memory as a Cryptanalytic Side-Channel / P. Dan // IACR Cryptology ePrint Archive. - 2002. – Vol. 169 – P. 170-184.
8. Samer M. Hardware attacks: an algebraic approach / M. Samer, G. Fayez, G. T. Aaron // Journal of Cryptographic Engineering. – 2006. – Vol. 6 – P. 325-337. DOI: 6. 10.1007/s13389-016-0117-6
9. Hardware attack risk assessment / [M. Samer, F. Gebali, T. Gulliver et al.] // ICES. – 2015. - Vol. 1109. DOI: 10.1109/ICCES.2015.7393073
10. Voyiatzis A. Active hardware attacks and proactive countermeasures / A.Voyiatzis , D. Serpanos // International Symposium on Computers and Communications, Taormina 1-4 July 2002 – Vol. 10 - P. 361 - 366. DOI: 10.1109/ISCC.2002.102170
11. Bouffard G. Combined Software and Hardware Attacks on the Java Card Control Flow / G . Bouffard, J .Iguchi-Cartigny, JL. Lanet // Prouff E. (eds) Smart Card Research and Advanced Applications. – 2011. - Vol. 10 – Issue 2. - P. 283-296. DOI: 10.1007/978-3-642-27257-8_18
12. Exploiting the analog properties of digital circuits for malicious hardware / [Y. Kaiyuan, H. Matthew, D. Qing et al.] // Communications of the ACM – 2017- Vol. 60 – P. 83-91. DOI: 10.1145/3068776

13. Hardware Trojan Attacks: Threat Analysis and Countermeasures / [S. Bhunia, M. S. Hsiao, M. Banga et al.] // International Conference on Communications (ICC), Sydney, 10-14 June 2014: proceedings. – IEEE ICC, 2014 - P. 1229-1247.
14. Lattice Based Merkle / [M. Iavich, G. Iashvili, A. Gagnidze et al.] // IVUS 2019, Kaunas 25 April 2019: proceedings. - CEUR-WS - 2019 – vol. 2470 – P.13-16.
15. Protection against Hardware Trojan Attacks: Towards a Comprehensive Solution / [S. Bhunia, M.Abramovici, D. Agrawal et al.] // IEEE Design & Test – 2013. - Vol. 30 - P. 6-17.
16. Gagnidze A. Novel Version of Merkle Cryptosystem / A. Gagnidze, M. Iavich, G. Iashvili // Bulletin of the Georgian National Academy of Sciences. – 2017. – Vol. 11, Issue 4. – P. 28 – 33.
17. Deogirikar J. Security attacks in IoT: A survey / J. Deogirikar, A. Vidhate // International conference IoT in Social, Mobile, Analytics and Cloud, Coimbatore 10-11 February 2017: proceedings. IEEE, 2017 – P. 32-37.
18. Ronen E. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights / E. Ronen ,A. Shamir // European Symposium on Security and Privacy, Saarbrücken 21-24 March 2016: proceedings. IEEE, 2016 – P. 3-12.

**Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 12-17 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# IDENTIFICATION OF CYBER ATTACKS ON INFORMATION NETWORKS WITH A RANDOM MOMENT OF ITS APPEARANCE

# ВЫЯВЛЕНИЕ КИБЕРАТАК В ИНФОРМАЦИОННЫХ СЕТЯХ СО СЛУЧАЙНЫМ МОМЕНТОМ ЕЕ ПОЯВЛЕНИЯ

**Volodymyr Khoroshko, National Aviation University, Doctor of Engineering Science, Full Professor, Kiev, Ukraine,**
**Хорошко Владимир Алексеевич, доктор технических наук, профессор, профессор Национального авиационного университета (г. Киев).**

**Mykhailo Shelest, Chernihiv Polytechnic National University, Doctor of Technical Science, Full Professor, Chernihiv, Ukraine,**
**Шелест Михаил Евгеньевич, доктор технических наук, профессор, профессор Национального университета «Черниговская политехника» (г. Чернигов)**

**Yuliia Tkach, Chernihiv Polytechnic National University, Doctor of Pedagogical Science, Professor, Chernihiv, Ukraine,**
**Ткач Юлия Николаевна, доктор педагогических наук, профессор, завкафедрой кибербезопасности и математического моделирования Национального университета «Черниговская политехника» (г. Чернигов)**

**Nikolay Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor Kiev,**
**Браиловский Николай Николаевич, кандидат технических наук, доцент, доцент Киевского национального университета имени Тараса Шевченко (г. Киев).**

**ABSTRACT:** In information networks, when detecting and recognizing cyber-attacks, they are usually interested not only in the fact of the appearance of a particular attack, but also in its informative parameters. The result of actions performed in solving the problem of the presence of a cyberattack depends on the degree of closeness of the estimate to the true value of the parameters. Therefore, losses in the process of recognizing (detecting) and evaluating a cyberattack depend both on errors in its detection and on the inaccuracy of assessment, which will not allow providing adequate countermeasures, and at the same time the task of joint development and evaluation arises. In practice, the moment of making a decision is very important, since with an increase in the observation time, the costs increase and, therefore, the fastest decision-making is desirable. At the same time, sequential detection-estimation procedures are more effective than inconsistent ones. Therefore, finding the optimal, consistent or close to them procedures will increase the cybersecurity of information.

Some results related to joint sequential detection and estimation, obtained in the works of other authors, show that in the general case it is not possible to find a constructive solution even in a two-alternative problem. Therefore, the authors made an attempt to solve the problem of multi-alternative sequential detection and evaluation of a cyberattack with a random moment of its occurrence.

**АННОТАЦИЯ:** В информационных сетях при обнаружении и распознании кибератак обычно интересуются не только фактом появления той или иной атаки, но и ее информативными параметрами. Результат действий, совершаемых при решении задачи о наличии кибератаки, зависит от степени близости оценки к истинному значению параметров. Поэтому потери в процессе распознания (обнаружения) и оценивания кибератаки зависят как от ошибок в ее выявлении, так и от неточности оценивания, что не позволит обеспечить адекватное противодействие, и при этом возникает задача совместного развития и оценивания. На практике момент принятия решения очень важен, поскольку с увеличением времени наблюдения возрастают затраты и, поэтому, желательно быстрейшее принятие решений. При этом последовательные процедуры обнаружения-оценивания, имеют большую эффективность

по сравнению с непоследовательными. Поэтому нахождения оптимальных, последовательных или близких к ним процедур, позволит повысить кибербезопасность информации.

Некоторые результаты, связанные с совместным последовательным обнаружением и оцениванием, получены в работах других авторов, показывают, что в общем случае найти конструктивное решение не удается даже в двухальтернативной задаче. Поэтому авторами была сделана попытка решить задачу многоальтернативного последовательного обнаружения и оценивания кибератаки со случайным моментом ее появления.

**KEYWORDS:** *analysis of the processes of attack and counteraction in the information space, sequential detection and assessment of cyberattacks, multi-alternative tasks.*

**КЛЮЧЕВЫЕ СЛОВА***: анализа процессов нападения и противодействия в информационном пространстве, последовательное обнаружение и оценивание кибератак, многоальтернативные задачи.*

## Введение

При рассмотрении проблемы кибербезопасности информации необходимо учитывать возможные виды несанкционированных действий (кибератак) ведущих к потере или модификации данных. Выявление, предотвращение или существенное затруднение действия кибератак (КА) – одно из центральных направлений области кибербезопасности в информационных сетях. Определение обобщенных требований по киберзащите информационных сетей от кибератак на информацию и оценка степени их защищенности представляют достаточно сложными задачами. Опыт практической эксплуатации информационных сетей в различных сферах деятельности государства показывает, что существуют реальные угрозы КА, приводящие к негативному воздействию на составляющие кибербезопасности.

Существуют реальные возможности возникновения непредвиденных ситуаций в следствии воздействия КА, ведущие к утрате информации либо к ее потере и потере работоспособности информационной сети. В концепции кибербезопасности информационной сети на основе угроз от КА должны определяться требуемые средства, методы и процедуры обнаружения и оценивания КА в сетях [1].

Имеет место процесс разграничения разных видов угроз. При этом необходимость понимания роли КА и кибербезопасности связана в первую очередь с активизацией международных террористических, экстремистских организаций и преступных группировок, а также отдельных государств, которые осуществляют кибератаки и кибервоздействия на граждан, общество и государства с целью реализации своих интересов.

При этом в условиях ведения гибридных войн в последние годы систематически осуществляются различные КА, кибервоздействия и несанкционированные действия в информационных сетях, что подрывает экономическую, военную, техническую и другие сферы не только государства, но и отдельных его отраслей [1,2].

Поэтому для эффективного функционирования информационных сетей в современных условиях и средств их защиты, а также для надежного обнаружения и оценивания КА необходимо развивать новые подходы и методы, их реализации.

## Основная часть

При обнаружении и распознании кибератак обычно интересуются не только фактом появления той или иной атаки, но и ее информативными параметрами. Результат действий, совершаемых при решении задачи о наличии кибератаки, от степени близости оценки к истинному значению параметров. Поэтому потери в процессе распознания (обнаружения) и оценивания кибератаки зависит как от ошибок в ее выявлении, так и от неточности оценивания, что не позволит обеспечить адекватное противодействие, и при этом возникает задача совместного развития и оценивания [3,4]. Причем на практике момент принятия решения обычно не безразличен, поскольку с увеличением времени наблюдения, затраты возрастают и

желательно быстрейшее принятие решений. При этом последовательные процедуры обнаружения-оценивания, вообще говоря, имеют большую эффективность по сравнению с непоследовательными. Поэтому актуальность нахождения оптимальных, последовательных или близких к ним процедур, что позволит повысить кибербезопасность информации.

Некоторые результаты, связанные с совместным последовательным обнаружением и оцениванием, получены в [5]. Как следует из [5], в общем случае найти конструктивное решение не удается даже в двухальтернативной задаче. Поэтому попытаемся решить эту задачу многоальтернативного последовательного обнаружения и оценивания кибератаки со случайным моментом ее появления.

Пусть событие $\{\theta = 1\}$ означает наличие кибератаки (КА), которая может появиться в момент $\infty > \lambda_n = \lambda_0 > 0$, n ≥ 1, причем $\pi_{01} = P(\theta = 1) = P(\lambda_0 < \infty) < 1$ $(\pi_{00} = P(\theta = 0) = P(\lambda_0 = \infty) = 1 - \pi_{01})$. Положим, что $x_n,\ n \geq 1$, независимы или как до так и после появления КА, так что справедлива модель [6]

$$P_0(x_1^n) = p(x_1^n|\theta = 0) = \prod_{i=1}^{n} p_{oi}(x_i) = p(x_1^n|\theta = 1, \lambda_0 > n\Delta);$$

$$p_{11}(x_1^n|\lambda) = p(x_1^n|\theta = 1, \lambda_0 = \lambda) = \prod_{i=1}^{n} x_{oi}(x_i) P_{\lambda j+1}(x_{j+1}) \prod_{i=j+2}^{n} P_{1i}(x_i),$$

$$j\Delta \leq \lambda \leq (j+1)\Delta, j \leq n-1, n = 1, N,$$

где $P_{\lambda n}(x_n)$ – плотность, зависящая от $\lambda$ причем

$$P_{\lambda n}(x_n) = \begin{cases} P_{0n}(x_n) \text{ при } \lambda = n\Delta, \\ P_{1n}(x_n) \text{ при } \lambda = (n-1)\Delta; \end{cases}$$

принятая при рассмотрении в [6] задачи обнаружения сбоя последовательности без оценки его момента.

Задача состоит в построении оптимальной N-усеченной последовательной процедуры совместного обнаружения КА и оценивания момента ее появления при функции потерь:

$$g(\theta, \lambda, u_n, n) = \begin{cases} g_{01}(n), \theta = 0,\ u_n = (1, \lambda_n), \\ \widetilde{g_{11}}(n)\ \theta = 1, \lambda \geq n\Delta, u_n = \left(1, \hat{\lambda}_n\right), \\ g_{11}(n) + c(n - [\lambda]) + F_n\left(\lambda - \hat{\lambda}_n\right)^2, \theta = 1, \\ \lambda < n\Delta, u_n = \left(1, \hat{\lambda}_n\right), n = \overline{1, N} \end{cases} \quad (1)$$

где с-стоимость задержки в вычислении решения о наличии КА $u_n$ ее появления на один шаг; $[\lambda] = i$ при $(i-1)\Delta < \lambda \leq i\Delta$ (i – интервал между отсчетами).

Решение $u_n = 0$ на шагах n=1, N-1 эквивалентно по решению $u_n$ о продолжении наблюдений [6]. На N-м шаге это решение является окончательным, поскольку процесс $\{x_n\}$ наблюдению более недоступен и потери $g(\theta, \lambda, u_n = 0, N)$ связанные и имеют вид:

$$g(\theta, \lambda, u_n, N) = \begin{cases} g_{00}(N), \theta = 0,\ u_n = 0, \\ g_{10}(N) + c(N - [\lambda]), \theta = 1, \lambda < N\Delta, u_n = 0, \\ \tilde{g}_{10}(N)\ \theta = 1, \lambda \geq N\Delta, u_n = 0. \end{cases} \quad (2)$$

Функция потерь (1), (2) отличается от [4]

$$g_{ij}\left(\lambda_n^{(i)}, \hat{\lambda}_n^{(j)} n\right) = \begin{cases} g_{ii}(n) + w_n\left(\lambda_n^{(i)} - \lambda_n^{(j)}\right) \text{ при } i, j \neq 0, \\ g_{j0}(n) \text{при } i = 0, j = \overline{0, m-1}, \\ g_{i0}(n) \text{ при } j = 0, i = \overline{0, m-1}, \end{cases} \quad (3)$$

где $w_n$ – неубывающая неотрицательная функция, определяющая зависимость потерь от неточности оценивания информационного параметра не зависящая от принимаемых гипотез и истинной гипотезы; тем, что от значений информационного параметра зависят не только потери за счет неточности его оценивания, но и сама величина $g_{ij}(n, \lambda)$.

Например $g_{11}(n, \lambda) = g_{11}(n) + c(n - [\lambda])$ при $\lambda \leq n\Delta,\ g_{11}(n, \lambda) = \widetilde{g_{01}}(n)$ при $\lambda > n\Delta$. В частном случае, когда

$$C = 0, g_{11}(n) = \widetilde{g_{11}}(n), g_{10}(N) = \tilde{g}_{10}(N) \quad (4)$$

потери (1), (2), (3) совпадают и можно воспользоваться результатами, получаемыми в [7]. Используя (1), нетрудно показать, что оптимальная оценка отличается от результатов, полученных в [7] – она представляет собой среднее апостериорное распределение $P(\lambda_0 \le \lambda | x_1^n, \theta = 1, \lambda \le n\Delta)$ с плотностью $\widetilde{p_{01}}(\lambda) = p_1(x_1^n|\lambda)p(\lambda)/[\int_0^{-n\Delta} p_1(x_1^n|\lambda)p(\lambda)d\lambda], \lambda \le n\Delta,$

$p(\lambda)$-плотность априорного распределения $\prod(\lambda) = P_0(\lambda_0 \le \lambda | \theta = 1)$ т.е.

$\widetilde{\lambda_n^0} = \int_0^{n\Delta} \lambda \widetilde{p_{01}}(\lambda) d\lambda$ поскольку $w_n(\lambda - \widehat{\lambda_n}) = \begin{cases} F_n(\lambda - \widehat{\lambda_n})^2, \lambda < n\Delta \\ 0, \lambda \ge n\Delta \end{cases}$

Введем обозначение: $m_n^{(i)}(x_1^n) = M[\lambda_0^i | x_1^n, \theta = 1, \lambda_0 \le n\Delta], i \ge 1;$

$$D_n(x_1^n) = M[\left(\lambda_0 - m_n^{(i)}\right)^2 | x_1^n, \theta = 1, \lambda_0 \le n\Delta] \quad (5)$$

– i-й нецентральный момент и дисперсия апостериорного распределения;

$L_n(x_1^n)$ – статистика, связанная с усредненным объёмом прогноза (УОП)

$$\wedge_n (x_1^n) = \int_0^{\infty} [p_1(n_1^n|\lambda)/p_0(x_1^n)]\, p(\lambda) d\lambda \quad (6)$$

Используя (2), можно показать [8], что для $\{m_n^{(i)}\}$ справедливы рекуррентные равенства.

$$m_{n+1}^{(i)} = L_n L_{n+1}^{-1} \left\{ \gamma_{n+1}(x_{n+1}) m_n^{(i)} + \frac{\nu_{n+1}^{(i)}}{L_n} \right\}, n \ge 0, m_0^{(i)} = 0, i \ge 1 \quad (7)$$

Здесь $\gamma_n(x_n) = \frac{p_{1n}(x_n)}{p_{0n}(x_n)}$ статистика $L_n$ удовлетворяет рекуррентному соотношению [3]:

$L_{n+1} = \beta_{n+1}(x_{n+1}) + \gamma_{n+1}(x_{n+1}) L_n, n \ge 0, L_0 = 0$

Следовательно $\nu_n^{(i)}(x_n) = \int_{(n-1)\Delta}^{n\Delta} \lambda^i \frac{p_{\lambda n}(x_n)}{p_{0n}(x_n)} p(\lambda) d\lambda, i \ge 0$ причем $\nu_n^0(x_n) = \beta_n(x_n)$.

При i = 1 соотношение (7) задает алгоритм формирования оптимальной оценки момента выявления КА (6), при i = 2 – второго апостериорного момента. Также

$$D_n(x_1^n) = m_n^{(2)}(x_1^n) - [m_n^{(1)}(x_1^n)] \quad (8)$$

с помощью (7), (8) и [5] определяется апостериорная дисперсия, а значит

$$\varphi^0(x_1^n, n) = F_n D_n(x_1^n) \quad (9)$$

Если сбой последовательности при появлении КА происходит, т.е.

$$P_{\lambda n}(x_n) = p_{1n}(x_n) \text{ для всех } \lambda \in [(n-1)\Delta, n\Delta], \quad (10)$$

либо КА может появится лишь в дискретные моменты $n\Delta, n = 0,1,2 \ldots$

$$p(\lambda) = p_n \delta(\lambda - n\Delta), (\textstyle\sum_{n \ge 0} p_n = 1), \quad (11)$$

то $\nu_{n+1}^{(i)} = \alpha_{n+1}^{(i)} \gamma_{n+1}(x_{n+1})$ и из [3], (7) следует, что

$$m_{n+1}^{(i)} = L_n (\alpha_{n+1}^0 + L_n)^{-1} \left( m_n^{(i)} + \frac{\alpha_{n+1}^{(i)}}{L_n} \right), n \ge 0, m_0^{(i)} = 0, i \ge 1 \quad (12)$$

где $\alpha_{n+1}^{(i)} = \int_{n\Delta}^{(n+1)} \lambda^i p(\lambda) d\lambda;\ \alpha_{n+1}^{(0)} = \alpha_{n+1}.$

Из 12 следует, что значение любого момента апостериорного распределения (5) на $(n+1)$ – м шаге при выполнении (10) или (11) зависит лишь от n наблюдений, причем посредством $(L_n, m_n^{(i)})$:

$$m_n^{(i)}(x_1^{n+1}) = m_{n+1}^{(i)}(x_{n+1}) = m_{n+1}^{(i)}(L_n, m_n^{(i)}) \quad (13)$$

В более общем случае (7,8, [5]) можем записать

$$m_n^{(i)}(x_1^{n+1}) = m_{n+1}^{(i)}\left(x_{n+1}, m_n^{(i)}, L_n\right), i \ge 1 \quad (14)$$

$$D_{n+1}(x_1^{n+1}) = D_{n+1}(S_{n+1}) = D_{n11}(x_n, x_{n+1}), \quad (15)$$

где $S_n = \left(m_n^{(1)}, m_n^{(2)}\right); Z_n = (L_n, S_n).$

В силу выражения (14) $Z_n$–транзитивная статистика

$$Z_{n+1}(x_1^{n+1}) = Z_{n+1}(x_{n+1}, Z_n), n \ge 0 \quad (16)$$

Статистика $\pi_n$ связана с $L_n$ равенством

$$\pi_n = \frac{\nu(L_n + A_n)}{[1 + \nu(L_n + A_n)]}, \quad (17)$$

$A_n = P(\lambda_0 \ge n\Delta | \theta = 1), \nu = \frac{\pi_{01}}{1 - \pi_{01}}$.

Из (14), (16), (17) следует, что условия принятые в [9] выполнены, причем $T_n = Z_n = (L_n, S_n), S_n = (m_n^{(1)}, m_n^{(2)}), S_{n+1} = S_{n+1}(x_{n+1}, Z_n).$

Таким образом, можно воспользоваться теоремой [10]: последовательность $\{Z_n, n = 1, n\}$ является достаточной, а оптимальная процедура последовательного обнаружения-оценивания имеет вид приведенный в [11], где T=$Z_n$ – трехмерная статистика согласно (9), (15), причем в соответствии с [10] $V_{n0}^N = V_{nn}^N, n = 1,\ N = 1$.

В том случае, когда (4) не выполнено, непосредственно применить теорему [10] невозможно и задача немного усложняется, однако трёхмерная статистика $Z_n = = (L_n, m_n^{(1)}, m_n^{(2)})$ остается достоверной и в этом случае. Действительно, используя (1) и (17), нетрудно показать, что

$$R_{n1}\left(x_1^n, \widehat{\lambda_n^0}\right) = \Gamma_{n1}(Z_n) = \mathrm{c}\sum_{i=1}^n \widetilde{\pi_{in}}, \quad (18)$$

где $\Gamma_{n1}(Z_n) = (1 + \nu \wedge_n)^{-1}\{\nu L_n[g_{11}(n) + + F_n D_n(S_n)] + g_{01}(n) + \nu \mathrm{A}_n \widetilde{g_{11}}(n)\}$; (19)

$\pi_{in} = P(\lambda_0 < i\Delta | x_1^n)$ – апостериорная вероятность наличия КА и моменту $i\Delta$. Апостериорный риск $R_{No}(x_1^N)$ определяется равенствами из [10]. С помощью (18), (19) и [12] получаем, что оптимальная процедура на N-м шаге имеет вид:

$$u_N^0(Z_n) = \begin{cases} 1, m_N^{(i)}, L_n \geq L_N^0(D_N) \\ 0, L_n \geq L_N^0(D_N) \end{cases}$$

где $L_n$, $m_N^{(i)}$, $D_N$ – находятся в соответствии с (8) и (9), а

$L_N^0(D_N) = \frac{\nu \mathrm{A}_n[\widetilde{g_{11}}(N) - \widetilde{g_{10}}(N) + g_{01}(N) - g_{00}(N)]}{\nu[g_{10}(N) - g_{11}(N) - F_N D_N(S_N)]}$ (20)

- порог, зависящий от апостериорной точности оценивания момента появления КА $\lambda_0$.

Последующие результаты получаем для случая скачкообразного сбоя последовательности при появлении КА, когда выполняется условие (10), либо для случая дискретного распределения момента $\lambda_0$ (11). При этом, как следует из (13) согласно [13]:

$$D_{n+1}(x_0^{n+1}) = D_{n+1}[Z_n(x_1^n)], n \geq 0, \quad (21)$$

где Zn – транзитная статистика. Используя (19) – (21), (16), (18), аналогично [6,14], можно показать, что наименьший апостериорный риск (НАР) в области продолжения наблюдений $V_{n0}^N = V_{n1}^N = [R_{n0}^N(x_1^n) \leq R_{n0}(x_1^n)]$ имеет вид

$$R_{n0}^N(x_1^n) = \tilde{\Gamma}_{n0}^N(Z_n) + \sum_{i=1}^n \tilde{\pi}_{in}, \quad (22)$$

где $\tilde{\Gamma}_{n0}^N(Z_n) = \Gamma_{n0}^N(Z_n) + \sum_{V=1}^{N-n} \frac{D_n^{(\mathrm{V})}(Z_n, N)}{1 + \nu \wedge_n}$, (23)

Величины $D_n^{(V)}$ определяются рекуррентно в соответствии с уравнениями

$$D_n^{(V)}(Z_n, N) = \int D_{n+1}^{(V)-1}[Z_{n+1}(x_{n+1} Z_n), N]\ p_{0n+1}(x_n + 1) dx_{n+1}, v \geq 2, \quad (24)$$

$$D_n^{(1)}(Z_n, N) = F_{n+1} D_{n+1}(Z_n, n, N) v(L_n + \alpha_{n+1}). \quad (25)$$

Функция $\Gamma_{n0}^N$ определяется с помощью [15], в которых Ln заменяется на Zn, так как области

$$X_{n+1}^0(Z_n, N) = [x_{n+1} : \tilde{\Gamma}_{n+10}^N(Z_{n+1}) \leq \tilde{\Gamma}_{n+11}^N(Z_{n+1})]; \quad (26)$$

$$X_{n+1}^1(Z_n, N) = [x_{n+1} : \tilde{\Gamma}_{n+10}^N(Z_{n+1}) > \tilde{\Gamma}_{n+11}^N(Z_{n+1})]$$

зависят не только от Ln , но и от $m_n^{(1)}, m_n^{(2)}$.

Из выражений (18) и (22) следует, что оптимальная процедура последовательного обнаружения-оценивания КА с неизвестным моментом появляется при потерях (1) в общем случае при невыполнении условий (4) имеет вид:

$$u_N^0(Z_n) = \begin{cases} 1, m_N^{(i)}, Z_n \in V_{n1}^N \\ 0, Z_n \notin V_{n1}^N, n = 1, N \end{cases} \quad (27)$$

где $V_{n1}^N = [Z_n : \Gamma_{n1}(Z_n) \leq F_{n0}^N(Z_n)]$ - область остановки наблюдений, причем на N-м шаге процедура определяется соотношениями (19) и (20).

Пользуясь соотношениями (23) – (26), можно показать, что $F_{n0}^N(\pi_n, S_n)$ является непрерывной функцией $\pi_n$ При каждом фиксированном значении Sn. Это свидетельствует о возможности представления правила (27) в виде

$$u_N^0(Z_n) = \begin{cases} \left(1, m_N^{(i)}\right), L_n \geq L_n^0(S_n, N) \\ 0, \qquad L_n < L_n^0(S_n, N), n = 1, N \end{cases} \quad (28)$$

где $L_n^0(S_n, N)$, - порог, находимый из уравнения

$$\tilde{\Gamma}_{n0}^{N}(y, S_n) = \Gamma_{n1}(y, S_n), n = 1, N-1, \quad (29)$$

причем при n = N порог определения равенством (20). Описание выражением (28) может оказаться более удобным с практической точки зрения, нежели (27).

Структура процедур обнаружения вида (27) и (28) остается оптимальной и при невыполнении условий (10) и (11). Однако соотношения (23) – (25) при этом уже не справедливы.

**Выводы**

Таким образом, если в задаче обнаружения без оценивания момент появления КА или при решении задачи обнаружения и оценивания раздельно оптимальная процедура основана на сравнении одномерной статистики Ln с детерминированным порогом, то при совместном решении этих задач оптимальные области остановки и продолжения наблюдений определяется в трехмерном пространстве при помощи равенств (23) – (26).

## Литература


1. Brailovskyi N., Khoroshko V., Kozura V., Kondakova S. Analysis of the Cybersecurity Status of the Information Space. Scientific and Practical Cyber Security Journal (SPCSJ), vol2, #4, december, 2018.-p.64-74.
2. Brailovskyi N., Khokhlacheva Y., Khoroshko V., Ayasrah Ahmad. Evaluation of the Level of Cyber Security of Information. Scientific and Practical Cyber Security Journal (SPCSJ), vol3, #3, september, 2019.-p.18-24.
3. Левин Б.Р. Теоретические основы статистической радиотехники / Б.Р. Левин. – М.: Радио и связь, 1989. – 656 с.
4. Сосулин Ю.Г. Теория обнаружения и оценивание стохастических сигналов. Изд. 2-е / Ю.Г. Сосулин. – М.: Сов. радио, 2001. – 323 с.
5. Ширяев А.Н. Статистический, последовательный анализ. Оптимальные правила постановки. Изд. 3-е, допол./ А.Н. Ширяев. – М.: Наука, 2002. – 282 с.
6. Огірський І.Р. Загальні проблеми прогнозування НСД в інформаційних системах держави / І.Р. Огірський // Правове, нормативне та метрологічне забезпечення системи захисту інформаціх в Україні. Вип. 2 (30), 2015. – С. 31-34.
7. Леман Э. Проверка статистических гипотез. Изд-е 2-е / Э. Леман. М.: Наука, 2000. – 418 с.
8. Кокс Д. Статистический анализ последовательностей событий. Изд-е 2-е доп. / Д.Кокс, П. Лбюис. – М.: Наука, 2001. – 315 с.
9. Суслин Ю.Г. Теория последовательных решений и ее применение. Изд-е 2-е доп. /Ю.Г. Суслин, М.М. Фишман. – М.: Радио и связь, 2005. – 292 с.
10. Де Гроот М. Оптимальные статистические решения. Изд-е 3-е доп. / М. Де Гроот. – М.: Мир, 2004. – 506 с.
11. Иоффе А.Д. Теория экстремальных задач. Изд-е 3-е /А.Д. Иоффе, В.М. Тихомиров. – М.: Наука, 1999. – 558 с.
12. Ковалевский В.Н. Методы оптимальных решений в распознавании изображений. Изд-е 2 доп. / В.Н. Ковалевский. – М.: Наука, 1996. – 348 с.
13. Браіловський М.М. Технології захисту інформації / М.М. Браіловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова – К.: ЦП «Компринт», 2021.-296 с.
14. Козюра В.Д., Захист інформації в комп'ютерних системах: підручник / В.Д. Козюра, В.О. Хорошко, М.Е. Шелест, Ю.М. Ткач, О.О. Балюнов.
15. Закс Ш. Теория статистических выводов. Изд. 2-е доп. / Ш. Закс. – М.: Мир, 1995. – 775 с.

**Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 18-26 ISSN 2587-4667**
**Scientific Cyber Security Association (SCSA)**

# INFORMATION WAR IN MODERN CONDITIONS PART 1

**Volodymyr Khoroshko, National Aviation University, Doctor in Technical Sciences, Professor, Kyiv, Ukraine**
**Volodymyr Artemov, National Aviation University, Doctor of pedagogical sciences, Professor, Kiev, Ukraine**
**Oleksandr Lytvynenko, Taras Shevchenko National University of Kyiv, Doctor in Technical Sciences, Professor, Kyiv, Ukraine**
**Mykola Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor, Kyiv**

**ABSTRACT:** The article deals with direct and reverse optimization of the distribution of information space between countries and states. An algorithm for information warfare of the first and second generation has been developed. The analysis of the confrontation between Russia and Ukraine and the impact of the media model on society have been shown. The concept of the strategy of the information war of the first and second generation has been introduced and it has been proved that a new era of transition from the strategy of nuclear restraint to high-precision counter-force information weapons, the main task of which is mass manipulation, has begun.
**KEYWORDS:** *information warfare, information confrontation, disinformation, psychological impact, information attack*

## Introduction

At all stages of the historical development of human civilization, information has been both the most important object and a means of struggle between peoples, nations, states, military-political blocs and alliances. Some facts of informational influence on a wide audience can be found throughout human history. It is clear that in different periods the intensity of the application of certain methods of influence, as well as the perfection of its organization, differed greatly.

As a result, information and information technology in general have become extremely important for national security and particularly for military security. A number of countries, most notably Russia, have been intensifying the study and resolution of information and information warfare since the 1990s. Thus, the information war has turned from a futurological ghost into a real military discipline, which is being under development and study [1,2,3].

Thus, the geopolitical authority of the state in the international arena and its ability to influence world events today depends not only on economic and military power. Informational factors rather than the power ones are becoming increasingly important, i.e. the ability to effectively influence the intellectual potential of other countries, to disseminate and implement in the public consciousness the relevant spiritual and ideological values, to transform and undermine the traditional foundations of nations and peoples. A new stage is coming in military affairs, which is the transition from a strategy of nuclear deterrence to high-precision counter-force information weapons [4,5].

The role of information struggle is constantly growing in the system of national security of the states. The leading countries of the world, first of all Russia, the USA, France, Germany, Great Britain, Japan, that possess powerful information potential, are constantly increasing it on a scientific basis and at high culture of management.

In these and other countries, the scientific basis for the creation and application of means of information confrontation is the achievement of two main branches of science: cybernetics and computer science, which have been able to integrate many provisions of not only natural but also humanities.

Information is a terrible thing. Now it is indeed the fourth element of state power, which very often comes to the fore in the 21st century. It is enough to take a look at the influence of information on the electorate of such countries as France, Germany, and the United States. And

Russia uses it very well: it creates an artificial world, and if the real world brings it up all the time, it's very soon that the real world begins to believe in the unreal one.

Therefore, information confrontation is the rivalry of social systems (nations, blocs of countries) in the information sphere over the impact on certain areas of social relations and the establishment of control over the sources of strategic resources, as a result of which one group of rivals gets the benefits they need for further development.

According to the intensity, scale and means used, the following stages of information confrontation are distinguished: information expansion, information aggression and information war [6,7].

Information expansion i.e. the activities to achieve national interests by the method of conflict-free penetration into the information sphere in order to:

- carry out gradual and planned change in the system of social relations on the model of the source of expansion invisible to the society;
- displace the provisions of national ideology and national value system and replace them with their own values and ideological attitudes;
- increase the degree of its influence and presence, establish the control over strategic resources, information and telecommunication structure and national mass media (mass media);
- increase the presence of their own media in the information sphere of the object (system), penetration, etc.

Information aggression can be defined as illegal actions of one of the parties in the information sphere, aimed at inflicting specific, tangible damage to the enemy in certain areas of its activities through limited and local use of force.

Information warfare is the highest degree of information confrontation aimed at resolving socio-political, ideological, as well as national, territorial and other conflicts between states, peoples, nations, classes and social groups through the large-scale implementation of means and methods of information violence. (information weapons) [4,5].

Information aggression in the information sphere is assumed to escalate into war if one of the parties to the conflict begins to use information weapons widely against its opponents. This criterion makes it possible to distinguish from all the variety of processes and phenomena occurring in the information society those that pose a danger to its normal (peaceful) development.

In addition, it should be noted that currently there are no international and national legal norms that allow in peacetime (in the absence of an official declaration of war by the aggressor) to legally qualify hostile actions of a foreign state in the information sphere, accompanied by damage to information or other security such, as actions of information aggression or information war of material, moral, other damage. This allows to actively use the most dangerous and aggressive arsenal of forces and means of information warfare as the main means of achieving a political goal in peacetime.

**Main part**

Information War is the use and management of information in order to gain a competitive advantage over the enemy.

Information warfare may include [8]:

- collection of tactical information;
- ensuring the security of own information resources;
- spreading propaganda or misinformation to demoralize the enemy's army and population;
- undermining the quality of enemy information and preventing the possibility of gathering information by the enemy

Information warfare is often waged in conjunction with cyber and psychological wars in order to broader coverage of targets, involving electronic warfare and network technologies [8,9].

There are first and second generation strategic information wars. First-generation strategic information warfare includes the basic methods of information warfare that are currently being implemented at the state and military levels and which are not intended to be abandoned in the foreseeable future. The forms of information warfare of the first generation include [1,8,9]:

- fire suppression (in wartime) of infrastructure elements of state and military administration;
- conducting electronic warfare;
- obtaining intelligence information by intercepting and decrypting information flows;
- unauthorized access to information resources, followed by their falsification or theft;
- mass presentation in the information channels of the enemy or global networks of information to influence decision-makers;
- obtaining information from the interception of open sources.

At the same time, the concept of second-generation strategic information warfare was introduced. The development and conduct of the second generation of strategic information warfare, its coordinated information operations in the long run may lead to the complete abandonment of the use of military force.

The second generation information war involves the following [1,8,9]:

- creating an atmosphere of spirituality and immorality, a negative attitude towards the cultural heritage of the enemy;
- manipulation of the public consciousness of social groups of the population in order to create political tension and chaos;
- destabilization of political relations between parties, associations and movements in order to provoke conflicts, incite distrust, suspicion, intensify political struggle. Provoking repression against organizations and even civil war;
- reduction of the level of information support of authorities and management, inspiration of erroneous management decisions;
- misinformation about the work of state bodies, undermining their authority, discrediting government agencies;
- undermining the international prestige of the state, its cooperation with other countries;
- damage to vital interests of the state in political, economic, defence and other spheres.

The purpose of information warfare is to weaken the moral and material forces of the adversary or competitor and to strengthen one's own. It provides for measures to promote human consciousness in the ideological and emotional spheres. It is obvious that the information war is an integral part of the ideological struggle. It does not lead directly to bloodshed, destruction, no casualties, no one is deprived of food, no roof over their heads. In addition, it does not create dangerous security in relation to them. Meanwhile, the destruction caused by information wars in social psychology, the psychology of the individual, in scale and significance are quite commensurate, and sometimes exceed the consequences of armed wars.

The main task of information wars is to manipulate the masses. That is, the purpose of such manipulation lies often in the following [9]:

- introduction of hostile, harmful ideas and views into the public and individual consciousness;
- disorientation and misinformation of the masses;
- weakening of certain beliefs and foundations;
- intimidation of his people in the image of the enemy;
- intimidate the enemy with his power.

Finally, the last but no less important task: to provide a market for their economy. In this case, information warfare is part of the competition.

A successful information campaign conducted at the operational level will support strategic goals, influencing the enemy's ability to make decisions quickly and effectively. In other words,

the purpose of information attacks at the operational level is to create such obstacles to the enemy's decision-making process that the enemy cannot act or wage war in a coordinated and effective manner. In information warfare, the goal is to harmonize actions at the operational level with actions at the strategic level, so that united, they force the enemy to make decisions that would lead to action that help the subject to achieve its own goals and prevent the enemy from achieving their own.

As for the goals of attacks in the information war, the more dependent the enemy is on information systems in decision-making, the more vulnerable he is to hostile manipulation of these systems. Software viruses only affect systems that have programs.

The more modern society is, the more it relies on information and its means of delivery. This also includes the Internet - but this is only the tip of the iceberg. Every developed country has telephone, banking and many other computer-controlled networks, so they have their own weaknesses.

Information warfare is no longer a vague branch of futurology, but a real scientific discipline that is being studied and developed. In the broadest sense, information warfare includes propaganda.

Thus, the general purpose of information warfare is to disrupt the exchange of information in the camp of the enemy (competitor). It is easy to understand that this type of weapon is usually not aimed at the loss of manpower. In this sense, the technology curve has finally led to a bloodless and at the same time extremely effective weapon. It destroys not the population, but the state mechanism.

The information and computer revolution has opened wide opportunities for influencing peoples and power, manipulating the consciousness and behavior of people, even in remote areas. Taking into account the process of globalization of telecommunication networks taking place in the world, it is possible to assume that information types of aggression will be given priority in the future. Serious attention of experts of various profiles to this question is required to avoid the most negative consequences of this guilt for all mankind [10,11].

In the context of the ongoing confrontation between Russia and Ukraine, the information war is rapidly gaining momentum. Since the media today is the main source of informing society and the accumulation of all political processes, it is possible to influence and even form a new public opinion due to the media that.

In a time of rapid scientific and technological process and globalization of society, the media have become an integral part of modern life, they are able to reform the perception of reality. Today, the Russian media are creating negative stereotypes about Ukraine. After analyzing the materials of the leading Russian media (RTR. ORT, NTV channels) for the period 2013-2017 [12], we can identify a number of stereotypes that have formed in the Russians about Ukraine:

1. Ukraine is a part of Russia and it cannot exist without it. Thus, Ukrainians are a regional group of Russians who have their own dialect and certain territorial features.

2. The Ukrainian language does not exist. Many Russians believe that the Ukrainian language is a dialect formed from Russian. Namely, the design of the independent Ukrainian language was inspired by the Poles or the Austro-Hungarian authorities.

3. Western Ukraine is the center of the "Banderites", and Lviv is their capital. For the Russians, the Banderas are especially cruel people to be feared because they are murderers. However, no one can give a more specific definition of them.

4. Maidan - a manifestation of aggression against Russia. Many Russian media outlets reported that Bandera members and representatives of the Right Sector were standing for money in Kyiv and on the Maidan. Their goal is to kill as many Russians as possible, and they are also preparing an uprising against the fraternal people.

5. Ethnic Russians are under threat in Ukraine. That is why they are asking Russia to stand up for them, intervene and show Ukraine who is the "master".

6. Crimea is Russia, according to Russian media and politicians. It should be borne in mind that Crimea became part of Russia only in the XVIII century. In the XIX century for this territory with Russia fought the troops of the Ottoman Empire, Britain, France and the Kingdom of Sardinia. Despite the fact that Russia lost this war, Crimea remained part of it. Crimea became a part of Ukraine in 1954 in an abandoned state. And only with Ukraine he was reborn.

7. Ukrainian culture does not exist, say Russians. Many Russians believe that there is nothing cultural in Ukraine other than embroideries, folk songs and a few writers. And Ukraine owes all other cultural heritage to the Soviet Union.

8. Ukraine is suffering from the crisis, so hundreds of thousands of Ukrainians are seeking asylum in Russia. Propagandists are actively spreading information about the high quality of life in Russia. An example of this is the broadcast of the May Day parades in annexed Crimea and captured Donetsk. The media reported that Crimea had fallen into safe hands and had been abandoned.

9. The Ukrainian army is killing civilians in eastern Ukraine. Thus, this stereotype casts a shadow on Ukraine not only in the eyes of Russians, but also in the East. Russian TV channels falsify the "picture" on the screen. To show what is good for them. This fact is one of the reasons for the continuing conflict, which kills Ukrainian troops and civilians in the East every day. After all, people are disoriented, they can't figure out who is a friend and who is an enemy. Thus, today we see numerous support from the Russian army by the people of eastern Ukraine. And many Russians, even those who have never been to Ukraine, have formed a hostile attitude towards their fraternal people. Most of them, and especially young people, are ready to fight the mythical "Bandera", encroaching on the territorial integrity of Ukraine.

In addition, rumours are circulating that mass attacks by the Ukrainian army on churches and synagogues are taking place in southern and eastern Ukraine.

Not only ordinary people are exposed to this propaganda, but also many who create and influence public opinion: journalists, pop and cinema stars, athletes, businessmen, officials and others.

Until recently, it was not entirely clear what Russian propaganda was. Now the picture is clear, it is a multifunctional tool with a very high level of expertise, which involves not only experts in Europe, the US and Russia, but also large groups of experts, providing an accurate analysis of current situations and respond very quickly. Moreover, this analysis is psychological, political and military [12].

In addition, the Western media and institutions are also influenced. In fact, journalists and European politicians are being bribed in the tens of millions of dollars. And this is without taking into account the projects converted into propaganda tools - television, radio, newspapers, Internet - publications, as well as (as stated in the resolution of the European Parliament) a large number of institutions operating in the United States, Europe, Israel and elsewhere. In addition, an individual agreement with lobbyists. In a general sense, a propaganda campaign is a very expensive project.

Very often comparisons are made between the propaganda campaigns of Nazi Germany and modern Russia. These are not comparable things. Now a qualitatively different toolkit is used and, accordingly, a different level of influence is achieved.

Over the last 70 years, science has made great strides in developing mechanisms for influencing mass consciousness (neurolinguistic programming technologies). All this is now used for propaganda purposes. One of the Russian experts involved in the propaganda process stated: "The level of our developments is such that if we could talk about them openly, we would probably qualify for the Nobel Prize." And we see the result of 100 million completely intoxicated Russian citizens and at least half of Russian-speaking US citizens, as well as people in Germany, Israel and other countries - all affected by this [13,14, 15].

Propaganda campaigns used to be viewed as an ideological tool for carrying out their concepts. First, the propaganda campaigns of modern Russia were considered in this way as promoting the idea of a "Russian world." The new quality is that it is not only the promotion of ideology, but it is a tool of warfare [12, 16].

Russian propaganda aims to strengthen its moral and material position by humiliating Ukrainians and Ukraine. Therefore, the situation is not in Ukraine's favor. After all, the Russians are covering the events in Ukraine in their favor in order to win over as many supporters of the so-called "DPR" and "LPR" as possible, and this is a way to divide the country and threaten our image in the eyes of the democratic world. Russians skillfully manipulate the Ukrainian media audience and disorient society. Today, Russian journalists cover information about Ukraine in a way that benefits the Kremlin. They ignore the principles and ethical principles of journalism, as they use methods of misinformation [14, 17].

Since today the attention of the whole world community is focused on the events unfolding in eastern Ukraine, it is now quite obvious that Ukraine is seen by the Russian command as a testing ground for improving tactical concepts, testing new equipment and ammunition and information and psychological influence. Politically, the importance of what is happening in Ukraine is difficult to underestimate: it was Russia's successful tactics of warfare, some of the Donetsk and Luhansk regions, were not only completely occupied, but also acted upon to build plans for the forced return to Russian policy. In scientific terms, many scholars continue to emphasize that the Ukrainian-Russian armed conflict is developing quite differently from its predecessors, and if we analyse it purely militarily, many actions of the Russian command are not just incomprehensible, but sometimes seem illogical. Primitive, such that do not take into account local specifics.

For outside observers watching the conflict on television, the aggressor and local separatists have suggested that the Russians were either embroiled in the conflict with no clear plans to suppress Ukraine's defence or faced unexpectedly strong resistance they were not ready for. As for the relatively weak initial readiness of the Russian army to conduct hostilities in Ukraine, from our point of view, this is, of course, not the case. If Russian troops had begun to conquer Ukraine without a well-thought-out plan, they would hardly have been able to gain a foothold in such a large area with such minimal losses and in such a short time. This allows us to conclude that none of the actions of the Russian command was accidental - just in front of outside observers played a well-directed spectacle, designed to keep the audience in constant tension, controlling its emotions in the interests of its own public policy. Such a scenario, in fact, is a kind of technology of information warfare or information-psychological influence on consciousness, in which they work with reality as they do with the plot of a journalistic report. In this case, the actual hostilities will become one of the scenes provided for in the script, and lose their key, independent role. Watching from TV screens the "strange" war in Ukraine, the world saw the emergence of a new generation of wars - information, in which the actual fighting plays a subordinate service role. The plan of the armed campaign is based on the rules and in accordance with the scenario of PR influence on its own citizens, on the citizens of political allies and opponents and on the international community as a whole.

Thus, we can rightly say that the modern armed conflict is developing in the genre of reporting to generate news that in its form-volume would correspond as closely as possible to the format of PR material needed to implement the technology of information and psychological influence. As a result, such a chain of production (combat units of the armed forces) and practical implementation (forces of psychological operations) news from the theater of operations becomes a high-tech pipeline for the production of tools for processing and forming civic opinion, ensuring voluntary subordination and control of the political activity of elites. are in power in different countries. The product of the modern operation of information warfare is the compilation of media news in the format of a journalistic report. Today, information wars of the new generation are

becoming an effective tool of foreign policy. Let the society not deceive that in reports from theater of military actions the spectator sees that victims of aggression - not themselves, and citizens in remote Donetsk and Luhansk areas which location on a demarcation line not all will specify from the first times. The purpose of the information-psychological operation is the voluntary subjugation of society, which is ensured by means of technologies of psychological influence on the consciousness of its citizens. The Russian PR company that accompanies the hostilities in Ukraine is a clear confirmation of that. The format and nature of the speech are intended mainly for the citizens of those countries that in one way or another have a negative attitude to the Kremlin's political course, and in the materials provided to the audience it is easy to identify typical manipulative methods of working with information. This suggests that in the information war being waged in Ukraine, not only Ukrainian citizens are in sight, but also residents of Russia and the world [9,14,15].

Introducing the term "information warfare", the Russian leadership has already studied the psychology of people so well and learned to manage it that they do not need to use brute force - the army and the police - to ensure its unconditional obedience. It is clear to everyone that from the beginning it was tested on its own citizens. Such methods of subordination can be applied to any social system. If the social system does not want to submit voluntarily, they are ready to force it to do so with the help of modern complex technologies of secret information and psychological influence, and for a rebellious social system the result of such confrontation will be tantamount to defeat in war. Experts are convinced that the Russians use information warfare not so much as a term denoting the current phase of development of conflicting socio-political relations, but as a vector of foreign policy formation, as a program for choosing a political course and the ultimate goal of the evolution of tools. political governance. Recognizing information confrontation as the most general category of social relations, we can say that information confrontation can include any form of social and political competition, in which to achieve competitive advantage, preference is given to means, methods and ways of information. -psychological impact. It is considered that the concept of information confrontation includes the whole spectrum of conflict situations in the information and psychological sphere - from interpersonal conflicts to open confrontation of social systems (states). Information warfare is, undoubtedly, also a type of information warfare. There are several main reasons why the threat of "information wars" should be taken very seriously to carefully study their patterns and conditions of development [3, 6,8,9,12]:

1) Modern wars are becoming more informational and psychological, reminiscent of a large-scale PR campaign, and military operations themselves are gradually relegated to the background and play a clearly defined and limited role assigned to them in the general scenario of a military company;

2) modern information warfare technologies are capable of inflicting no less damage on the enemy than means of armed attack, and information weapons built on the basis of psychological influence technologies have a much greater impressive, penetrating and selective ability than modern high-precision weapons systems;

3) in international politics, other, more traditional forms of political regulation, such as war in general and military operations in particular, are being pushed out of political practice or replaced in it;

4) there is a need to emphasize the high social danger of some modern organizational forms and technologies of information and psychological influence used for political purposes.

As for war or local armed conflict, they can be generated almost anywhere in the world and at the same time when it is provided by the scenario of a psychological operation. It is no coincidence that, on the example of the war in Georgia and Ukraine, we see that the modern war resembles a large-scale PR show. Thus, at the present stage of development of political technologies, information warfare does not always begin with military action, but military action

becomes a necessary factor in any combat psychological operation - as a means of initiating chain psychological reactions provided by the scenario of information warfare. In the world of these provisions, it seems that some "illogical" episodes of the war in eastern Ukraine are becoming clear. Information war gives birth to a local one: for the transition of an informational, psychological operation from a latent stage to an active one, an initiative drive is needed, and, consequently, a local armed conflict is needed. The fact that traditional war plays a limited, strictly assigned role in information warfare does not make it less dangerous, does not reduce its scale and does not displace it from the sphere of political relations - global military conflicts are gradually disappearing from the political orbit, the number of local armed conflicts and their frequency is growing. Today there is a gradual transfer of political struggle in the information-psychological sphere, which increases the risk of local armed conflicts, which in psychological operations play the role of the initiating mechanism. In addition, information warfare technologies seem attractive to many precisely because of their relative cheapness, accessibility, and effectiveness, which ultimately leads to the widespread use of armed violence itself: where information warfare begins, non-local armed conflict does not necessarily arise. Thus, the information war is a combat action planned in accordance with the PR scenario, the purpose of which is not to destroy the enemy's manpower and equipment, but to achieve a PR effect.

**Conclusions**

At all stages of the historical development of human civilization, information has been both the most important object and a means of confrontation between peoples, nations, states, military-political blocs and alliances. Some facts of information and psychological influence on the general public can be found throughout the history of society. It is clear that in different periods the intensity of application of certain methods and methods of influence, as well as the perfection of their organization, differed greatly.

At the present stage, science has such theoretical constructions, on the basis of which the technology of information confrontation is carried out, i.e. the relevant state and non-state structures involved in such activities, develop and test new information technologies, techniques, methods of implementation, information and psychological impact, technical means necessary for such activities. Such shifts could not but affect the growth of the efficiency of information technology, which can lead to radical changes in society, economic, political and other spheres of an individual country, or globally.

The uncontrolled spread of the information space, along with the significant benefits of their use, has led to fundamentally new problems. The main issue was the sharp intensification of international competition for ownership of information markets. At the same time, the countries like Libya, Chechnya, Georgia, Ukraine etc. began to actively employ the opportunities of the information space (Internet) in order to ensure information confrontations and conduct separate operations during local hostilities and armed conflicts, the so-called information confrontation. This state of affairs, as a consequence, in turn led to the strengthening of integration processes in the infosphere, gave rise to information confrontation, i.e. information warfare.

In modern world, interstate conflicts are fraught with excessive losses for each of the warring parties. Therefore, the technique used is only half-truth - half-cooperation, mutual competition in development, in the pursuit of moral leadership. Activities in information confrontation and information-psychological influence give opportunities for the use of this approach.

It is proved that information war is an element of information confrontation - a political conflict in which the political struggle is conducted in the form of information and psychological operations with the use of information weapons.

**References**

1. Panarin I.N. - Information warfare and geopolitics / Panarin I.N. - Moscow: World of Security, 2011. - 719p.
2. Rastorguev S.P. Philosophy of information war / Rastorguev S.P. - M.: MPSI, 2003. - 496c.
3. Pirtskhalava L.G. Information confrontation in modern conditions / Pirtskhalava L.G., Khoroshko V.A., Khokhlacheva Yu.E., Shelest M.E. - K: «Compint», 2019.-226c.
4. Litvinenko O.V. - Special information operations and propaganda companies / Litvinenko O.V. - K: Satsanga, 2000.-242p.
5. Grishchuk R.V. Cyber weapons: classification, basic principles of construction, methods and means of application and protection against it / Grishchuk R.V., Khoroshko V.O. // Modern special equipment, №4. 2016. - P. 30-37
6. World hybrid war: the Ukrainian front / For general. ed. V.P. Gorbulina - K: NISD, 2007.-496p.
7. Eremenko V.T. - Actual problems of information confrontation in sociotechnical systems / Eremenko V.T., Pershukov VM, Pikalov B.V., Tretyakov O.V. - Orel: Iz-vo Gosuni-versitet - UNPK, 2015. - 291p.
8. Tolubko V.B. Information struggle (conceptual, theoretical, psychological aspects) / To-lubko V.B. - K.: NAMU 2003. – 320 p.
9. Grigoriev V.I. - Technologies of modern information and psychological warfare / Grigoriev V.I. // Information security of man. society. States, № 2 (18), 2015.– P6-16
10. Kozyura V.D. Analysis of cyber security of the information society / Kozyura V.D., Khoroshko V.O., Shelest M.E. // Information security of man, society, state, № 1 (21), 2017. - P163-171
11. Artemov V., Khoroshko V., Ivanchenko I., Brailovskyi N. Geopolitics and Information Warfare // SPCSJ, vol. 4, # 1, 2020.-p.61-64
12. Khoroshko V.A. Information and analytical security / Khoroshko V.A., Shelest M.E. - K.: VPV "Zadruga", 2016. - 183 p.
13. Prokofiev M.I. - The concept of application of information influences and counteraction to information weapons / Prokofiev M.I., Khoroshko V.O., Khokhlacheva Y.E. // Legal, regulatory and logistical support of information security systems in Ukraine, Vol. 1 (31), 2016. - P.9-14
14. Khoroshko V.O. - Information war. Mass media as a tool of informational influence on society. Part 1. / Khoroshko V.O., Khokhlacheva Y.E. // Information Security, Volume 22, №3,2016. - P.283-289.
15. Zelinsky S.A. - Information and psychological impact on mass consciousness / Zelinsky S.A. - SPb.: Skifiya, 2008.-403 p.
16. Ostapenko G.A. Information operations and attacks of socio-technical systems / Ostapenko G.A. - M: Hotline - Telecom, 2007.-134 p.
17. Khoroshko V.O. Information war. Protection against destructive information and psychological influences. Part 2 / Khoroshko V.O., Khokhlachova Y.E. // Information Security Vol.25, №1, 2019-P.18-24.

**Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 27-38 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# BB84 PROTOCOL AS A PROTOCOL FOR QUANTUM KEY DISTRIBUTION (QKD).

**Giorgi Labadze Georgian Technical University**

**ABSTRACT:** The publication of the BB84 protocol by Bennett and Brassard in 1984 marks the beginning of quantum key distribution. Since then, many other protocols have been invented. Yet, BB84 keeps a privileged place in the list of existing protocols: it is the one of the most analyzed and most often implemented, including those used in commercial products. We offer the analysis of BB84 protocol. The physical implementation of the protocol is investigated. Finally, we analyze the eavesdropping strategies against BB84 and deduce the secret key rate.

**KEYWORDS:** *quantum kay, secret key*

## 1. შესავალი

BB84 პროტოკოლის პრაქტიკული რიალიზაცია ტექნიკური გამოწვევაა.
სიგნალის წამმოება მაგალითად ფოტონი-არ არის მარტივი ამოცანა. თუმცა ბოლო მიღწევები აჩვენებს, რომ BB84 შესაძლებელია რიალიზებული იქნას თანამედროვე ტექნოლოგიების ეპოქაში.
BB84 პროტოკლში ინფორმაციის საუკეთესო მატარებლებათ ითვლება ფოტონი და მისი ერთი მდგომარეობა. ამასთან უნდა აღინიშნოს წარმოებასთან დაკავშირებით არის სირთულეები და ალტერნატიულ გამოსავალი არის გამოვიყენეოთ სუსტი კონგერენტული მდგომარეობები დაბალი საშვალო რაოდენობის ფოტონებით. მიახლოებით ერთფოტონური მდგომარეობის, სუსტი კონგერენტული მდგომარეობა შეიძლება მოცავდეს ერთზე მეტ ფოტონს, ამ მდგომარეობის ალბათობა შესაძლებელია გაკონტროლებული იქნას. გარდა ამისა დაკარგული ფოტონის წყვილი შესაძლებელია გამოყენებული იქნას ინფორმაციის მატარებლის წარმოებისთვის [1-3].

ფოტონები შესაძლებელია გაგზავნილი იქნას ან ოფტკური არხის დახმარებით ან უკაბელო ქსელით, ეს დამოკიდებულია თუ რას მოითხოვს გარემო პირობები. უნდა აღინიშნოს რომ ოფტიკურ ბოჭკოვაბი კავშირი უნდა ინეს უპირატესად მიჩნეული ტელეკონუნიკაციური ქსელისთვის.

ქუბიტი კოდირება შესაძლებელია შესრულებული იქნას ფოტონის პოლარიზაციით ან მისი ფაზით. ფაზირებული კოდირება ძირითადათ უკეთესია ფოტონებისთვის.

1.შემთხვევითი ბიტების კოდირება, ქუბიტების დახმარებით

კლასიკური ინფორმაციის თეორიაში ყველა შეტყობინება რაღაც მომენტში შესაძლებელია გარდაიქმნას ნულებად და ერთებად. ამიტომ ინფორმაციის ერთეულს ეწოდება ბიტი ანუ $\{0,1\}$ ნაკრები. კვანტურ მატარებელს BB84 - ს ვერ აღვწერთ კლასიკური ტერმინებით, ამიტომ ჩვენ უნდა მოვახერხოთ ჩვენი ენის ადაპტაცია ამ ახალ პარამეტრთან. არსებობს შესაბამისობა ზოგიერთი ფიზიკური სისტემის კვანტურ მდგომარეობასა და მის მატარებელ ინფორმაციას შორის.

კვანტური მდგომარეობა ძირითადად იწერება დირაკის აღნიშვნებით, ვერტიკალურ ხაზსა და კუთხოვან ფრჩხილს შორის, როგროც $|\psi\rangle, |1\rangle$ ან $|x\rangle$; კვანტური იმფორმაციის ნაწილაკები, გამოისახებიან იგივე აღნიშვნებით.

კვანტურ თეორიაში ინფორმაციის უმცირეს ნაწილაკს წარმოადგენს ქუბიტი, ბიტის კვანტური ექვივალენტი. ფიზიკურ სისტემაში ქუბიტის შესაბამისობა არის ელექტრონის ბრუნვა ან ფოტონის პოლარიზაცია . მათემატიკურად ქუბიტი აღიწერება ორი კომპლექსური რიცხვის ნაკრებით.

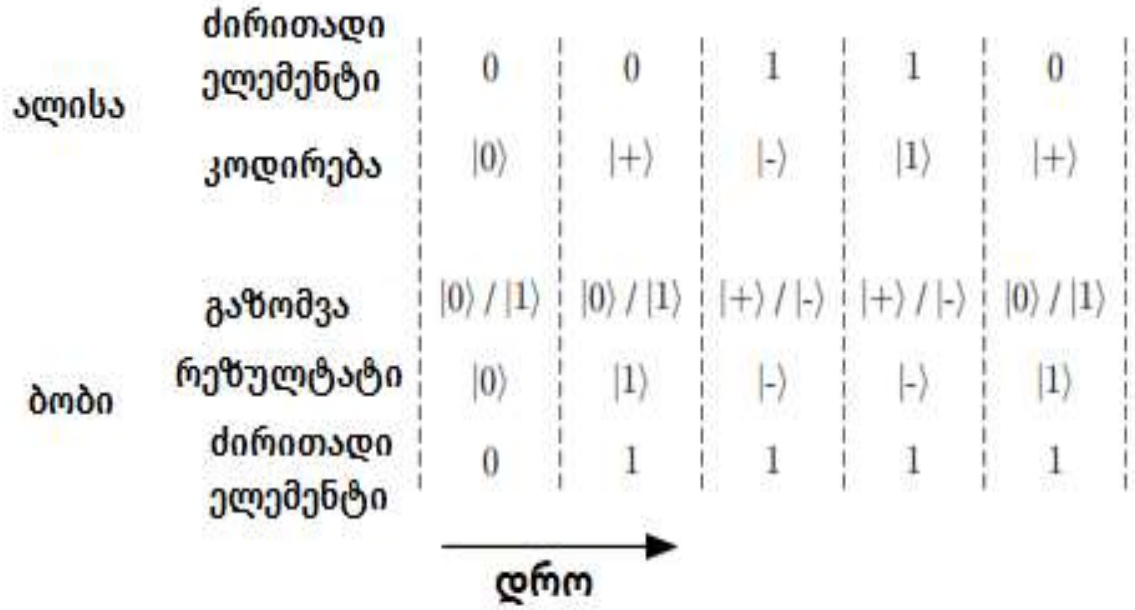
$$\{\alpha|0\rangle + \beta|1\rangle : \ |\alpha|^2 + |\beta|^2 = 1 \ \ \alpha, \beta \in C\}$$

ორი საბაზო ქუბიტი, რომელიც შესაბამება ორ ორთოგონალურ მდგომარეობას კვანტურ სისტემაში. ქუბიტებს $|0\rangle$ $(\alpha = 1, \beta = 0)$ და $|1\rangle$ $(\alpha = 0, \beta = 1)$ შეიძლება შევხედოთ როგორც ბიტის კვანტურ ექვივალენტს 0-ს და 1-ს შესაბამისად. $\alpha$ და $\beta$ სხვა მნიშვნელობით ჩვენ ვამბობთ, რომ ქუბიტი არის სუპერპოზიციაში $|0\rangle$ და $|1\rangle$. მაგალითად, ქუბიტები $2^{-1/2}|0\rangle + 2^{-1/2}|1\rangle$ და $\sin\pi/6\,|0\rangle + \cos\pi/|1\rangle$ ; $|0\rangle$ და $|1\rangle$ ორივე არის სუპერპოზიციაში, იმის მიუხედავად რომ განსხვავდებიან. BB84 ალისა იყენებს კოდირებას შემთხვევითი (კლასიკური) ბიტების, რომელსაც საკვანძო ელემენტები ეწოდება ოთხი განსხვავებული ქუბიტის გამოყენებით. ბიტი 0 შეიძლება იყოს კოდირებული $|0\rangle$ ან $|+\rangle = 2^{-1/2}|0\rangle + 2^{-1/2}|1\rangle$. ბიტი 0 შეიძლება კოდირებული იყოს $|1\rangle$ ან $|-\rangle = 2^{-1/2}|0\rangle + 2^{-1/2}|1\rangle$. გავითვალისწინოთ ნიშნების განსხვავება. ორივე შემთხვევაში ალისა ირჩევს კოდირების ნებისმერ წესს შემთხვევითობის პრინციპით,

ალბათობის მიხედვით. შემდეგ ის აგზავნის ფოტონს არჩეული ქუბიტით ბობთან. როდესაც ფოტონი მიდის ბობის გაჩერებაზე , მას სურს გაშიფროს ის რაც ალისამ გაუგზავნა. ამისთვის მან უნდა ჩაატაროს გაზომვები. თუმცა კვანტური მექანიკის კანონები არ აძლევს საშუალებას ბობს ბოლომდე გაშიფროს ქუბიტი. ხშირად შეუძლებელია ზუსტად გავიგოთ მიღებული ქუბიტის $\alpha|0\rangle + \beta|1\rangle$ $\alpha$ და $\beta$ კოეფიციენტი. ამის მაგივრად ბობმა უნდა აირჩიოს ორთოგონალური ქუბიტების წყვილი და გააკეთოს გაზომვები, რომელიც ანსხვავებს მხოლოდ მათ. ჩვენ ვაბობთ რომ ორი ქუბიტი $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ და $|\psi\rangle = \alpha'|0\rangle + \beta'|1\rangle$ არის ორთოგონალური თუ $\alpha\alpha' * + \beta\beta' * = 0$.

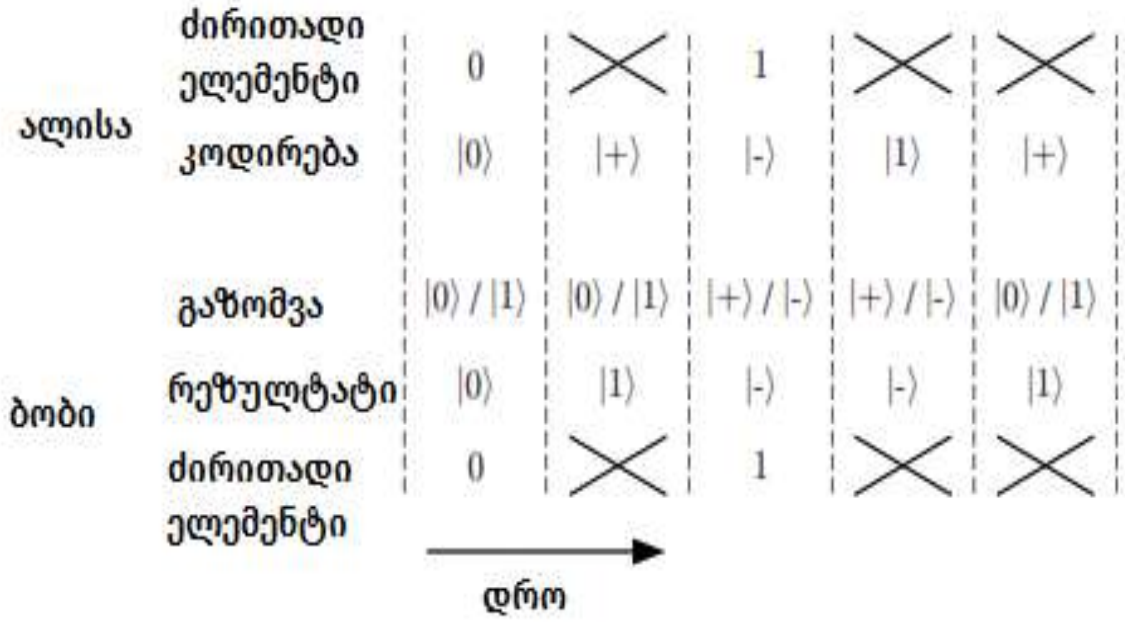
მაგალითად ავიღოთ ორთოგონალური ქუბიტები $|0\rangle$ და $|1\rangle$. ბობს შეუძლია ჩაატაროს გაზომვები რომელიც გაარკვევს ალისას გამოგზავნილი $|0\rangle$ ან $|1\rangle$. მაგრამ რა ხდება თუ ის აგზავნის $|+\rangle$ ან $|-\rangle$ ? ფაქტობრივად , ბობი იღებს რეზულტატს შემთხვევით! ზოგადად თუ ბობი მიიღებს $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ ის გაზომავს $|0\rangle$ ალბათობით $|\alpha|^2$ და $|1\rangle$ ალბათობით $|\beta|^2$, დავიმახსოვროთ $|\alpha|^2 + |\beta|^2 = 1$. პრაქტიკაში $|+\rangle$ და $|-\rangle$ ბობი იღებს $|0\rangle$ და $|1\rangle$ თითეულს ალბათობით ½. მაშასადამე, ბობს არ შეუძლია განასხვავოს $|+\rangle$ და $|-\rangle$ ამ შემთხვევაში ის იღებს არაკორერილებუ ბიტების მნიშვნელობას. რა არის განსაკუთრებული ქუბიტებში $|0\rangle$ და $|1\rangle$ შეძლება ევივალენტურად ჩაიწეროს $|0\rangle = 2^{-1/2}|+\rangle + 2^{-1/2}|-\rangle$ და
$|0\rangle = 2^{-1/2}|+\rangle - 2^{-1/2}|-\rangle$ შესაბამისად ამ შემთხვევაში, ბობს შეუძლია ალისას შეტყობინების დეკოდირება როცა ის აგზავნის $|+\rangle$ და $|-\rangle$, მაგრამ ის ვერ შეძლებს გაარჩიოს $|0\rangle$ და $|1\rangle$. ტრანსმიის დედექციის მაგალითი მოცემულია ნახაზი 1.2-ზე.

BB84 პროტოკოლში ,ბობი შემთხვევით ირჩევს გაზომვებს , დაახლობით ნახევარ შემთხვევაში ის არჩევს $|0\rangle$ და $|1\rangle$, სხვა შემთხევაში ის განასხვავებს $|+\rangle$ და $|-\rangle$. ამ ეტაპზე ალისა არ ამჟღავნებს კოდირების რომელი წესი გამოიყენა. შესაბამისად ბობი სწორად ზომავს მხოლოდ ბიტების ნახევარს, რომელიც ალისამ გაუგზავნა მას და არ იცის რომელი მათგანია სწორი. ძირითადი ელემენტების გრძელი ნაკადის გაგზავნის შემოდგომ , ალისა ატყობინებს ბობს კოდირების წესს.




ნახაზი 1.2 ტრანსმისიის მაგალითი BB84 გამოყენებით. პირველი ორი სტრიქონი არის რას აგზავნის ალისა. მესამე სტრიქონი გვაჩვენებს ბობის მიერ არჩეულ გაზომვის მეთოდს და გაზომვის შედეგად მიღებულ შესაძლო რეულტატს [4-6].

ალისამ აირჩია ყველა ძირითადი ელემენტი , ახლა ბობს შეუძლია გადაყაროს ყველა არასწორი გაზომვა; პროტოკოლის ამ ნაწილს ეწოდება გაცრა (ე.წ. შიფტინგი) რომელიც ნაჩვენებია ნახაზი 1.3-ზე




ნახაზი 1.3 ნახაზი 1.2 ტრანსმისიის შიფტინგი, ძირითადი ელემენტები რომლისთვისაც ბობის გაზომვები არ ემთხვევა ალისას კოდირების წესი იყრება.

ჯერჯერობით რომ შევაჯამოთ, ალისა უგზავნის ბობს შემთხვევით ბიტებს. ალისა ირჩევს ოთხი განსხვაბევული ქუბიტისგან ბიტების კოდირებისთვის (ორი სავარაუდო ქუბიტი ბიტზე). ბობი ირჩევს ორი გაზომვის მეთოდიდან ერთ-ერთს დეკოდირებისთვის. ბობს ყოველთვის არ შეუძლია დეტერმინირება რა გაუგზავნა ალისამ, მაგრამ გაცრის( შიფტინგის) შემდგომ ალისა და ბობი ინახავენ ბიტების უმრავლესობას რომელთათვისაც ტრანსიმისია წარმატებით განხორციელდა. ტრანსმისის ეს სქემა ალისას და ბობს აძლევს საშალებას შეამჩნიონ მოსმენა.

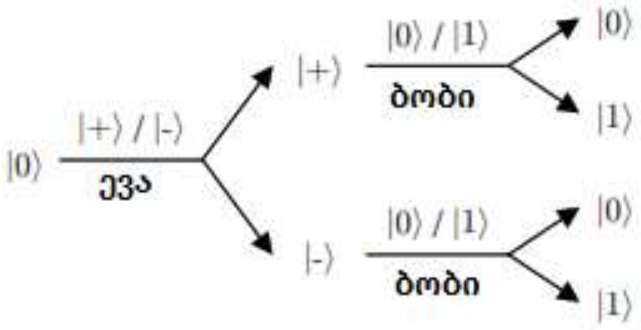
2.მოსმენის ამოცნობა

მოსმენის ამოცნობის ძირითადი თავისებურება გახლავთ ის ფაქტი, რომ ინფორმაცია კოდირებულია არაორთოგონალურ ქუბიტებში. ევას რა თქმა უნდა შეუძლია დაიჭიროს კვანტური მატარებელი და სცადოს მისი გაზომვა. მაგრამ ისევე როგორც ბობმა მან არი იცის წინასწარ, მატარებლის რომელი წყვილი აირჩია ალისამ, ყველა ძირითადი ელემენტისთვის. როგორც ბობს, ასევე ევას შეუძლია წარმატებულად გაარჩიოს $|0\rangle$ და $|1\rangle$ შორის , როცა ალისა იყენებს $|+\rangle$ და $|-\rangle$, ან პირიქით.

კვანტურ მექანიკაში გაზომვები დესტრუქციულია. ნაწილაკის გაზომვის შემდეგ, რეზულტატს ვიღებთ როგორც მდგომარეობას. უფრო ზუსტად, დავუშვათ, რომ დამკვირვებელი ზომავს ქუბიტს $|\phi\rangle$ რათა განასხვავოს $|0\rangle$ და $|1\rangle$. გაზომვის შემდეგ ქუბიტი გახდება $|\phi\rangle \rightarrow |\phi'\rangle = |0\rangle$ ან $|\phi\rangle \rightarrow |\phi'\rangle = |1\rangle$, დამოკიდებულია გაზომვის რეზულტატზე, მნიშვნელობა არ აქვს რა იყო $|\phi\rangle$, გარდა იმ შემთხვევისა როცა ქუბიტი არის რომელიმე მათგანი, რომელიც დამკვირვებელს სურს რომ გაარჩიოს (მაგალითად: $|0\rangle$ ან $|1\rangle$).

ყველა შემთხვევაში, როცა ევა იჭერს ფოტონს ზომავს მას და უგზავნის ბობს , მას აქვს ალბათობა ¼ შეცდომის ალბათობა ალისას და ბობის ბიტებს შორის.

მოდით დავანგრიოთ ეს შესაძლებლობა. ევას აქვს ალბათობა ½ გაზომოს სწორი წყვილი. როდესაც ევა ამას აკეთებს ის არ ეხება მდგომარეობას და რჩება შეუმჩნეველი. მაგრამ მას ყოველთვის არ უმართლებს. თუმცა, როდესაც ის ზომავს არასწორ ნაკრებს , ის უგზავნის ბობს არასწორ მდგომარეობას (მაგალითად: $|+\rangle$ ან $|-\rangle$, $|0\rangle$ ან $|1\rangle$ მაგივრად). ეს სიტუაცია აღწერილია ნახაზი 1.4 -ზე. არასწორ მდგომარეობაში ბობი ძირითადად ზომავს შემთხვევით ბიტს, რომელსაც აქვს ალბათობა ½ დამთხვევის ალისას ბიტთთან და ალბათობა ½ შეცდომის.




ნახაზი 1.4 შესაძლო შედეგები როცა ევა იყენებს არასწორ გაზომვებს მოსმენისათვის

აქედან გამომდინარე როდესაც ევა ცდილობს მოუსმინოს , ის დაახლოებით ½ შემთხვევაში იღებს არარელევანტურ შედეგს. მან შეიძლება გადაწყვიტოს არ მიწეროს ბობს მდგომარეობები, რომელთათვისაც მან მიიღო არარელევანტური შედეგი. მაგრამ მისთვის შეუძლებელია გააკეთოს მსგავსი განსხვავება, რადგან მან არ იცის კოდირების რა მეთოდია გამოყენებული.

ძირითად ელემენტებზე უარის თქმა ევასთვის უაზრობაა, რადგან ამ ნიმუშს არ გამოყენებენ ალისა და ბობი გასაღების დასამზადებლად. თუმცა, თუ ის მაინც მოახდენს მდგომარეობების რეტრანსლირებას (მიუხედავად იმისა, რომ ის არასწორია ½ შემთხვევაში), ალისა და ბობი

აღმოაჩენენ მის არსებობას, უჩვეულოდ დიდი რაოდენობის შეცდომების გამო მათ ძირითად ელემენტებში.

ბობს და ევას აქვთ ერთი და იგივე სირთულე, ალისას გამოგზავნილ ინფორმაციასთან მიმართებაში, რადგან მათ არ იციან კოდირების რომელი წესია გამოყენებული. მაგრამ სიტუაცია არ არის სიმეტრიული ბობისთვის და ევასთვის: ყველა კომუნიკაცია, აუცილებელია შიფტინგის შესასრულებლად , კლასიკურ აუთენთიფიცირებულ არხში. ეს საშუალებას აძლევს ალისას გაარკვიოს, რომ ესაუბრება ბობს და არა ევას. შესაბამისად, კანონიერი მხარეები იძლევა იმის გარანტიას რომ შიფტინგის პროცესზე ევა ვერ იქონიებს გავლენას. ამრიგად ალისას და ბობს შეუძლიათ მხოლოდ ის ძირითადი ელემენტები შეადარონ რომელიც სწორად გაიზომა. მსმენელის არსებობის დასადგენად , ალისას და ბობს უნდა ქონდეთ საშუალება ტრანსმისიის შეცდომების აღმოჩენის. ამისთვის არის საშუალება გავხსნათ ნაწილი გაცრილი გასაღების. მოცემულ პროტოკოლს შეუძლია ტრანსმისიის შემდეგ აჩვენოს $l + n$ ძირითადი ელემენტი( მაგალითად., l+n =100 000) ინდექსირებული 0 დან l+n -1, ალისა შემთხვევით ირჩევს n ინდექსს (მაგალითად n= 1000) შემდეგ ახდენს კომუნიკაციას ბობთან. შემდეგ ალისა და ბობი ხსნიან შესაბამის n ძირითად ელემენტებს, რათა დაითვალონ შეცდომების რაოდენობა, ნებისმიერ შეცდომა ნიშნავს რომ იყო გარკვეული მოსმენა. შეცდომების არ არსებობა გვაძლევას გარკვეულ სტატისტიკურ ნდობას იმაზე, რომ არ ყოფილა მოსმენა. მაგრამ შესაძლებელია ევას გაუმართლა, ან გამოიცნო კოდირების წესი ან დაუშვა შეცდომები სხვა ძირითად ელემენტებზე. რა თქმა უნდა მაშინ დარჩენილი ძირითადი ელემენტები იქნება გამოყენებული საიდუმლო გასაღების შესაქმნელად.

3.საიდუმლო გასაღების შექმნა.

იმ შემთხვევაში, თუ შეცდომები გამოვლინდა, ალისას და ბობს შეუძლიათ გაწყვიტონ პროტოკოლი, რადგან შეცდომები შეძლება გამოწვეული იქნას მოსმენისგან. უკიდურეს შემთხვევაში ეს ხელს უშლის გასაღების შექმნას, რომელიც შეიძლება ცნობილი გახდეს მოწინააღმდეგისთვის. გადაწყვეტილების ეს მხარე შეიძლება იყოს ცოტათი მკაცრი. პრაქტიკაში ფიზიკური რეალიზაცია არ არის იდეალური, რადგან შეცდომები შეიძლება

გამოწვეული იქნას ბევრი მიზეზით, გარდა მოსმენისა, ისეთი როგორიცაა მაგალითად ხმაური ან კვანტურ არხში დაკარგვა, არასრული გენერაცია კვანტური მდგომარეობის ან არასრული დედექცია. ასევე, ევამ შეიძლება მოისმინა პატარა ნაწილი დაშიფრული გასაღების, შექნას გასაღების დარჩენილი ელემენტები, საიდუმლო გასაღების შესაქმნელად. შესაბამისად უნდა გამოინახოს გზა შეიქმნას კვანტური გასაღების პროტოკოლი უფრო მდგრადი ხმაურთან მიმართებაში.

ალისა და ბობი ითვლიან შეცდომების რაოდენობას გამოვლენილ ძირითად ელემენტებში და ყოფენ ამ რიცხვს n-ზე, რომ მიიღონ მოსალოდნელ წილადის e შეფასების მისაღებად, ძირითადი ელემენტების მთელი ნაკრების შეცდომებს, შეფასებას e, ეწოდება ბიტების შეცდომის ნორმა. ამის შემდგომ, მათ შეუძლიათ დაასკვნან რამხელა ინფორმაციას ფლობს ევა ძირითად ელემენტებზე. მაგალითად მათ შეუძლიათ სტატისიკურად შეაფასონ, რომ ევამ იცის არაუმეტეს $I_E$ ბიტისა l ძირითად ელემენტებში. ეს არის პროტოკოლის შეფასების ნაწილი. ფორმულა რომელიც გვაძლევს $I_E$ რაოდენობას აქ არ არის განმარტებული; ეს შედეგია იმ ანალიზისა, თუ რა შეუძლია გააკეთოს მოსმენამ , კვანტური მექანიკის კანონების გათვალისწინებით. აგრეთვე $I_E$ ზუსტად არ ეუბნება ალისას და ბობს , თუ რა იცის ევამ ძირითადი ელემენტების შესახებ. ევამ შეიძლება იცოდეს ზუსტი მნიშვნელობა $I_E$ ელემენტების ან მხოლოდ რეზულტატი რამოდენიმე წარმოებული ფუნქციის l . რაც აძლევს $I_E$ ინფორმაციას შენონის გაგებით.

ამ ეტაპზე ალისამ და ბობმა იციან, რომ გახსნილ ძირითად ელემენტებს აქვთ e შეცდომების ნორმა და პოტენციური მსმენელს აქვს $I_E$ ინფორმაცია მათზე. კლასიკური საერთო აუთენთიფიცირებული არხით , ალისას და ბობს შეუძლათ კიდევ სცადონ შექმნან სრულად საიდუმლო გასაღები; ამ ნაწილს ეწოდება საიდუმლო გასაღების დისტილაცია.

საიდუმლო გასაღების დისტილაცია, მოიცავს ეტაპს რომელსაც ეწოდება შეთანხმება, რომლის მიზანია გადაცემის შეცდომების შესწორება. ნაბიჯს რომელსაც ეწოდება კონფიდენციალურობის გაძლიერება, რომელიც შლის ევას ინფორმაციას გასაღების სიგრძის შემოკლების ხარჯზე. მოკლეთ აღვწერთ ამ ორ პროცესს.

BB84 შემთხვევაში, შეთანხმება ჩვეულებრივ იღებს ინტერაქტიულ სახეს, შეცდომების შეასწორებს პროტოკოლი. ალისა და ბობბი ალტერნატიულად ამჟღავნებენ მათი ძირითადი ელემენტების ტოლ ქვესიმრავლეებს. როდესაც ისინი აღმოაჩენენ თანაფარდობის სხვაობას, ეს ნიშნავს, რომ შესაბამისი ქვესიმრავლეები შეიცავს გაურკეველი რაოდენობის შეცდომებს. უკიდურეს შემთხვევაში ერთს მაინც. დიხოტომიის გამოყენებით მათ შეუძლიათ შეცდომის ადგილმდებარეობის დაფიქსირება და მისი შესწორება. ისინი იმეორებენ ამ პროცეს საკმარისი რაოდენობით და შედეგად ალისა და ბობი ცვლიან ტოლ ბიტებს.

საიდუმლო გასაღების დისტილაციისას , ყველა კომუნიკაცია ხდება საერთო აუთენთიფიცირებული კლასიკური არხით. დავიმახსოროთ, რომ ევას არ შეუძლია ინტერვენცია ამ პროცესში, მაგრამ მას შეუძლია მოუსმინოს გაცვილილ შეტყობინებებს. რომელიც ამ შემთხვევაში შეიცავს გაცვლილ თანაბარ ბიტებს. მაშასადამე, ევას ცოდნა მოიცავს $I_E + |M|$ ბიტს, $|M|$ მნიშვნელობის თანაბარი ბიტებით, რომელიც შესწორებისას იქნა აღმოჩენილი. იმისთვის, რომ გასაღები იყოს საიდუმლო, კონფიდენციალურობის გაძლიერების იდეა მდგომარეობს იმაში, რომ გამოვიყენოთ ის რაც არ იცის ევამ. ალისას და ბობს შეუძლიათ დაითვალონ გასაღების ელემენტების ფუნქცია f-ი, ისე რომ გაავრცელონ ნაწილობრივი ევას უცოდინარობა მთელ რეზულტატზე. ასეთი ფუნქცია ( მაგალითად, როგორც ჰეშ ფუნქცია კლასიკურ კრიფტოგრაფიაში) ირჩევა ისე რომ თითეული გამომავალი ბიტი დამოკიდებულია შემავალი ბიტების უმეტეს ნაწილზე თუ არა ყველაზე. მაგალითად, ასეთი ფუნქცია შედგება თანაბარი შემთხევითი ქვესიმრავლეების ბიტების გამოთვლით. დავუშვათ, რომ ევამ იცის ბიტი $x_1$ მაგრამ არაფერი იცის $x_2$ ბიტის მნიშვნელობის შესახებ. თუ f ფუნქცია $x_1 + x_2 \, mod \, 2,$ ევას არ შეუძლია გახსნას გამომალი მნიშვნელობა , მანამ სანამ ორი შესაძლებლობა

$x_1 + x_2 = 0(mod)\, 2$ და $x_1 + x_2 = 1(mod)\, 2$ არის ტოლი მიუხედავად იმისა თუ რა მნიშვნელობა ექნება $x_1$. ფასი რომლის გადახდაც გვიწევს კონფიდენციალურობის გასამყარებლად არის ის , რომ გამომავალი საიდუმლო გასაღების სიგრძე უნდა იყოს ნაკლები, ვიდრე შემავალი ნაწილობრივ საიდუმლო გასაღების სიგრძე. შემოკლების ზომა დაახლოებით ტოლია ბიტების იმ რაოდენობისა რაც იცის ევამ და გასაღების ზომის რეზულტატი $l - I_E -$

$|M|$ ბიტებში. გასაღების მაქსიმალური ზომის მღება შესლებელია როცა ევამ არი იცის არაფერი გასაღების შემადგენელ ბიტებზე და (მაგალითად $l - I_E - |M| = 0$). მნიშვნელოვანია რომ გამოხშირვა , შესაძლებობის ფარგლებში ხსნიდეს მაქსიმალურად ნაკლებ ინფორმაციას, საკმარისს იმისთვის, რომ ალისამ და ბობმა შეძლონ შეასწორონ ყველა შეცდომა. მივაქციოთ ყურადღება იმას, რომ საიდუმლო გასაღების ნაწარმოები ბიტების რაოდენობიდან უხეშად რომ ვთქვათ, კვანტური გადაცემისას შეცდომების გასწორება გვიწევს ორჯერ. პირველ რიგში შეცდომები უნდა მივაკუთნოთ მოსმენას და $I_E$ ჩავთვალოთ. ასევე , შეცდომები უნდა იქნას სწრაფად გამოსწორებული, რისთვისაც ბიტების ნაწილი უნდა იქნას გახსინილი და ჩაითვალოს $|M|$.

საბოლოოდ, საიდუმლო გასაღები, მიღებული კომფედენციალურობის გაძლიერების შემდგომ, ალისას და ბობს შეუძლიათ გამოიყენონ კრიფტოგრაფიული მიზნებისთვის. კერძოდ, მათ შეუძლიათ გასაღების გამოყენება შეტყობინების დასაშიფრად ან საიდუმლო არხის შესაქმნელად.

## ბიბლიოგრაფია


1. Li, HW., Yin, ZQ., Wang, S. *et al.* Randomness determines practical security of BB84 quantum key distribution. *Sci Rep* 5, 16200 (2015). https://doi.org/10.1038/srep16200
2. Zhizhong Yan, Evan Meyer-Scott, Jean-Philippe Bourgoin, Brendon L. Higgins, Nikolay Gigov, Allison MacDonald, Hannes Hübel, and Thomas Jennewein, "Novel High-Speed Polarization Source for Decoy-State BB84 Quantum Key Distribution Over Free Space and Satellite Links," J. Lightwave Technol. 31, 1399-1408 (2013)
3. Chen, F.-L.; Wang, Z.-H.; Hu, Y.-M. A New Quantum Blind Signature Scheme with BB84-State. Entropy 2019, 21, 336. https://doi.org/10.3390/e21040336
4. S. Gnatyuk, T. Okhrimenko, M. Iavich and R. Berdibayev, "Intruder Control Mode Simulation of Deterministic Quantum Cryptography Protocol for Depolarized Quantum Channel," *2019 IEEE*

*International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, 2019, pp. 825-828, doi: 10.1109/PICST47496.2019.9061293.

**5.** Hu, S. Gnatyuk, T. Okhrimenko, 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.

**6.** J. Huang, Y. Wang, H. Wang, Z. Li and J. Huang, "Man-in-the-middle attack on BB84 protocol and its defence," *2009 2nd IEEE International Conference on Computer Science and Information Technology*, 2009, pp. 438-439, doi: 10.1109/ICCSIT.2009.5234678.

**Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 39-44 ISSN 2587-4667**
**Scientific Cyber Security Association (SCSA)**

# განათლების მნიშვნელობა კიბერუსაფრთხოების განვითარებაში

# THE IMPORTANCE OF EDUCATION IN THE DEVELOPMENT OF CYBER SECURITY

**ვლადიმერ სვანაძე საქართველოს ტექნიკური უნივერსიტეტის დოქტორანტი, საქართველოს ტექნოლოგიური ინოვაციების აკადემიის დირექტორი**

**Vladimer Svanadze, Georgian Technical University PhD Candidate. Director of Georgian Academy of Technological Innovations**

**რეზიუმე**: ქვეყნის კრიტიკულ ინფრასტრუქტურაზე განხორციელებული წარმატებული კიბერშეტევების აღკვეთა დამოკიდებულია არსებულ კვალიფიციურ კადრებზე, და შესაბამისად განათლების სისტემაზე, რომელსაც შეუძლია შექმნას მსგავსი კვალიფიციური ადამიანური რესურსი. აქვე შეიძლება აღინიშნოს, რომ შესაძლებელია მოხდეს უცხოელი სპეციალისტების მოზიდვა, ან ბევრი კიბერთავდაცვითი ღონისძიებები გადაეცეს კერძო სექტორს, ანუ გატანილ იქნეს ე. წ. „აუთსორსინგად“. თუმცა ორივე ეს ფაქტორი წარმოშობს სხვა პრობლემებს, რაც უკავშირდება როგორც დიდ ფინანსურ საშუალებებს, ისე ნდობის საკითხს დაკავშირებულს კრიტიკული ინფრასტრუქტურის სუბიექტების კიბერთავდაცვით უზრუნველყოფაზე უცხო კომპანიებისთვის გადაცემასთან, რაც ეროვნული უსაფრთხოების თვალსაზრისით ყოვლად დაუშვებელია. ბევრი ექსპერტი ამახვილებს ყურადღებას მოცემულ ფაქტორზე და იძლევიან სტრატეგიულ რეკომენდაციებს კიბერუსაფრთხოების სფეროში ეროვნული საკადრო რესურსის აღზრდისა და განვითარების შესახებ, რაც ნებისმიერი ქვეყნისთვის ასე აუცილებელი და მნიშვნელოვანი ფაქტორია. ნაშრომში ჩატარებული კვლევა აჩვენებს რომ კიბერუსაფრთხოების განვითარებისა და მდგრადობის შენარჩუნებისთვის მის ყველა ცალკეულ მიმართულებაზე, აუცილებელი არის შესაბამისი განათლებული და კვალიფიციური კადრების არსებობა, რაც თავის მხრივ უზრუნველყოფს კრიტიკული ინფრასტრუქტურის დაცულობის გაზრდას როგორც გლობალურ, ისე ეროვნულ დონეზე.

**საკვანძო სიტყვები:** *კიბერშეტევა, კიბერთავდაცვა, კიბერუსაფრთოება, განვითარება*

**ABSTRACT:** The prevention of successful cyber-attacks on the critical infrastructure of the country depends on the available qualified personnel, and consequently on the education system, which can create a similarly qualified human resource. It can also be mentioned that it is possible to attract foreign specialists, or to transfer many cyber security measures to the private sector. However, both of these factors give rise to other problems related to both large financial resources and the issue of trust in the transfer of critical infrastructure entities cyber security to foreign companies, which is totally unacceptable from the point of view of national security. Many experts focus on this factor and make strategic recommendations on the development of national human resources in the field of cyber security, which is very necessary and important factor for any country.

The research conducted in the paper shows that in order to to develop and maintain cybersecurity in all its individual areas, it is necessary to have adequately educated and qualified personnel, which in turn provides increased critical infrastructure protection both globally and nationally.

KEYWORDS: *cyber-attacks, cyber security, cyber safety,development*

მსოფლიო ეკონომიკური ფორუმის 2021 წლის გლობალური რისკების ანგარიშის მიხედვით, კიბერსივრცეში არსებული რისკები კვლავ შედიან გლობალური რისკების რიცხვში. პანდემიამ COVID – 19 დააჩქარა ტექნოლოგიების დანერგვის პროცესი, თუმცა, გამოავლინა კიბერ სისუსტეები და არამზაობა. ამვდროულად, გაამწვავა ტექნიკური უთანასწორობა როგორც საზოგადოებებს შორის გარედან, ისე მათ შიგნითაც [1, 2].

იგივე ანგარიშის მიხედვით „მომავალ წელს ძალზედ მნიშვნელოვანია კიბერუსაფრთხოება განხილულ იქნეს, როგორც სტრატეგიული ბიზნეს - საკითხი და განვითარდეს მჭიდრო საპარტნიორო ურთიერთობები ინდუსტრიებს, ბიზნესის ლიდერებს, მარეგულირებელ ორგანოებსა და პოლიტიკოსებს შორის. ისევე, როგორც ნებისმიერი სხვა სტრატეგიული საზოგადოებრივი გამოწვევა, კიბერუსაფრთხოებაც ვერ მოგვარდება იზოლირებულად” [3].

ზოგადად ქვეყნის კრიტიკულ ინფრასტრუქტურაზე განხორციელებული წარმატებული კიბერშეტევების აღკვეთა დამოკიდებულია არსებულ კვალიფიციურ კადრებზე, და შესაბამისად განათლების სისტემაზე, რომელსაც შეუძლია შექმნას მსგავსი კვალიფიციური ადამიანური რესურსი. აქვე შეიძლება აღინიშნოს, რომ შესაძლებელია მოხდეს უცხოელი სპეციალისტების მოზიდვა, ან ბევრი კიბერთავდაცვითი ღონისძიებები გადაეცეს კერძო სექტორს, ანუ გატანილ იქნეს ე. წ. „აუთსორსინგად“. თუმცა ორივე ეს ფაქტორი წარმოშობს სხვა პრობლემებს, რაც უკავშირდება როგორც დიდ ფინანსურ საშუალებებს, ისე ნდობის საკითხს დაკავშირებულს კრიტიკული ინფრასტრუქტურის სუბიექტების კიბერთავდაცვით უზრუნველყოფაზე უცხო კომპანიებისთვის გადაცემასთან, რაც ეროვნული უსაფრთხოების თვალსაზრისით ყოვლად დაუშვებელია. ბევრი ექსპერტი ამახვილებს ყურადღებას მოცემულ ფაქტორზე და იძლევიან სტრატეგიულ რეკომენდაციებს კიბერუსაფრთხოების სფეროში ეროვნული საკადრო რესურსის აღზრდისა და განვითარების შესახებ, რაც ნებისმიერი ქვეყნისთვის ასე აუცილებელი და მნიშვნელოვანი ფაქტორია.

კიბერუსაფრთხოების სფეროში კვალიფიციური ადამიანური რესურსის ყოლა არის საკმაოდ დეფიციტური არა მარტო განვითარებადი, არამედ განვითარებული ქვეყნებისთვისაც. მოცემული პროფესიის ადამიანებზე მოთხოვნა გაიზარდა განსაკუთრებით მას შემდეგ, რაც ინტერნეტისა და ინტერნეტ ტექნოლოგიების სწრაფმა განვითარებამ და გლობალურად არსებულმა ვითარებამ, განსაკუთრებით კი პანდემიამ, დააჩქარა ციფრული ტრანსფორმაციის დანერგვაზე მოთხოვნილების გაზრდა. ციფრული ტრანსფორმაციის დანერგვის პროცესში იქნება ეს კერძო თუ საჯარო სექტორში, აუცილებელია მოხდეს ბალანსის შენარჩუნება ტექნოლოგიურ ინოვაციებსა და კიბერუსაფრთხოებას შორის, რაც

კომპლექსური პროცესია და მოითხოვს ორგანიზაციის ყველა სტრუქტურული ერთეულის ჩართულობას. ეს კი თავის მხრივ ხელს უწყობს ციფრული ტრანსფორმაციის ფარგლებში კიბერუსაფრთხოების სტრატეგიისა და პოლიტიკის სწორი მიმართულებით შემუშავებას, პროცესის სწორ დაგეგმვას. ყოველივე ეს მოითხოვს კიბერუსაფრთხოების მიმართულებით კვალიფიციურ და გამოცდილ ადამიანურ რესურსს, რაც თავის მხრივ პირდაპირ კავშირშია განათლების სისტემასთან.

კიბერუსაფრთხოების შესახებ განათლების ზრდის ხელშეწყობა და ცნობიერების გაზრდა ქვეყნებისთვის იმდენად პრიორიტეტულ და მნიშვნელოვან მიმართულებას წარმოადგენს, რომ ის შეყვანილი არის თითოეული ქვეყნის კიბერუსაფრთხოების ეროვნულ სტრატეგიებში [4]. ამ მხრივ არც საქართველოს „კიბერუსაფრთხოების 2017 – 2018 წლების ეროვნული სტრატეგია და სამოქმედო გეგმა“ [5] არის გამონაკლისი, სადაც მოცემული მიმართულება მოხსენიებულია როგორც ერთ - ერთი ძირითადი მიმართულება, კერძოდ:

1. კვლევა და ანალიზი;
2. სამართლებრივი ბაზის შემუშავება და სრულყოფა;
3. კიბერუსაფრთხოების სფეროში შესაძლებლობათა ამაღლება;
4. საზოგადოებრივი ცნობიერების ამაღლება და საგანმანათლებლო ბაზის შექმნა;
5. საერთაშორისო თანამშრომლობა.

უნდა ითქვას, რომ სტრატეგიებში განათლების სფეროს ასახვა ნათლად აჩვენებს ქვეყნების დიდ ინტერესს განავითარონ თავიანთი კიბერუსაფრთხოებითი შესაძლებლობა, რაც პირდაპირ კავშირშია პროფესიული და კვალიფიციური ადამიანური რესურსის არსებობასთან. აქვე ცალკე აღსანიშნავია ის გარემოებაც, რომ სტრატეგიებში მოცემული კიბერუსაფრთხოების ძირითადი მიმართულებები, იქნება ეს კვლევა და ანალიზი, საერთაშორისო თანამშრომლობა, სამართლებრივ ბაზებზე მუშაობა და მისი განვითარება, თუ თავად კიბერუსაფრთხოების სფეროს შესაძლებლობების განვითარება და საზოგადოებრივი ცნობიერების ამაღლება, პირდაპირ კავშირშია სწორად დაგეგმილი და ძლიერი საგანმანათლებლო ბაზის განვითარებასთან, რადგან სტრატეგიის ყველა ჩამოთვლილი მიმართულება მოითხოვს კვალიფიციურ კადრს.

როცა ვსაუბრობთ კვალიფიციურ კადრზე იგულისხმება აკადემიური განათლების მქონე პირები, რომლებსაც მიღებული აქვთ სულ ცოტა ბაკალავრის აკადემიური ხარისხი. გარდა ამისა, არსებობს საერთაშორისო დონეზე აღიარებული სერტიფიცირებული კურსები, თუმცა მათი უმრავლესობა კონკრეტული მიმართულებით ითხოვს საბაზისო ცოდნას, რაც შესაბამისობაშია ბაკალავრის დონესთან. ასევე დამსაქმებელთა დიდი ნაწილი ვაკანტური ადგილის დასაკავებელი კონკურსის მოთხოვნების განათლების სექციაში პირდაპირ უთითებენ მინიმუმ ბაკალავრის დონეს. შესაძლებელია კიდევ ბევრი მაგალითის მოყვანა, თუმცა ეს ორი ერთმანეთისგან განსხვავებული მაგალითი პირდაპირ მიუთითებს კიბერუსაფრთხოების სფეროში აკადემიური განათლების მნიშვნელობაზე. აქვე თუ დავამატებთ იმ ფაქტს, რომ გლობალურად კიბერუსაფრთხოების სპეციალისტთა აშკარა დეფიციტია, ხოლო მათზე მოთხოვნილება სულ უფრო იზრდება, მაშინ შეიძლება ითქვას, რომ ეს იქნება უახლესი მომავლის ერთ - ერთი მოთხოვნადი სპეციალობა. აგრეთვე, თუ

გავითვალისწინებთ ასეთ მზარდ მოთხოვნილებას, თავისუფლად შეიძლება ითქვას, რომ მოცემული მიმართულების სპეციალისტების შრომითი ანაზღაურება არის საკმაოდ მაღალი. კერძოდ, მაგალითისთვის, https://www.payscale.com/ - ის მიხედვით, უსაფრთხოების ოპერაციების ცენტრის (Security Operations Center SOC) დამწყები ანალიტიკოსის წლიური ხელფასი 81,351 აშშ დოლარს შეადგენს. იგივე წყაროს ინფორმციით, საკმაოდ მაღალანაზღაურებადი არის ისეთი სპეციალობები როგორებიც არის [6, 7]:

- Penetration Tester;
- Information Security Analyst;
- Security Analyst;
- Ethical Hacker.

ჩამოთვლილი სპეციალობების საშუალო წლიური ანაზღაურება დაახლოებით 83,968 აშშ დოლარს შეადგენს. ალბათ ყველაზე უფრო გასათვალისწინებელი ფაქტი არის ის, რომ მოცემული სპეციალობების ხალხის დასაქმება სირთულეს არ წარმოადგენს და საერთაშორისო და ადგილობრივ ბაზარზე ძნელად თუ მოიძებნება მოცემული სპეციალობების კარგი და კვალიფიციური კადრები. ამიტომ, შეიძლება ითქვას, რომ კიბერუსაფრთხოების მიმართულებით მაღალი დონის განათლების მიღებაში ფინანსური საშუალებების „დაბანდება“ საკმაოდ წარმატებულ ინვესტირებას უნდა წარმოადგენდეს.

განვითარებად ქვეყნებში კიბერუსაფრთხოების მიმართულებით განათლების განვითარების პროცესი არათანმიმდევრულად და რთულად მიმდინარეობს, ხოლო ხშირ შემთხვევაში ეს პროცესი საერთოდ არ არსებობს, ან თუ არსებობს საერთოდ არის მოწყვეტილი დარგის განვითარებისა და მისი მდგრადობის შენარჩუნებასთან. გამონაკლისს არ წარმოადგენს არც საქართველო. შეიძლება თამამად ითქვას, რომ საქართველოში კიბერუსაფრთხოების მიმართულებით აკადემიურ დონეზე განათლება საერთოდ არ არსებობს, არის მხოლოდ სხვადასხვა უნივერსიტეტებში არსებული ცალკეული მოდულები. ქვეყანაში არ არის საბაკალავრო და სამაგისტრო პროგრამები, როცა საქართველოს კიბერსივრცე, კრიტიკული ინფრასტრუქტურა დგას გლობალურად არსებული სულ უფრო ახალი გამოწვევების წინაშე.

საქართველოს კიბერსივრცეზე, დაწყებული 2008 წლის „აგვისტოს ომის“ დროიდან მოყოლებული დღემდე, განხორციელდა არა ერთი სერიოზული კიბერთავდასხმა, რომლის დროსაც დარღვეული იყო კიბერსივრცის მდგრადობა. თითქმის ყველა კიბერთავდასხმის თავიდან აღკვეთის, ან საგამოძიებო პროცესში ჩართული იყვნენ ქვეყნის სტრატეგიული პარტნიორები და მათი დახმარებით ხდებოდა ქვეყნის კრიტიკული ინფრასტრუქტურის ერთიანობის შენარჩუნება. ქვეყნის წინაშე მდგარი საფრთხეების, კვალიფიციური კადრების აშკარა ნაკლებობის ფონზე და ასევე მიუხედავად, ორივე სტრატეგიაში განათლების განვითარების მიმართულების მნიშვნელობის აღნიშვნისა, ქვეყანაში მაინც ვერ მოხერხდა კიბერუსაფრთხოების საგანმანათლებლო აკადემიური პროგრამების დანერგვა და განვითარება. ეს პროცესი დაკავშირებულია რიგ საკითხებთან. კერძოდ, ქვეყნის წამყვანი უნივერსიტეტები არის კერძო სექტორის წარმომადგენლები, რომლებისთვისაც ყოველი ახალი პროგრამის დანერგვა დაკავშირებულია გარკვეულ ფინანსურ დანახარჯებთან და,

რომლებიც ყველა ამ პროცესს უყურებს მოგების მიღების გადასახედიდან, ანუ ორიენტირებულნი არიან მოგებაზე და ბიზნესის განვითარებაზე, და ეს ბუნებრივიც არის. ეს კი იძლევა იმის ვარაუდს, რომ კერძო უმაღლეს სასწავლებლებს ამ ეტაპზე არ უღირთ კიბერუსაფრთხოების მიმართულებით საბაკალავრო და სამაგისტრო პროგრამების დანერგვა, თუ მათ არ დაინახეს იქიდან წამოსული მოგება. მეორე მხარეა, სახელმწიფო, რომლის ინტერესებშიც შედის იყოლიოს მაღალი კვალიფიკაციის კადრები, რათა დააკომპლექტოს ის საჯარო სამსახურები, რომლებიც პასუხისმგებელნი არიან ქვეყნის კრიტიკული ინფრასტრუქტურის დაცვაზე და ასევე დააკომპლექტოს კრიტიკული ინფრასტრუქტურის სუბიექტები, რასაც ავალდებულებს კანონი „ინფორმაციული უსაფრთხოების შესახებ“.

აღსანიშნავია ის გარემოებაც, რომ კანონში „ინფორმაციული უსაფრთხოების შესახებ“ შედის ცვლილებები, რომლის მიხედვითაც არსებული კრიტიკული ინფრასტრუქტურის სუბიექტების ნუსხას ემატება ასევე ორი კატეგორია კერძო სექტორიდან - სატელეკომუნიკაციო კომპანიები და საბანკო სექტორი, რომლებსაც ექნებათ ასევე ვალდებულება თავისთან იყოლიონ როგორც ინფორმაციული უსაფრთხოების მენეჯერები, ისე კიბერუსაფრთხოების სპეციალისტები [8, 9]. გარდა ამისა, ყოველივეს ემატება ის გარემოებაც, რომ მოცემულ კანონში შეტანილი ცვლილებებით გარკვეული ვალდებულების ქვეშ იქნებიან ასევე კერძო სექტორის სხვა ინდუსტრიული სეგმენტებიც. ფაქტიურად, შეიძლება ითქვას, რომ ქვეყანაში სულ უფრო იზრდება მოთხოვნილება კიბერუსაფრთხოების და მათ შორის ასევე, ინფორმაციული უსაფრთხოების მაღალი კვალიფიკაციის კადრების მიმართ. თუმცა სახელმწიფოს მხრიდან ამ მიმართულებით სამწუხაროდ არაფერი არ კეთდება, ვერ მოხერხდა ვერც ერთ სახელმწიფო უმაღლეს სასწავლებელში შესაბამისი პროგრამების ჩამოყალიბება და განვითარება. სტუდენტები და კურსდამთავრებულები თავად ცდილობენ აიმაღლონ კვალიფიკაცია სხვადასხვა სერტიფიცირებული კურსების გავლით როგორც საერთაშორისო, ისე ლოკალურ დონეზე. თუმცა აქაც გარკვეულ პრობლემებს აწყდებიან, რადგან საერთაშორისო სერტიფიცირებული კურსები, რომლებიც ფაქტიურად სპეციალობას იძლევა, არის საკმაოდ ძვირადღირებული, ხოლო ლოკალურ დონეზე არსებული კურსები არ იძლევა იმ დონის კვალიფიკაციას, რომ შესაძლებელი იყოს კარგად დასაქმება. სამწუხაროდ, არც სახელმწიფო არ სთავაზობს რაიმე სახის კვალიფიკაციის ასამაღლებელ კურსებს.

ფაქტიურად, მოცემული მიმართულებით დარღვეული არის კავშირი საჯარო სექტორსა და აკადემიურ წრეებს შორის, როცა ამ უკანასკნელისთვის შეიძლება თავად სახლემწიფო ყოფილიყო დამკვეთი მისთვის აუცილებელი კადრების მომზადებასა და გადამზადებაში. არ შეიძლება არ აღინიშნოს ასევე თანამშრომლობის აუცილებლობა სამეცნიერო კვლევების ჩატარების მიმართულებითაც, რაც დღეს ფაქტიურად საერთოდ მოშლილია და არ ტარდება აკადემიური დონის სამეცნიერო კვლევითი საქმიანობა.

მსგავსი თანამშრომლობა იქნებოდა ე. წ. „სტეიქჰოლდერიზმის“ კარგი მაგალითი, რაც ასე აპრობირებულია დასავლეთში. ეს  არის აუცილებელი როგორც დარგის აკადემიურ დონეზე განვითარებისთვის, ისე ზოგადად, ქვეყნის კრიტიკული ინფრასტრუქტურის დაცულობის მაქსიმალურად გაზრდისთვის.

დასკვნის სახით შეიძლება ითქვას, რომ კიბერუსაფრთხოების განვითარებისა და მდგრადობის შენარჩუნებისთვის მის ყველა ცალკეულ მიმართულებაზე, აუცილებელი არის შესაბამისი განათლებული და კვალიფიციური კადრების არსებობა, რაც თავის მხრივ უზრუნველყოფს კრიტიკული ინფრასტრუქტურის დაცულობის გაზრდას როგორც გლობალურ, ისე ეროვნულ დონეზე.

## გამოყენებული ლიტერატურა

1. The Global Risks Report 2021, 16th Edition of the World Economic Forum, In partnership with Marsh McLennan, SK Group and Zurich Insurance Group, 19 January, 2021;
2. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019
3. GUIDE TO GOOD GOVERNANCE IN CYBERSECURITY, DCAF Business and Security Division, Directorate for Security Cooperation and Defence (DCSD) of the French Ministry of Europe and Foreign Affairs, 19 January, 2021;
4. Cybersecurity education in a developing nation: the Ecuadorian environment, Frankie E. Catota1,2,*, M. Granger Morgan1 and Douglas C. Sicker, Journal of Cybersecurity, 2019, 1–19
5. საქართველოს კიბერუსაფრთხოების 2017 – 2018 წლების სტრატეგია და სამოქმედო გეგმა, საქართველოს მთავრობა, 13 იანვარი, 2017;
6. Cybercrime in Georgia: Current Challenges and Possible Developments, Nata Goderdzishvili, Shalva Khutsishvili, PMCG Research Center, 2021;
7. კანონი „ინფორმაციული უსაფრთხოების შესახებ“, საქართველოს საკანონმდებლო მაცნე, 2012;
8. კიბერ თავდაცვა. კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები (ნაშრომების და სტატიების კრებული), ვლადიმერ სვანაძე, ანდრია გოცირიძე, 2015.
9. Sergiy Gnatyuk , Maksim Iavich , Giorgi Iashvili , Andriy Fesenko ENSURING EUROPEAN CIVIL AVIATION CYBERSECURITY, Scientific and practical cyber security journal, 2019

**Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 45-50 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# LINKS BETWEEN 5G PPP PROJECTS: THE ROAD FROM THE PAST TO THE FUTURE

**Roman Odarchenko National aviation university, Kyiv, Ukraine**
**Giorgi Labadze Georgian technical university**

**ABSTRACT:** Creating an information society in the world is one of the most urgent and important tasks today. In such conditions 5G networks will become the most widespread telecommunication technological solution in the next decade. To ensure the European leadership in the direction of the development and deployment of 5G networks 5G PPP in close collaboration with EC supports different related activities. There were already launched the 5G PPP project of three phases. It was shown that they are closely linked. This aims to present and analyze the links between 5G-Xcast, 5G-TOURS, and 5GASP projects, the continuity of the conducted research activities, and new directions of future research. There were showcased which technologies and solutions from the past projects were reused for other projects and probably will be reused for further studies. Was underlined that the most valuable is the long-term follow-up of research according to the 5G PPP research roadmap. This hopefully will help to support vendors, MNOs, SMEs, and verticals in the EU on the road to the future information society.

**KEYWORDS***: 5G, 5G PPP, networks, projects, standardization, Horizon 2020.*

## INTRODUCTION

Creating an information society in the world is one of the most urgent and important tasks today [1]. The priorities for the formation of modern information infrastructure in the EU include the creation of high-speed mobile broadband access to Internet resources throughout the territory. This is broadband access based on the use of mobile technologies of the fourth generation 4G (Fourth Generation) and 5G (Fifth Generation). To address the implementation of 5G technologies on the targeted efforts of the largest cellular operators (Orange, Vodafone, etc.). At the same time, the impact of these technologies on modern society cannot be overestimated. Cellular communication is currently considered the norm, and mobile technologies are the most popular and rapidly evolving.
Along with the growing number of disparate devices connected to the Internet and new popular services (transmission of high-definition video 4K, 8K, virtual reality (Virtual Reality - VR), augmented reality (Augmented Reality - AR), the concept of Connected Cars, etc.), which put forward new requirements for the targeted efficiency of cellular networks (reducing latency, increasing the required bandwidth, etc.), the world is experiencing an exponential increase in data transmission, which is not always able to effectively cope with existing 4G cellular networks [2]. It is obvious that in the near future the existing networks will be unable to provide the required quality of service to mobile subscribers, cars and IoT devices. That is why it is the time for rising of 5G networks.

## THE DEVELOPMENT OF CELLULAR NETWORKS

The 4G standard is capable of providing data rates of more than 100 Mbps to high-speed subscribers (eg trains and cars) and 1 Gbps to low mobility subscribers (eg pedestrians and fixed subscribers) according to the International Mobile Telecommunications Advanced International Specification (IMT). -Advanced) [3]. In general, 5G networks will be able to use the capabilities of all running cellular networks of previous generations simultaneously with the new radio interface New Radio (NR). So 5G should deliver significantly increased operational performance (e.g. increased spectral efficiency, higher data rates, low latency), as well as superior user experience (near to fixed network but offering full mobility and coverage) [4].

Comparison of key capabilities of IMT-Advanced (4th generation) with IMT-2020 (5th generation) according to ITU-R M.2083 is presented on the Figure 1 [5].

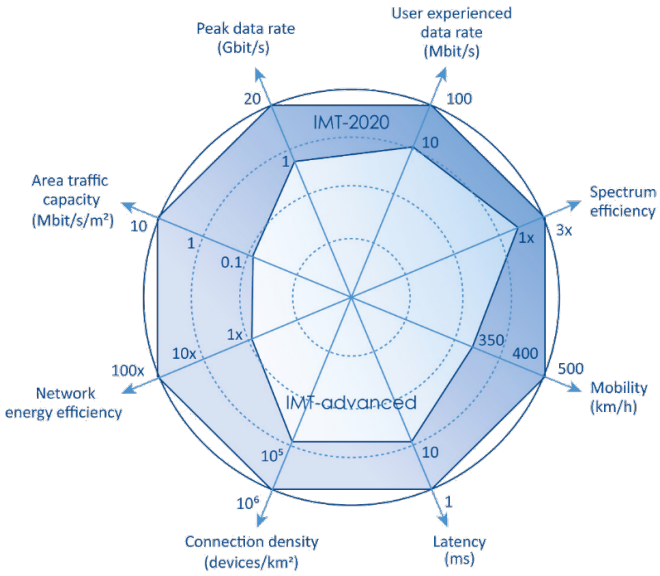
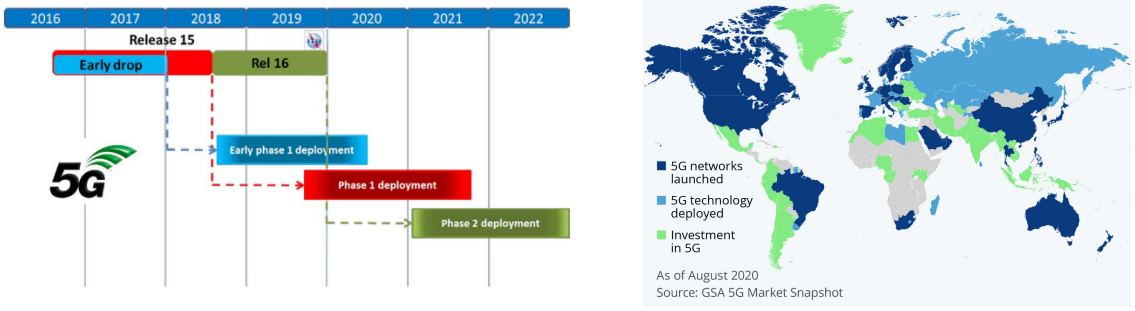



***Fig.1**. 5G networks requirements*

As already noted, the number of devices connected to the World Wide Web and the requirements of subscribers to the speed of mobile Internet access are increasing every year. Developers of telecom equipment and telecom operators, striving to respond to new challenges [6], are preparing to seriously transform the network architecture and interaction regulations. This is how the first ubiquitous fifth generation (5G) networks emerge. The first commercial network of the fifth generation was launched in 2018 - telecom operator Verizon announced the launch of "the world's first 5G network" in four US cities: Houston, Indianapolis, Los Angeles and Sacramento [7]. At the same time, the launch of the first nationwide 5G network, which provided continuous coverage in South Korea in April 2019, turned out to be less effective [8]. To be honest it is fear to mention that almost all of the developments in 5G networks were made and continue in strict accordance with the 3GPP roadmap (Figure 2a) [9]. And the current situation regarding the deployment of the different types of 5G networks is represented on the Figure 2b [10].




(a) (b)

***Fig.2**. Current status of 5G networks deployment (a) according to the 5G networks standardisation roadmap (b)*

**LINKS BETWEEN 5G PPP PROJECTS**

To achieve already mentioned above requirements defined for the 5G networks was made a lot of job, lot of tasks were solved in different working groups. Their activities were related to the development of novel solutions, architecture, standards etc. To support all these activities was organized the 5G PPP organization.

**The 5G Infrastructure Public Private Partnership (5G PPP)** is a joint initiative between the European Commission and European ICT industry (ICT manufacturers, telecommunications

operators, service providers, SMEs and researcher Institutions) [11]. The 5G-PPP is now in its third phase and many new projects were launched in June 2018. The aim of the 5G PPP is to deliver solutions, architectures, technologies and standards for the next generation communication infrastructures in the nearest future. The challenge for the 5G Public Private Partnership (5G PPP) is to secure Europe's leadership in the particular areas where Europe is strong or where there is potential for creating new markets such as smart cities, e-health, intelligent transport, education or entertainment & media [11]. The 5G PPP was organised in three phases, encompassing research, optimisation and large scale trials. The aim of this paper is to showcase the links between different phases of 5G PPP and exact projects (Figure 3). It is made on the basis of the experience from participation in 5G PPP projects supported by European Comission (EC).
Currently for the Phase 3 have been retained 8 Projects in response to the 5G-PPP ICT-19-2019 call [12].


***Fig.3**. Links between three 5G PPP projects*

The first left project on Figure 3 is 5G-Xcast [13]. It was Phase 2 5G PPP research project. The main goal of this project was to bring the ability of multicast/broadcast delivery for 5G networks and it implementation to the architecture through the contributions to the standards (3GPP, ETSI, GSMA, DVB, etc.). The goals of the research were achieved by the very experienced consortium, which included manufacturers, academia, SMEs etc. The most outstanding achievement of the project was the 5G-Xcast core architecture for broadcast/multicast data delivery (Figure 4) [13].

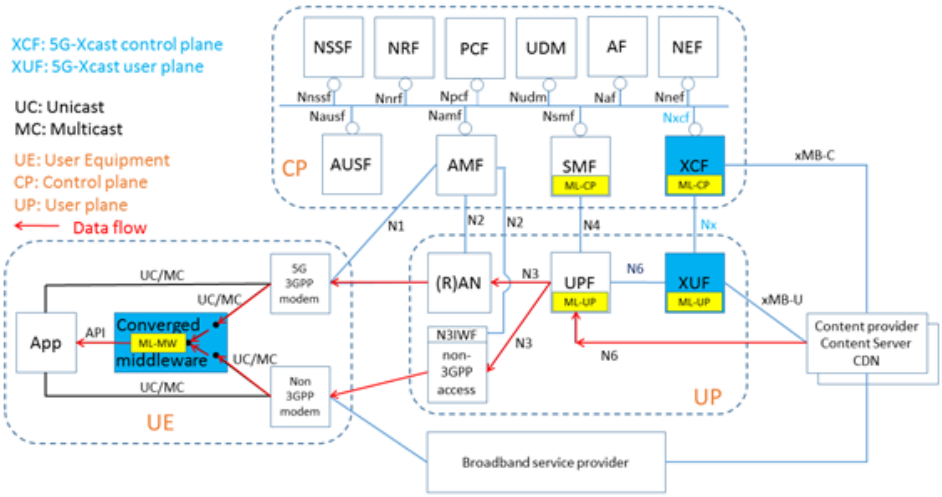



***Fig.4**. Developed 5G-Xcast core architecture for broadcast/multicast data delivery*

The functionality of new networks functions, architecture analysis were presented in the deliverables of the project [14] and of course in the research papers [15 – 17].
Some of the project results were successfully reused in the Phase 3 5G PPP projects. These eight projects are ongoing. They started in June 2019. The main goal of lunching these projects is to get the European 5G Vision of "5G empowering vertical industries" closer to deployment.

5G-Xcast's results were used in 5G-TOURS project. 5G-TOURS vision is to improve the life in the city for the citizens and tourists, making cities more attractive to visit, more efficient in terms of mobility and safer for everybody [18]. 5G-TOURS is focused on the realization of 13 highly innovative use cases in three types of cities: Touristic city (Turin, Italy); Safe city (Rennes, France) and Mobility efficient city (Athens, Greece) (Figure 5).


***Fig.5**. 5G-TOURS vision*

To achieve the goals of the project was developed the unified 5G-TOURS architecture (Figure 6), which included the results from the past projects: 5G-MoNArch, 5G-Xcast and 5G-EVE. 5G-Xcast feature for the multicast/broadcast delivery was reused for the realization of the UC4 dedicated to the high definition multimedia content delivery in the center of Turin. Details regarding this realization can be found in the 5G-TOURS official newsletter [19].

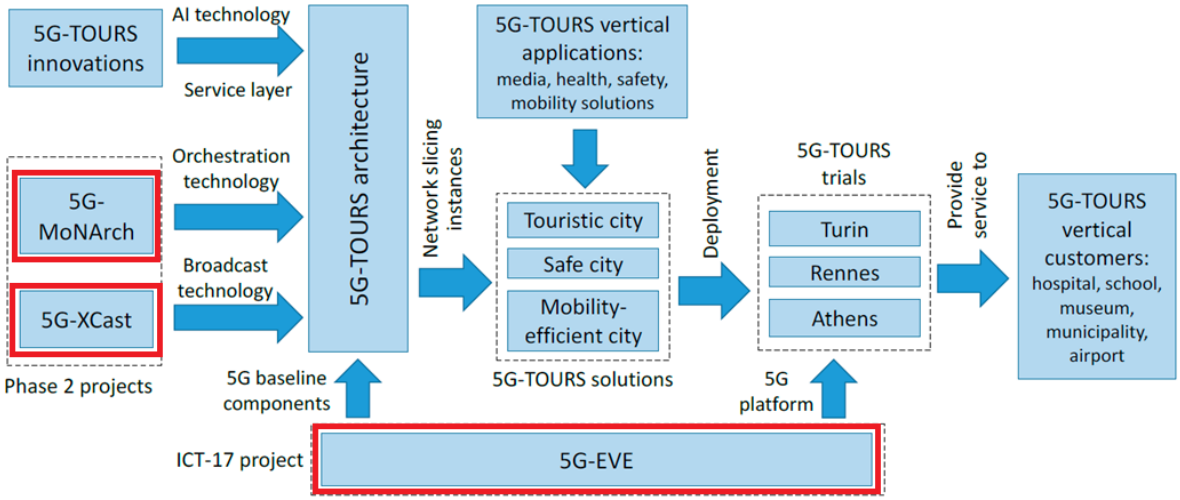



***Fig.6**. 5G-TOURS architecture*

The next project in which will be reused the results from the past and ongoing projects is 5GASP [20]. It just started in January 2021. It will be based on the achievements of 5G-VINNI [21] and 5G EVE [22] projects. Also, some methods for testing, validation and the whole methodology for QoE/QoE analysis probably will be used by the project, which aims at shortening the idea-to-market process through the creation of a European testbed for SMEs that is fully automated and self-service, in order to foster rapid development and testing of new and innovative NetApps built using the 5G NFV based reference architecture [20]. The architecture of the project and related projects are represented on Figure 7.

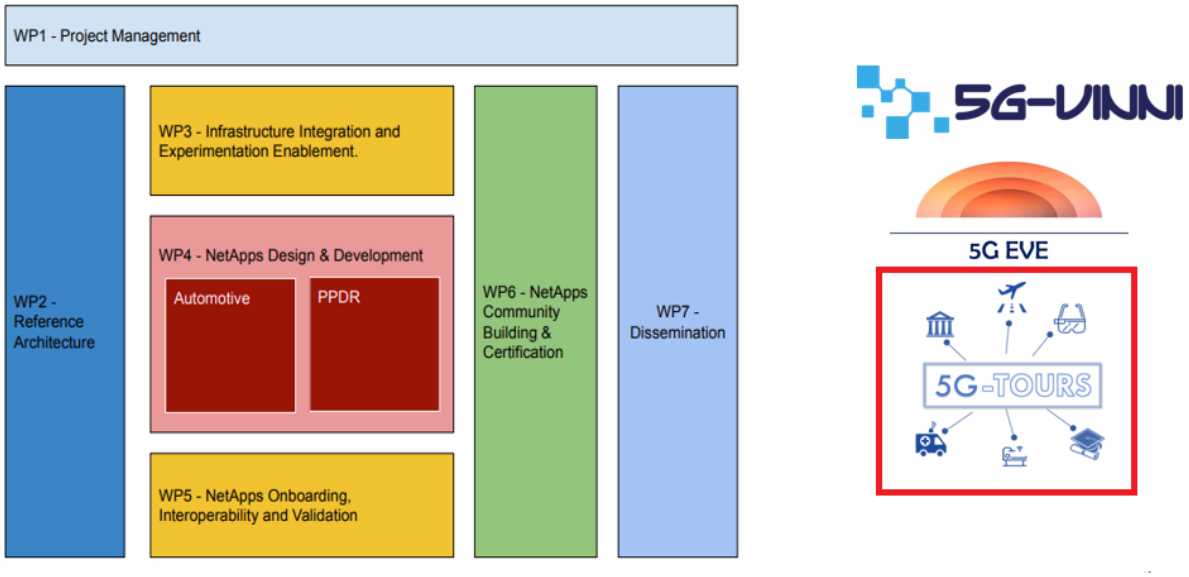



***Fig.7**. 5GASP project structure*

## CONCLUSIONS

5G networks are the future of the telecom industry. It is obvious that these networks will become the most widespread telecommunication technological solution in the next decade. To ensure the European leadership in the direction of the development and deployment of 5G networks 5G PPP in close collaboration with EC supports these activities. There were already launched the 5G PPP project of three phases. Projects of different phases are closely linked. This paper presented the links between 5G-Xcast, 5G-TOURS, and 5GASP projects, the continuity of the conducted research activities, and new directions of future research. There were showcased which technologies and solutions from the past projects were reused for other projects and probably will be reused for further studies. And the most valuable is the long-term follow-up of research according to the 5G PPP research roadmap. This hopefully will help to support vendors, MNOs, SMEs, and verticals in the EU on the road to the future information society.

## REFERENCES

1. Webster, F. (2014). Theories of the information society. Routledge.
2. https://www.gsma.com/futurenetworks/wiki/cloud-ar-vr-whitepaper/
3. Report M.2134: Requirements related to technical performance for IMT-Advanced radio interface(s)". ITU-R. November 2008. Retrieved 25 August 2011
4. https://www.etsi.org/technologies/5G
5. https://www.etsi.org/technologies/5G
6. Benisha, M., Prabu, R. T., & Bai, V. T. (2016, February). Requirements and challenges of 5G cellular systems. In 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB) (pp. 251-254). IEEE.
7. https://venturebeat.com/2018/10/01/verizon-activates-worlds-first-5g-network-in-4-u-s-cities/
8. https://www.mobileworldlive.com/blog/intelligence-brief-how-is-5g-faring-in-south-korea
9. https://artes.esa.int/news/integration-non-terrestrial-solutions-5g-standardisation-roadmap
10. https://www.statista.com/chart/23194/5g-networks-deployment-world-map/
11. 5G PPP official website: https://5g-ppp.eu/
12. Phase 3 5G PPP projects: https://5g-ppp.eu/5g-ppp-phase-3-projects/
13. 5G-Xcast project official website: https://5g-xcast.eu/
14. 5G-Xcast deliverables: http://5g-xcast.eu/documents/

15. Roman Odarchenko, Baruch Altman, Rui Aguiar and Yevgeniya Sulema Multilink Approach for the Content Delivery in 5G Networks 5th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2018 - Conference Proceedings, pp 140-144
16. D. Mi, R. Odarchenko et al., "Demonstrating Immersive Media Delivery on 5G Broadcast and Multicast Testing Networks," in IEEE Transactions on Broadcasting, doi: 10.1109/TBC.2020.2977546.
17. Odarchenko, R., Tran, T., Navrátil, D., Sanders, P., (...), Burdinat, C., Gomez-Barquero, D. Enabling Multicast and Broadcast in the 5G Core for Converged Fixed and Mobile Networks IEEE Transactions on Broadcasting. 66(2),9099058, c. 428-439. **DOI:** 10.1109/TBC.2020.2991548 https://ieeexplore.ieee.org/document/9099058]
18. 5G-TOURS project official website: http://5gtours.eu/
19. 5G-TOURS official newsletter 1: http://5gtours.eu/documents/newsletters/issue-1.pdf
20. 5GASP project official website: https://5gasp.eu/
21. 5G-VINNI official website: https://www.5g-vinni.eu/
22. 5G EVE official website: https://www.5g-eve.eu/

**Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 51-63 ISSN 2587-4667**
**Scientific Cyber Security Association (SCSA)**

# THE MODEL NEW QUANTUM RANDOM NUMBER GENERATOR WITH THE CORRESPONDING VERIFICATION METHOD.

**Tamari Kuchukhidze, Georgian Technical University, Scientific Cyber Security Association**
**Tbilisi, Georgia**

**ABSTRACT**: Random number generators are widely used in various fields including encryption, statistical analysis and numerical simulations. They are also a fundamental resource in science and engineering.
There are algorithmically generated numbers that look like random numbers but are not truly random, called pseudo random number generators. In cases where true randomness is necessary, we use true random number generators, where unpredictable random events are used as a random source.
Quantum Random Number Generators (QRNGs) generate real random numbers based on the inherent randomness of quantum measurements. Our goal is to generate fast random numbers at a lower cost. At the same time, a high level of randomness is essential.
It is essential to trust cryptographic random number generators to generate only true random numbers. This is why certification methods are needed which will check both the operation of the device and the quality of the random bits generated.
We present the improved novel quantum random number generator, which is based the on time of arrival QRNG. It is rather efficient, as it uses the simple version of the detectors with rather few requirements. The novel QRNG produces more than one random bit per each photon detection.
Self-testing as well as device independent quantum random number generation methods are analyzed. The advantages and disadvantages of both methods are identified. The model of a novel semi self-testing certification method for quantum random number generators (QRNG) is offered in the paper. This method combines different types of certification approaches and is rather secure and efficient. The paper analyzes its security and efficiency.

**KEYWORDS:** *quantum, random number generator, quantum random number generator, novel quantum random number generator, certification.*

**რეზიუმე**: შემთხვევითი რიცხვის გენერატორები ფართოდ გამოიყენება სხვადასხვა სფეროში, მათ შორის დაშიფვრა, სტატისტიკური ანალიზი და რიცხვითი სიმულაციები. ისინი ასევე ფუნდამენტური რესურსია მეცნიერებასა და ინჟინერიაში.
არსებობს ალგორითმულად გამომუშავებული ციფრები, რომლებიც შემთხვევითი განაწილების მსგავსია, მაგრამ სინამდვილეში შემთხვევითი არ არის, რომლებსაც ფსევდო შემთხვევითი რიცხვის გენერატორებს უწოდებენ. იმ შემთხვევებში, როცა ჭეშმარიტი შემთხვევითობა აუცილებელია, ჩვენ ვიყენებთ ნამდვილ შემთხვევითი რიცხვის გენერატორებს. ამ შემთხვევაში, არაპროგნოზირებადი შემთხვევითი მოვლენებია, როგორც შემთხვევითი წყარო.
კვანტური შემთხვევითი რიცხვის გენერატორებმა (QRNG) გამოაქვთ ნამდვილი შემთხვევითი რიცხვები კვანტური გაზომვების თანდაყოლილი შემთხვევითობის

საფუძველზე. ჩვენი მიზანია სწრაფი შემთხვევითი რიცხვების გენერირება უფრო დაბალ ფასად. ამავე დროს, აუცილებელია შემთხვევითობის მაღალი დონე.
საჭიროა ვენდოთ კრიპტოგრაფიული შემთხვევითი რიცხვის გენერატორებს, რომ ისინი წარმოქმნიან მხოლოდ ჭეშმარიტი შემთხვევითი რიცხვებს. ამიტომ გვჭირდება სერთიფიცირების მეთოდები, რომლებიც შეამოწმებს როგორც მოწყობილობის მუშაობას, ასევე წარმოქმნილი შემთხვევითი ბიტების ხარისხს.
ჩვენ წარმოგიდგენთ გაუმჯობესებულ ახალ კვანტურ შემთხვევითი რიცხვების გენერატორს, რომელიც ემყარება QRNG ჩამოსვლის დროს. ეს საკმაოდ ეფექტურია, რადგან იყენებს დეტექტორების მარტივ ვერსიას, საკმაოდ მცირე მოთხოვნებით. ახალ QRNG -ს შეუძლია ერთზე მეტ შემთხვევით ბიტის გამოვლენა თითოეულ ფოტონის აღმოჩენისას.
გავაანალიზებთ როგორც თვითტესტირებას, აგრეთვე მოწყობილობაზე დამოუკიდებელი კვანტური შემთხვევითი რიცხვის წარმოქმნის მეთოდებს. განვიხილავთ ორივე მეთოდის დადებით და უარყოფითი მხარეებს. ნაშრომში მოცემულია ახალი ნახევრად თვითტესტირების სერთიფიცირების მეთოდის მოდელი კვანტური შემთხვევითი რიცხვის გენერატორებისთვის (QRNG). ეს მეთოდი აერთიანებს სხვადასხვა ტიპის სერთიფიკაციის მიდგომებს, საკმაოდ უსაფრთხო და ეფექტურია. ნაშრომი აანალიზებს მის უსაფრთხოებასა და ეფექტურობას.

**საკვანძო სიტყვები:** *კვანტური, შემთხვევითი რიცხვების გენერატორები, კვანტური შემთხვევითი რიცხვების გენერატორები, ახალიკვანტური შემთხვევითი რიცხვების გენერატორები, სერტიფიკაცია.*

## 1. შესავალი

შემთხვევითი რიცხვები ფართოდ გამოიყენება სხვადასხვა სფეროში, მაგალითად, სიმულაცია, კრიპტოგრაფია, ფუნდამენტური მეცნიერება [1,2]. ალგორითმულად გამომუშავებული რიცხვები ჰგავს შემთხვევით რიცხვებს, მაგრამ ისინი ნამდვილად არ არიან შემთხვევითი; მათ ფსევდო შემთხვევით რიცხვებს უწოდებენ. ეს რიცხვები წარმოიქმნება კომპიუტერის გამოყენებით, დეტერმინესიული ალგორითმების საშუალებით, რომლებსაც ფსევდო შემთხვევითი რიცხვის გენერატორებს უწოდებენ [3-5]. რადგან, ჩვენ არ შეგვიძლია გამოვიყენოთ ფსევდო შემთხვევითი გენერატორები ისეთ სიტუაციებში, როდესაც ჭეშმარიტი შემთხვევითი შემთხვევაა საჭირო, ჩვენ ვიყენებთ ნამდვილი შემთხვევითი რიცხვის გენერატორებს. ამ შემთხვევაში, ჩვენ ვიყენებთ არაპროგნოზირებად შემთხვევით მოვლენებს, როგორც შემთხვევით წყაროს.

ზოგიერთ პროგრამაში, მაგალითად კვანტური კრიპტოგრაფია, ყველა ჭეშმარიტი შემთხვევითი რიცხვის გენერატორი არ არის კრიპტოგრაფიულად დაცული. ჩვენ შეგვიძლია გამოვყოთ TRNG ტიპის QRNG, რომელიც კვანტურ პროცესებში იყენებს თანდაყოლილ შემთხვევითობას, როგორც შემთხვევით წყაროს. არსებული QRNG– ების უმეტესობა ემყარება

კვანტურ ოპტიკას. სინათლის კვანტური მდგომარეობის ბევრ პარამეტრს აქვს თანდაყოლილი შემთხვევითობა, რის შედეგად მრავალი ვარიანტი შეგვიძლია განვახორციელოთ. ლაზერების, დიოდების ან ფოტონის სხვადასხვა წყაროდან მიღებული სინათლე უფრო ხელმისაწვდომია, ვიდრე რადიოაქტიური მასალა. სინათლის ნაწილაკები გამოიყენება კვანტური შემთხვევითობის წყაროდ და ხელმისაწვდომია მრავალი დეტექტორისთვის. შედეგად, ოპტიკური კვანტური შემთხვევითი გენერატორები უფრო სწრაფი და ეფექტურია [6].

საჭიროა ვენდოთ კრიპტოგრაფიული შემთხვევითი რიცხვის გენერატორებს, რომ ისინი წარმოქმნიან მხოლოდ ჭეშმარიტი შემთხვევითი რიცხვებს. მომხმარებლები სრულად უნდა ენდობოდნენ ფსევდო შემთხვევითი რიცხვის გენერატორების ან მოწყობილობის ალგორითმებს, რომელიც ახორციელებს ჭეშმარიტად შემთხვევითი რიცხვების გენერირების მეთოდს. შეგვიძლია ჩვენ თავიდან შევქმნათ შემთხვევითი რიცხვების გენერატორი, მაგრამ ეს არასასურველია. უკვე არსებობს მრავალი საიმედო ალგორითმი და მოწყობილობა, რომლებმაც გაუძლეს წლების განმავლობაში კრიპტანალიზისა და თავდასხმის მცდელობებს.

ეს ნიშნავს, რომ მომხმარებელი უნდა ენდოს მოწყობილობას ან ალგორითმს. პრობლემა, რომელიც თეორიულად ან მარტივად გამოიყურება, შეიძლება ადვილად არ გამოსწორდეს. ბოლოდროინდელმა მოვლენებმა აჩვენა, რომ RNGs მაცდური სამიზნეა ფარული შეტევებისთვის [7-9].

ჩვენ გვაქვს მაგალითები მოწყობილობის დონის თავდასხმის შემთხვევაში, თუ როგორ შეძლო არაკეთილსინდისიერმა მწარმოებელმა ან რომელიმე თავდამსხმელმა შეცდომა გამოიწვიოს მოწყობილობაში შესვლისას. ასეთ ტექნიკურად განვითარებულ შეტევაში თავდამსხმელს შეეძლო დაუშვა შეცდომები, რომელთა ამოცნობაც რთულია რეალურ სამყაროში RNG– ებში.

ფიზიკური შემთხვევითი რიცხვის გენერატორებისთვის გვაქვს ისეთი პრობლემები, როგორიცაა შესაძლო სპონტანური შეწყვეტა. თუ მოწყობილობის კომპონენტი შეწყვეტს მუშაობას ან დეგრადირდება, გამომავალი ბიტების ხარისხი შეიძლება შეიცვალოს. თუ მოწყობილობა ქმნის მნიშვნელობებს, მოწყობილობის ფარული ხარვეზების გამოვლენა განსაკუთრებით რთულია. ამ მიზეზით, უსაფრთხოების რეკომენდაციები საჭიროებს ერთგვარ თვით ტესტირებას ნამდვილი კვანტური რიცხვის გენერატორებში. ქვესისტემამ უნდა გააკონტროლოს მოწყობილობის მდგომარეობა ნებისმიერ დროს.

ნაშრომის მიზანია სწრაფი შემთხვევითი რიცხვების გენერირება დაბალ ფასად. შემთხვევითობის მაღალი დონე სავალდებულოა. ჩვენ წარმოგიდგენთ გაუმჯობესებულ ახალ კვანტურ შემთხვევითი რიცხვების გენერატორს, რომელიც ემყარება მოსვლის დროზე დაფუძნებულ. ეს საკმაოდ ეფექტურია, რადგან იყენებს დეტექტორების მარტივ ვერსიას, საკმაოდ მცირე მოთხოვნებით. ახალ QRNG -ს შეუძლია ერთზე მეტ შემთხვევით ბიტის გამოვლენა თითოეულ ფოტონის აღმოჩენისას.

შევისწავლეთ არასანდო მოწყობილობებთან მუშაობის კვანტური გზები. პირველად გაანალიზებულია QRNG- ის თვითტესტირების მეთოდი, შემდეგ კი მოწყობილობაზე დამოუკიდებელი კვანტური შემთხვევითი რიცხვის გენერატორების ანალიზი. განვიხილეთ კვანტური სერტიფიკაციის სხვადასხვა ფორმები. ამ მეთოდების საფუძველზე შემოგთა კვანტური სვაზებთ ერტიფიკაციის ახალი მეთოდს [10].

## 2. შემთხვევითი რიცხვების გენერატორები

შემთხვევითი რიცხვის გენერატორები ფართოდ გამოიყენება სხვადასხვა სფეროში, მათ შორის დაშიფვრა, სტატისტიკური ანალიზი და რიცხვითი სიმულაციები. არსებობს ალგორითმულად გამომუშავებული ციფრები, რომლებიც შემთხვევითი განაწილების მსგავსია, რომლებსაც ფსევდო შემთხვევითი რიცხვის გენერატორებს უწოდებენ და არის შემთხვევითი რიცხვები, რომლებიც წარმოიქმნება არაპროგნოზირებადი ფიზიკური მოვლენების შედეგად. იმის გამო, რომ ჩვენ არ შეგვიძლია გამოვიყენოთ ფსევდო შემთხვევითი გენერატორები ისეთ სიტუაციებში, სადაც ჭეშმარიტი შემთხვევითი შემთხვევაა საჭირო, ჩვენ ვიყენებთ ნამდვილი შემთხვევითი რიცხვის გენერატორებს. ამ შემთხვევაში, არაპროგნოზირებადი შემთხვევით მოვლენები გამოიყენება როგორც შემთხვევითობის წყაროს.

მეთოდებს, რომლებიც წარმოქმნიან შემთხვევითი რიცხვებს დეტერმინული ალგორითმებიდან, ეწოდება ფსევდორანდომული რიცხვის გენერატორი (PRNG). ბუნებრივია, რომ ალგორითმის მიერ გამომუშავებული თანმიმდევრობა ჭეშმარიტად არ არის შემთხვევითი, ხშირ შემთხვევაში ამ ტიპის შემთხვევითობა საკმარისია. სიჩქარის დიდი უპირატესობის გამო, ხშირად გამოიყენება ასეთი გენერატორი, დეტერმინირებული მეთოდი, რომელიც ბაძავს ნამდვილად შემთხვევითი წყაროს მოსალოდნელ ქცევას [11].

PRNG ეფექტურია, შეუძლია მოკლე დროში შექმნას მრავალი რიცხვი. განსაკუთრებით ისეთ შემთხვევაში, თუ გვინდა ბევრი შემთხვევითი რიცხვი, ან მოგვიანებით აუცილებელია არსებული განაწილების გამეორება. ფსევდო შემთხვევითი რიცხვის გენერატორები პერიოდულია, რაც არ არის სასურველი მახასიათებელი, თუმცა, ხანგრძლივი პერიოდის შემთხვევაში, მას თავიდან ავიცილებთ.

PRNG განკუთვნილია ისეთი პროგრამებისთვის, როგორიცაა სიმულაცია და მოდელირება. PRNG არ არის შესაფერისი განხორციელებებისთვის, სადაც ციფრები უნდა იყოს არაპროგნოზირებადი, როგორიცაა მონაცემთა დაშიფვრა და აზარტული თამაშები. ასეთ შემთხვევებში საჭიროა ჭეშმარიტი შემთხვევითი რიცხვის გენერატორების (TRNG) გამოყენება.

TRNG იყენებს რეალურ არაპროგნოზირებად ან ძალიან რთულად პროგნოზირებად რეალურ პროცესებს, შემთხვვევითი თანმიმდევრობების წარმოქმნის მიზნით. ისინი ეყრდნობიან

არაპროგნოზირებად მნიშვნელობებს, რომლებიც კომპიუტერში, პროგრამაში ან სპეციალურ მოწყობილობებშია დაყენებული და გადაეცემა ოპერაციულ სისტემებს. ჭეშმარიტი შემთხვევითი რიცხვის გენერატორები შედგება ორი კომპონენტისგან: არაპროგნოზირებადი წყარო მაღალი ენტროპიით და ფუნქცია, რომელიც გვაძლევს თანაბარი განაწილების მიახლოებას [12,13].

კლასიკური მოვლენები ვერ ჩავთვლით ჭეშმარიტად შემთხვევითად. საეჭვოა, ფიზიკური პროცესი ნამდვილად შემთხვევითია თუ მისი პროგნოზირება ძალიან რთულია. თუ გვინდა ვიყოთ დარწმუნებული გამომავალი რიცხვების შემთხვევითობაში, უნდაგამოიყენეთ კვანტური შემთხვევითი რიცხვების გენერატორები. ეს არის TRNG– ის განსაკუთრებული შემთხვევა, როდესაც მონაცემები მიიღება კვანტური მოვლენის შედეგად. სხვა ფიზიკური სისტემებისგან განსხვავებით, ნამდვილი შემთხვევითობა კვანტური მექანიკის მნიშვნელოვანი ნაწილია. კვანტური შემთხვევითი რიცხვის გენერატორები გამოირჩევიან ამ ასპექტით, კარგად განსაზღვრული თანდაყოლილი, მემკვიდრეობით მიღებული შემთხვევითი პროცესების გამოყენებით, ბიტების წარმოსაქმნელად.

## 3. კვანტური შემთხვევითი რიცხვების გენერატორები.

PRNG– ს უმეტესობას არ შეუძლია შექმნას კრიპტოგრაფიულად დაცული შემთხვევითი რიცხვები [14-16]. არსებობს კრიპტოგრაფიაში ფსევდო-შემთხვევითი რიცხვის გენერატორების გამოყენების გზები. ალგორითმული გენერატორები, რომლებიც აკმაყოფილებენ დამატებით კრიტერიუმებს, ეწოდება კრიპტოგრაფიულად უსაფრთხო ფსევდორანდომიული გენერატორების, CSPRNG- ებს.

ფიზიკური შემთხვევითი რიცხვების გენერატორები, ასევე კვანტური შემთხვევითი რიცხვების გენერატორებიც შეიძლება გამოვიყენოთ როგორც საწყისი მნიშვნელობები CSPRNG– ებისთვის [17,18]. მაგრამ სიფრთხილე უნდა მივიღოთ. ზოგიერთი შეტევა უტევს TRNG– ებს და მგრძნობიარეა გარემო პირობებიდან მიღებულ ცვლადების მიმართ. არსებობს QRNG ონლაინ ტესტები, რომლებიც ამოწმებენ აკმაყოფილებს თუ არა BSI AIS 20/31 სტანდარტს. სანამ ეს ასპექტები გაითვალისწინება, მრავალი QRNG გვთავაზობს გასაღებების უშუალო წარმოქმნას გარკვეული ტიპის დამუშავების შემდეგ.

შემუშავებულია მრავალი სტატისტიკური ტესტი RNG შედეგების შემთხვევითობის შესამოწმებლად, მაგრამ RNG ტესტირება არ იძლევა უტყუარ შედეგებს. ამრიგად, ჭეშმარიტი შემთხვევითობის მიღება შესაძლებელია მხოლოდ ისეთი პროცესების საშუალებით, რომლებსაც თანდაყოლილი შემთხვევითობა გააჩნიათ. ასეთი წყაროა კვანტური შემთხვევითი რიცხვის გენერატორი.

## 4. ოპტიკური კვანტური შემთხვევითი რიცხვების გენერატორები.

ჭეშმარიტი შემთხვევითობა შეიძლება წარმოიშვას ნებისმიერი კვანტური პროცესისგან, რომელიც მდგომარეობების თანმიმდევრულ სუპერპოზიციას არღვევს. დღესდღეობით, ხელმისაწვდომია მაღალი ხარისხის ოპტიკური კომპონენტებია, ამიტომ ყველაზე პრაქტიკული QRNG- ები ხორციელდება ფოტოსისტემებში.

კოჰერენტული მდგომარეობა, რომელსაც კლასიკური სინათლის მრავალი თვისება იზიარებს, შეიძლება დაიწეროს რიცხვითი მდგომარეობის სუპერპოზიციაში

$$|\alpha>=e^{-\frac{|\alpha|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n>$$

სადაც α კომპლექსური რიცხვია, n ფოტონების რაოდენობა. ამპლიტუდა $|\alpha|^2$ შეესაბამება მდგომარეობაში ფოტონების საშუალო რაოდენობას. სუსტი ლაზერის სინათლე ახლოს არის კოჰერენტულ მდგომარეობასთან. შეგვიძლია გამოვიყენოთ ლაზერისგან მიღებული კოჰერენტული მდგომარეობა, ერთი ფოტონის მდგომარეობის მისაღებად, თუ საკმარისად დაბალ ინტენსივობას შევარჩევთ.

ხშირ შემთხვევაში გვაინტერესებს მხოლოდ არაკოლერირებული ფოტონების გამომუშავება. ამ შემთხვევაში, LED–დან მიღებული სინათლე ვალიდურია მანამ, სანამ მანძილი ფოტონების წარმოშობიდან უფრო მეტია, ვიდრე წყაროს კოჰერენტული დრო.

მრავალ ტექნოლოგიას შეუძლია შექმნას და გამოავლინოს ერთი ფოტონი, მაგალითად: ფოტომულტიპლიკაციური მილები (PMT), SPAD, ზეგამტარი ნანოსადენების დეტექტორები. ეს არის პოპულარული დეტექტორების მაგალითები.

ტრადიციულად, ერთ ფოტონის დეტექტორებს აქვთ ფოტონის დათვლის შეზღუდული შესაძლებლობა. შემთხვევითობის მიღება ისეთი კვანტური მდგომარეობებიდანაც შეიძლება, რომლებიც მრავალ ფოტონს შეიცავს. არის გაუმჯობესებული დეტექტორები, მაგრამ ძვირია. აპლიკაციების უმეტესობა ფოტონის გამოვლენის ოროობით მიდგომას იყენებს. ერთი ფოტონის დეტექტორების შემდეგი შეზღუდვაა ფოტონების გამოვლენის შემდეგ აღდგენისთვის საჭირო დრო, რომელსაც ეწოდება მკვდარი დრო.

## 5. ახალი კვანტური შემთხვევითი რიცხვების გენერატორები.

ჩვენი მიზანია უფრო დაბალ ფასად მოვახდინოთ სწრაფი შემთხვევითი რიცხვების გენერირება. ამავე დროს, აუცილებელია შემთხვევითობის მაღალი დონე. ნებისმიერი კვანტური პროცესის დარღვევა იწვევს ჭეშმარიტ შემთხვევითობას, მაგრამ წარმოქმნის სიხშირე დამოკიდებულია დეტექტორის წარმოებაზე [19].

ჩვენ გთავაზობთ გაუმჯობესებულ კვანტურ შემთხვევითი რიცხვების გენერატორს, რომელიც ემყარება QRNG ჩამოსვლის დროს. საუკეთესო შემთხვევაში, თითოეული გამოვლენილი ფოტონიდან ვიღებთ მხოლოდ ერთ შემთხვევით ბიტს, ეს ალბათობა მცირდება დეტექტორის არაეფექტურობით ან მკვდარი დროით. უმეტეს შემთხვევაში, შემთხვევითი რიცხვის გენერატორების სიხშირე იზომება მეგაბაიტებით, რაც არ არის საკმარისი სწრაფი პროგრამებისთვის, როგორიცაა QKD. თუ მრავალ დეტექტორს გამოვიყენებთ უფრო მეტი შემთხვევითი ბიტების შესაქმნელად, ჩვენ გვექნება მიკერძოება, რომელიც წარმოიქმნება დეტექტორების სხვადასხვა ეფექტურობის შედეგად. ერთი დეტექტორის გამოყენებით და გამოვლენის დროის სამი წარმატებული მოვლენის შედარებით, შეგვიძლია გამოვრიცხოთ ეს მიკერძოება. საკმაოდ მოსახერხებელია დეტექტორების მარტივი ვერსიის გამოყენება, რომელსაც შედარებით მცირე მოთხოვნები გააჩნია. ჩვენ გთავაზობთ გამოვიყენოთ ტექნოლოგია, რომელიც გამოიყენება დასუსტებული პულსის კვანტური შემთხვევითი რიცხვის გენერატორებში.

ჩვენ გთავაზობთ OQRNG– ს, რომელსაც სინათლის სუსტი წყარო გააჩნია და ფოტონის გენერაციის ან არ წარმოქმნის ალბათობა თანაბარია. ისე, რომ ერთი ფოტონის მდგომარეობა უნდა იყოს:

$$\frac{|0>_1+|1>_1}{\sqrt{2}}$$

შეგვიძლია მივანიჭოთ 0 თუკი არ მოხდა აღმოჩენა, ხოლო 1 თუ დაკლიკება მოხდა. არ გვაინტერესებს რამდენი ფოტონი გამოვიყენეთ. სუპერპოზიციის დაწერა შეიძლება შემდეგნაირად:

$$\frac{1}{\sqrt{2}}|0>_1+\sum_{c=1}^{\infty}\alpha_c\,|c>_1$$

სადაც $\sum_{c-1}^{\infty}|\alpha_c|^2=\frac{1}{2}$ ვალიდურია. პირველი დაჭერისას ვიღებთ და არ გვაინნტერესებს ერთმა ფოტონმა გამოიყვია თუ მრავალმა. α ამპლიტუდის კოჰერენტული მდომარეობისთვის, ფოტონის პოვნის ალბათობაა 0 თუ

$$pr(n=0)=e^{-|\alpha|^2}$$

ერთი ამ მეტი ფოტონის პოვნის ალბათობაა

$$pr(n\geq 1)=(1-e^{-|\alpha|^2})$$

ყველაზე მარტივი იდეაა ვიპოვოთ α, რომლისთვისაც pr(n = 0) = pr (n ≥ 1). ამ ფორმულისთვის $\alpha=\sqrt{ln2}$. სასურველ აღმოჩენის ალბათობას გვაძლევს პუასონური წყარო, სადაც $\psi$T = ln2 ≈ 0.693.

პრაქტიკაში, გენერატორი მუშაობს ეფექტურ საშუალო ფოტონთა რიცხვზე $\eta\psi T$ დეტექტორზე, $\eta$ ეფექტურობით. ფონ ნოიმანის ექსტრაქცია უნდა გამოვიყენოთ, რომ არ გვქონდეს მუშაობის პროცესში მიკერძოება. ფოტონის ორი აღმოჩენისთვის, სადაც მათი რაოდენობა $n_1$ და $n_2$ -ია, გამომავალი მნიშვნელობაა 1, თუ $n_1 > 0$ და $n_2 = 0$ და 0 თუ $n_1 = 0$ და $n_2 > 1$. შედეგები, ორი თანმიმდევრული ცარიელი პერიოდით ან ორი დაწკაპებით უგულვებელყოფილია. პუასონური წყაროსთვის, ეს ორივე ბიტის მნიშვნელობა შეიძლება მოხდეს ალბათობით $pr(n > 0)pr(n = 0) = e^{-\eta\psi T}(1 - e^{-\eta\psi T})$. შედეგად მიღებული ბიტევის სიჩქარე ოთხჯერ მაინც ნელია, მაგრამ ყველანაირი მიკერძოებისგან თავისუფალი.

ეფექტურობის გასაუმჯობესებლად გთავაზობთ გენერატორის გამოყენებას, რომელიც ფოტონის გამოვლენის შემდეგ ერთზე მეტ შემთხვევით ბიტს წარმოქმნის. ასეთი ტიპისაა ფოტონის დათვლის კვანტური შემთხვევითი რიცხვების გენერატორები. მიღებული შედეგები დაიყოფა ჯგუფებად, რომლებსაც თანაბარი ალბათობა აქვთ. ამ შემთხვევაში, ჩვენ შეგვიძლია გამოვიყენოთ ერთი დეტექტორი მონაცემების გენერაციისთვის. ჩვენ შეგვიძლია ავიღოთ ფოტონების მოსვლის დრო, როგორც კვანტური შემთხვევითი ცვლადი. წარმატებული ფოტონის დრო შეიძლება დაიყოს დროის ბინებად, შექმნილი მრიცხველის მიერ, რომელიც მუშაობს დეტექტორის პარალელურად. მოცემული აღმოჩენის დროის ინტერვალი გვაძლევს რამდენიმე ბიტს თითო აღმოჩენისთვის. ამ პროცესში მოვლენები ვითარდება დამოუკიდებლად, არის პუასონური პროცესი [20].

შემთხვევითი რიცხვის წარმოქმნის სიხშირის გასაზრდელად გთავაზობთ გაზომვების ჩატარებას მაღალგანზომილებიან კვანტურ სივრცეში, მაგალითად ფოტონის დროით და სივრცული რეჟიმში. ფოტონის მოსვლის დროის გაზომვით, ვიღებთ შემთხვევით ბიტებს დროის ინტერვალის, $\Delta t$, ორი მოვლენის აღმოჩენის შედეგად. დროითი რეჟიმის შემთხვევაში ერთი ფოტონის გამოვლენისას შეგვიძლია ერთზე მეტი შემთხვევითი ბიტი მივიღოთ. ფოტონის სივრცული რეჟიმის გამოყენებით, შეგვიძლია მივითოთ შემთხვევითი რიცხვები დეტექტორის მატრიცაში პარალელურად. ამ მეთოდის გამოყენებისას უმჯობესია ყურადღება მიაქციოთ მკვდარ დროს, რადგან ეს გავლენას ახდენს დეტექტორის მრიცხველის სიჩქარეზე [21].

გაუმჯობესებული სიხშირე გვეხმარება არჩევანის გაკეთებაში, თუ რამდენი ბიტი გამოვიყენოთ დათვლილი რაოდენობის ფოტონებიდან და მივიღოთ შემთხვევითობის მაღალი დონე.

## 6. ახალი ნახევრად თვითტესტირების მეთოდი

ჭეშმარიტი შემთხვევითობა შეუძლებელია მხოლოდ კლასიკური მექანიკის პროცედურებით, ამიტომ ვიყენებთ კრიპტოგრაფიულ პროტოკოლებს. კვანტური შემთხვევითი გენერატორები, მოწყობილობის სანდოობის მიხედვით, შეიძლება დაიყოს რამდენიმე კატეგორიად. პირველია თვით ტესტირებადი QRNG, რომელიც არ არის დამოკიდებული მოწყობილობაზე.

ამ ტიპის QRNG–ის უპირატესობა არის თვითტესტირების შემთხვევითი თვისება. მაგრამ, როგორც წესი, მისი გენერაციის მაჩვენებელი ძალიან დაბალია. მეორე კატეგორია არის მოწყობილობისგან დამოუკიდებელი კვანტური შემთხვევითი რიცხვის გენერატორები. იგი შექმნილია სრულიად საიმედო მოწყობილობებით და შეუძლია მიაღწიოს მაღალი გენერაციის სიჩქარეს, თუ მოწყობილობა სწორად არის მოდელირებული. წინააღმდეგ შემთხვევაში, როდესაც მოწყობილობას მოწინააღმდეგები აკონტროლებენ, შედეგი აღარ იქნება შემთხვევითი.

ამ ორ მიდგომას გააჩნია, როგორც დადებითი, ასევე უარყოფითი მხარეები. რეალურად განხორციელებისას, უფრო მისაღებია ავიღოთ გარკვეული მახასიათებლები და რაღაც შუალედური სერთიფიცირების მეთოდის გამოვიყენოთ. პრაქტიკული, მოწყობილობისგან დამოუკიდებელი კვანტური შემთხვევითი რიცხვის გენერატორებისა და თვითტესტირებადი QRNG-ის გაერთიანებით მივიღებთ ნახევრად თვითტესტირებად გენერატორს. ამ შემთხვევაში ჩვენ არ ვიქნებით მთლიანად დამოკიდებული მოწყობილობებზე. მოწყობილობისგან დამოუკიდებელი QRNG ხასიათდება მაღალი პროდუქტიულობითა და ეფექტურობით, ხოლო თვით ტესტირებად QRNG–ს გააჩნია სერტიფიკაციის შემთხვევითობის უფრო დიდი უსაფრთხოება.

ჩვენ გთავაზობთ ნახევრად თვით ტესტირებად QRNG-ს, რომელიც აერთიანებს თვით ტესტირებისა და მოწყობილობისგან დამოუკიდებელ QRNG-ის მისაღებ მახასიათებლებს.

თვითტესტირება კვანტურ გარემოში, რომელიც შექმნილია ერთი ფოტონის პოლარიზაციის სუპერპოზიციაში მუშაობისთვის არის

$$\psi = \frac{|H> + |V>}{\sqrt{2}}$$

ან ჩახლართულ მდგომარეობაში

$$\psi = \frac{|H>_1 |V>_2 + |V>_1 |H>_2}{\sqrt{2}}$$

კვანტური შემთხვევითი რიცხვის გენერატორი იყენებს გზის განშტოების პრინციპებს. პოლარიზატორები ფოტონს 50% ალბათობით ძლევენ უფლებას რომ გაიაროს. თეორიულად, ამ შემთხვევაში დამთხვევის მრიცხველი აღნიშნავს სრულყოფილ ანტიკორელაციას.

მოწყობილობაში არის ტესტირების ეტაპი, სადაც გაზომვების კომპლექტიდან შეყვანილი მდგომარეობის სრულ ტომოგრაფიას ხორციელდება, რათა დადგინდეს 2×2 მატრიცა,

რომელიც აღწერს ფოტონურ ორი დონის სისტემას ერთი ფოტონისთვის ან თუ გვაქვს ფოტონური წყვილის შემთხვევა, ეფექტურ ორგანზომილებიან ჰილბერტის სივრცეს. გაზომვების შედეგების მიხედვით, გენერატორი აფასებს შესაძლო მინიმალურ ენტროპიას $H_\infty(\hat{p})$, რომელიც არის მომხმარებლისა და მსმენელის საერთო მდგომარეობის მინიმალური შესაძლო ენტროპია, და $\hat{p}$ კი ყველაზე უარესია შესაძლო შედეგებში. ამის შემდეგ ბიტები გადაეცემა შემთხვევითობის ექსტრაქტორებს, რომელიც დააგენერერირებს უფრო მოკლე, მიუკერძოებელ შემთხვევით სტრიქონს ხელმისაწვდომი ენტროპიისთვის.

ეს მეთოდი გვიცავს ისეთი თავდასხმებისგან, სადაც მოწინააღმდეგეს შეუძლია გააკონტროლოს კვანტური მდგომარეობა, საიდანაც ვიღებთ ენტროპიას, მანამ სანამ არ გავაკეთებთ განმეორებით გაზომვებს ერთ მდგომარეობაზე. პირობითი ტომოგრაფიის სწორად შესასრულებლად უნდა ჩავთვალოთ, რომ გაზომილი მდგომარეობა შენარჩუნებულია მთელი პროცესის განმავლობაში. ასეთი თვითტესტირება მხოლოდ შეზღუდულ დაცვას გვთავაზობს.

ტომოგრაფია გთავაზობთ ენტროპიის შეფასებას იმ მოდელებში, სადაც განხორციელებისას მოსალოდნელია შეცდომები ან ოპერაციის დროს შეიძლება მოხდეს დარღვევები. ჩვენ ვგულისხმობთ, რომ შეცდომები არ ხდება არასანდო მწარმოებლის გამო. ეს მოდელი წარმოდგენილია თვით ტესტირებად QRNG, სადაც კვანტური შემთხვევითობის წყარო განცალკევებულია ტექნიკური ხმაურისგან dimension witness-ის გამოყენებით.

$$W = \begin{vmatrix} p(1|0,0) - p(1|1,0) & p(1|2,0) - p(1|3,0) \\ p(1|0,1) - p(1|1,1) & p(1|2,1) - p(1|3,1) \end{vmatrix}$$

თვით ტესტირებადი კვანტური შემთხვევითი რიცხვების გენერატორის პროტოკოლი შედგება ამ ნაბიჯებისაგან. პირველ რიგში, ტარდება ექსპერიმენტი, სადაც მომხმარებელი უკვე მზა მდგომარეობა x-ს და გაზომვა y, ვიღებთ შედეგს b. ამის შემდეგ, მონაცემებიდან შეიძლება გავზომოთ განაწილება p (b | x, y) და W, მოწმის მნიშვნელობის შეფასება შეგვიძლია. W იძლევა იდეას იმის შესახებ, "რამდენად კვანტურია" მომზადებისა და გაზომვების კომბინაცია. ნებისმიერი W> 0 გვიჩვენებს, რომ ზოგიერთი გაზომვა შეუთავსებელია და არსებობს გარკვეული კვანტური შემთხვევითობა, რომელიც საშუალებას იძლევა მივანიჭოთ გამოსაცნობი ალბათობა. შედეგი შეიძლება გამოყენებულ იქნას შემთხვევითობის ექსტრაქტორში შეკუმშვის დონის დასადგენად [22,23].

ალტერნატივაა გაურკვევლობის პრინციპის გამოყენება, რასი საშუალებით ნებისმიერი მოწინააღმდეგე ფლობს მხოლოდ ინფორმაციის შეზღუდულ რაოდენობას. წინა მეთოდების მსგავსად, ჩვენი მიზანი არ არის მხოლოდ შემთხვევითი ბიტების გამომუშავება, მაგრამ დარწმუნებული უნდა ვიყოთ, რომ ეს ბიტები კონფიდენციალურია (არცერთ გარე შემტევს არ შეუძლია ჩვენი თანმიმდევრობის გაგება). მაგალითად, თუ ჰორიზონტალურ ვერტიკალურ ბაზაზე ვზომავთ ფოტონის პოლარიზაციას ჩახლართულ მდგომარეობაში, მივიღებთ აბსოლუტურად შემთხვევით რიცხვებს, მაგრამ მოწინააღმდეგე, რომელსაც აქვს წვდომა ბიტების მეორე ნახევარზე, გაიგებს ზუსტ თანმიმდევრობას, რომლის მიღებაც იგივე

გაზომვებიდან შეგვიძლია. ეს შეიძლება იყოს მისაღები პროგრამებისთვის, როგორიცაა სიმულაცია, მაგრამ თავიდან უნდა იქნას აცილებული ინფორმაციის გაჟონვა კრიპტოგრაფიაში.

ჩვენ შეგვიძლია გამოვიყენოთ ბელის უტოლობების ვარიანტი, CHSH ფორმულირება. ორი მოწყობილობის გაზომვით შევისწავლით გაზომვის კორელაციებს და განვსაზღვრავთ ორ ცვლადს x და y, თითოეული თითოეული მოწყობილობისთვის. ეს ცვლადები იღებს ორ მნიშვნელობას, 0 და 1, რაც შეესაბამება ორ ორობით გაზომვას შორის არჩევანს. ორივე საზომი მოწყობილობა იდენტურია. X კონფიგურაციაში გაზომვები იძლევა a-ს ორობით მნიშვნელობას და y- ით განსაზღვრული გაზომვა იძლევა შედეგს b. ჩვენ გვაინტერესებს კორელაციის ფუნქცია, რომელიც განისაზღვრება შემდეგნაირად:

$$I = \sum_{x,y} (-1)^{x,y} [\mathrm{P}\ (\mathrm{a}\ =\ \mathrm{b} \mid \mathrm{xy}) - \mathrm{P}\ (\mathrm{a}\ \neq\ \mathrm{b} \mid \mathrm{xy})\ ]$$

სადაც P (a = b | xy) და P (a ≠ b | xy) არის ალბათობები, რომ a = b ან a ≠ b, როდესაც პარამეტრები არის x და y. რეალისტური ლოკალური თეორიისთვის ყოველთვის უნდა ვიპოვოთ I ≤ 2, რადგან ნებისმიერი მნიშვნელობა 2-ზე მეტი მიუთითებს არა ლოკალურობაზე [24].

ბელის უთანასწორობის შესაფასებლად, ეს ექსპერიმენტი უნდა ჩატარდეს n-ჯერ. თითოეული (x, y) გაზომვა წარმოიქმნება იდენტური და დამოუკიდებელი ალბათობის განაწილებით P (xy). n-ის საბოლოო გამომავალი სტრიქონი არის r = ($a_1$, $b_1$;...; $a_n$, $b_n$), და შემავალი s = ($x_1$, $y_1$;...; $x_n$, $y_n$). $\tilde{I}$ კი CHSH ფორმულის შემფასებელია, რომელიც განისაზღვრება შემდეგნაირად

$$\tilde{I} = \frac{1}{n} \sum_{x,y} (-1)^{x,y} [\mathrm{N}\ (\mathrm{a}\ =\ \mathrm{b} \mid \mathrm{xy}) - \mathrm{N}(\mathrm{a}\ \neq\ \mathrm{b} \mid \mathrm{xy})/\mathrm{P}(\mathrm{xy})\ ]$$

სადაც N (a = b, xy) არის რიცხვი, რამდენჯერ გაიზომა (x, y). შედეგები a და b აღმოჩნდა n-ის ტოლი. N (a≠B, xy) განისაზღვრება მსგავსად.

## 7. დასკვნა

ჩვენი ახალი კვანტური შემთხვევითი რიცხვის გენერატორის გამოყენებით შესაძლებელია ეფექტურად წარმოქმნას მეგაბიტი ან გიგაბიტი სიჩქარე. ჩვენი გენერატორი ემყარება მოსვლის დროზე დაფუძნებულ QRNG. საკმაოდ ეფექტურია, რადგან იყენებს დეტექტორების მარტივ ვერსიას, საკმაოდ მცირე მოთხოვნებით. ახალ QRNG-ს შეუძლია ერთზე მეტ შემთხვევით ბიტის გამოვლენა თითოეულ ფოტონის აღმოჩენისას.

შევისწავლეთ არასანდო მოწყობილობებთან მუშაობის კვანტური გზები. პირველად გაანალიზებულია QRNG- ის თვითტესტირების მეთოდი, შემდეგ კი მოწყობილობაზე

დამოუკიდებელი კვანტური შემთხვევითი რიცხვის გენერატორების ანალიზი. განვიხილეთ კვანტური სერტიფიკაციის სხვადასხვა ფორმები. ამ მეთოდების საფუძველზე შემოთავაზებულია კვანტური სერტიფიკაციის ახალი მეთოდი.

ეს მეთოდი შემუშავებულია მოწყობილობაზე დამოუკიდებელი გენერატორებით, რომელიც იყენებს კვანტური თეორიის სხვადასხვა ასპექტის ნაკლებად მკაცრ ექსპერიმენტულ ტესტებს, რის შედეგადაც ხდება უფრო შეზღუდული სერტიფიცირება უსაფრთხოების უფრო მოდუნებული დაშვებებით.

## ბიბლიოგრაფია

1. Kabiri Chimeh, M., Heywood, P., Pennisi, M. et al. Parallelisation strategies for agent based simulation of immune systems. BMC Bioinformatics 20, 579 (2019). https://doi.org/10.1186/s12859-019-3181-y
2. Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili// Novel Version of Merkle Cryptosystem// Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 4, 2017, p. 28-33
3. P. A. W. Lewis, A. S. Goodman and J. M. Miller, "A pseudo-random number generator for the System/360," in IBM Systems Journal, vol. 8, no. 2, pp. 136-146, 1969, doi: 10.1147/sj.82.0136.
4. Lambić, D., Nikolić, M. Pseudo-random number generator based on discrete-space chaotic map. Nonlinear Dyn 90, 223–232 (2017). https://doi.org/10.1007/s11071-017-3656-1
5. J. M. Mcginthy and A. J. Michaels, "Further Analysis of PRNG-Based Key Derivation Functions," in IEEE Access, vol. 7, pp. 95978-95986, 2019, doi: 10.1109/ACCESS.2019.2928768.
6. Herrero-Collantes, Miguel & Garcia-Escartin, Juan Carlos. (2016). Quantum Random Number Generators. Reviews of Modern Physics. 89. 10.1103/RevModPhys.89.015004.
7. High-Speed and Secure PRNG for Cryptographic Applications; T. Okhrimenko, S. Tynymbayev, M. Iavich; mecs-press.org, 2020.
8. Post-Quantum Digital Signatures with Attenuated Pulse Generator; M. Iavich, R. Bocu, A. Arakelian, G. Iashvili; ceur-ws.org, Vol-2698, 2020.
9. Improvement of Merkle Signature Scheme by Means of Optical Quantum Random Number Generators; M. Iavich, A. Gagnidze, G. Iashvili, T. Okhrimenko, A. Arakelian, A. Fesenko; Springer, 2020.
10. Ma, X., Yuan, X., Cao, Z., Qi, B., & Zhang, Z. (2016). Quantum random number generation.
11. Michael A. Wayne and Paul G. Kwiat, "Low-bias high-speed quantum random number generator via shaped optical pulses," Opt. Express 18, 9351-9357 (2010)
12. Michael A. Wayne and Paul G. Kwiat, "Low-bias high-speed quantum random number generator via shaped optical pulses," Opt. Express 18, 9351-9357 (2010)
13. Wayne, Michael & Jeffrey, Evan & Akselrod, Gleb & Kwiat, Paul. (2009). Photon arrival time quantum random number generation. Journal of Modern Optics. 56. 516-522. 10.1080/09500340802553244.
14. Hu Z., Gnatyuk S., Okhrimenko T., Tynymbayev S., Iavich M. High-speed and secure PRNG for cryptographic applications, International Journal of Computer Network and Information Security, Issue 12 (3), pp. 1-10, 2020.
15. Gnatyuk S., Okhrimenko T., Azarenko O., Fesenko A., Berdibayev R. Experimental Study of Secure PRNG for Q-trits Quantum Crypto-graphy Protocols, Proceedings of the 2020 IEEE 11th

International Conference on Dependable Systems, Services and Technologies (DESSERT 2020), Kyiv, Ukraine, May 14, 2020, pp. 183-188.

16. Z. 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.
17. A.Gagnidze, M.Iavich, G. Iashvili, Advantages and challenges of QRNG integration into Merkle, Scientific and Practical Cyber Security Journal (SPCSJ) 4(1):93-102, 2020
18. Shrimpton T., Terashima R.S. (2015) A Provable-Security Analysis of Intel's Secure Key RNG. In: Oswald E., Fischlin M. (eds) Advances in Cryptology -- EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science, vol 9056. Springer, Berlin, Heidelberg.
19. Gnatyuk S., Okhrimenko T., Iavich M., Berdibayev R. Intruder control mode simulation of deterministic quantum cryptography protocol for depolarized quantum channel, Proceedings of 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019, Kyiv, Ukraine, October 8-11, 2019, pp. 825-828.
20. 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.
21. 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.
22. Lunghi, Tommaso, et al. "Self-testing quantum random number generator." Physical review letters 114.15 (2015): 150501.
23. Bowles, J., Quintino, M. T., & Brunner, N. (2014). Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. Physical review letters, 112(14), 140407.
24. Pironio, S., Acín, A., Massar, S., de La Giroday, A. B., Matsukevich, D. N., Maunz, P., ... & Monroe, C. (2010). Random numbers certified by Bell's theorem. Nature, 464(7291), 1021-1024.

Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 64-72 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

# RADIOWAVE PROPAGATION MODELS FOR VHF AND UHF BAND

**Ajit Singh Department of Computer Science Patna Women's College, INDIA**

**ABSTRACT :** Radiowave propagation model is an empirical mathematical formulation for characterization of radiowave propagation as a function of frequency, distance and other conditions. This study explains the various attenuating factors prevalent in radiowave propagation. It highlights the various types of radiowave propagation; its classification based on their propagation paths; its layers in the atmosphere, its frequency bands and propagation mechanism. The study also entails the various radiowave propagation models and their application in VHF and UHF band.

**KEYWORDS:** *Radiowave Propagation Models, VHF Band, UHF Band, Attenuating Factors, Radiowave Propagation.*

## 1. Introduction

Radiowave Propagation is the transfer of energy by electromagnetic radiation at radio frequencies from one point, a transmitter to another, a receiver. Radiowave Propagation comprises of two types: The Guided and Free (unguided). Free (unguided) Radiowave Propagation occurs between corresponding antennas in the earth's atmosphere, underwater or in free space while the Guided Radiowave Propagation takes place in manmade guiding systems such as wirelines, coaxial cables, waveguides and optical fibers [1]. VHF and UHF bands belong to the free (unguided) as opposed to the guided. VHF and UHF bands are seen as the "line of sight transmission" on account of their app. VHF is defined as the portion of the radio spectrum from approximately 30MHz to 300MHz while UHF band is the portion of radio spectrum from 300MHz to 3GHz [2].

### 1.1 Classification of Radiowave Based on their Propagating Paths

There exists four major propagating paths of radiowave namely surface wave, space wave, tropospheric and ionospheric [3].

Surface wave. Propagates in direct contact with the earth's surface and as a result suffers severe "frequency-dependent attenuation" occasioned by absorption into the ground, "space waves on account of their being radiated from an antenna with many wavelengths above the surface are far from being attenuated as no part of it is in contact with the surface of the earth. It is, however, worthy of note that the propagation modes of both the VHF and UHF bands are exclusively tied to space wave."

Space wave. Space wave as shown in figure 1 comprises two components "direct" and "reflected" and albeit it is grouped together with "surface wave" as "ground wave", their varied propagation characteristics warrant their being considered exclusively.

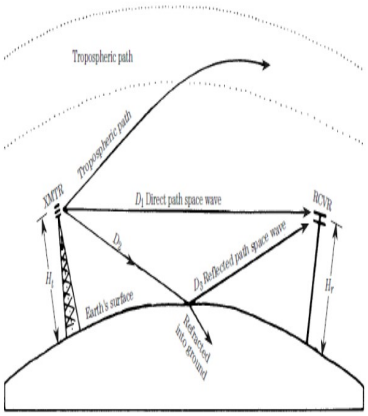


Fig. 1 Showing Space Wave Propagation [3]

Ionospheric. Ionospheric propagation is dependent on the ionization of the earth's atmosphere as a result of its being impacted upon by intervening factors such as ultra-violet radiation from the sun and cosmic rays. Ionospheric path is important to medium wave and HF Propagation but it is insignificant for VHF, UHF or microwave propagation. This phenomenon predisposes variation in electron density between day and night conditions with peaks in electron clarity that are in tandem with the height at which the evolved gases settle within the region of the upper atmosphere.

**1.2 Classification of Layers in the Atomsphere Layers in the upper atmosphere are classified into:**

C layer

D layer

E layer

summarized their localized frequencies and heights in order of magnitude comparison as shown in Table 1:

Table 1 Showing the Virtual Height, Critical Frequency and Maximum Single-Hop Range of the Ionospheric Layers

| IONOSPHERIC LAYERS | VIRTUAL HEIGHT | CRITICAL FREQUENCY | MAXIMUM SINGLE-HOP RANGE |
|---|---|---|---|
| | | | |
| C and D layers | 60-80km | Reflects low and very low frequencies | |
| | | | |
| E layer | 110km | 4MHz | 2350km |
| | | | |
| 1 layer | 180km | 5MHz | 3000km |
| | | | |
| 2 layer | 300km(day-time) and 350km(night time) | 8MHz(day time) and 6MHz(night time) | 3840km(day time and-4130km(night time) |

The study describes propagation of SURFACE WAVE as following the curvature of the earth due to refraction and categorizes it (Surface Wave) as being of importance at frequencies below about 2MHz with the conductivity and permittivity of the earth surface playing an important role in its propagation. This is due largely to the fact that it could introduce both displacement and conduction currents in the surface.

The study further states that at the highest frequency, these currents may penetrate depths ranging from about 1m to ten of meters at the lowest.

Attenuation thus occurs as the radio wave passes over the earth surface, even in an increased dimension as the frequency increases. Hence, the limitation of the usefulness of the SURFACE WAVE to frequencies below about 2MHz.

The study equally states that the DIRECT WAVE and the GROUND REFLECTED WAVE(both of which comprise the SPACE WAVE) are at low enough frequencies( where transmitting antenna height above ground, in terms of wavelength, is small) capable of cancelling out each other; with the corollary of leaving only the SURFACE WAVE.

Nevertheless, at higher frequencies, the height of the antenna may be such that makes the SPACE WAVE comparable in magnitude to the SURFACE WAVE, which results in the PHASOR SUM. The resultant wave in this instance is referred to as the GROUND WAVE, which should not in any way be confused as SURFACE WAVE alone.

**1.3 Classification of Radiowave Based on Frequency Bands sees radiowaves as being classified either by frequency bands or by propagation mechanisms nced Researches and Engineering Journal 05(02): 000-000, 2021**

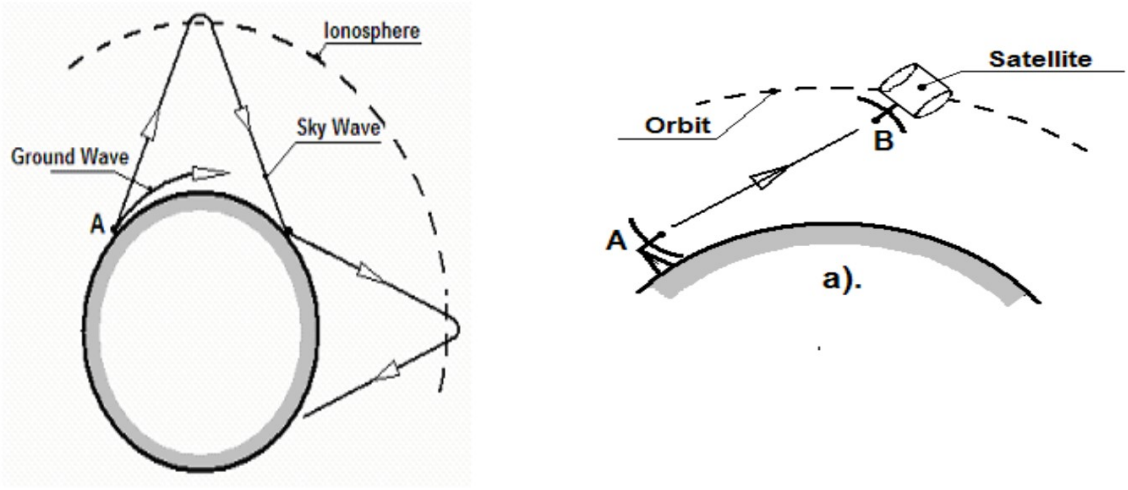



Fig.2 Showing Sky Wave Propagation [1]

“ground waves” as radio waves that propagate from a source in the vicinity of the surface of the earth as opposed to having its propagating path in the ionosphere. The study also sees two ground wave modes: “surface waves” and “space waves” as existing independently. This varies slightly from the position of [2] which sees “ground waves” as consisting of “surface waves”, “direct waves”

and “ground-reflected waves”. While highlighting “ground waves” and “sky waves” as those based on spatial area, [1] outlines four radio waveforms as falling into the category of THOSE EVOLVING UNDER THE

**MECHANISM BETWEEN THE TRANSMITTING AND RECEIVING ANTENNAS. They are:**

- Direct radio waves( or simply direct waves)
- Reflected radio waves(or reflected waves)
- Scattered(or secondary) radio waves
- Diffracted radio waves (or simply diffracted waves).
- Reflected Radio Waves. Reflected radio waves are those waves that travel to the receiving point via a reflection from an object, which has large dimensions compared to the wavelength [1, 5]. Occasioned by impedances between the air and the encountered object, a part of the energy is reflected whilst the

remaining part is refracted into the other medium. Figure 4 shows an ideal representation of this occurrence.

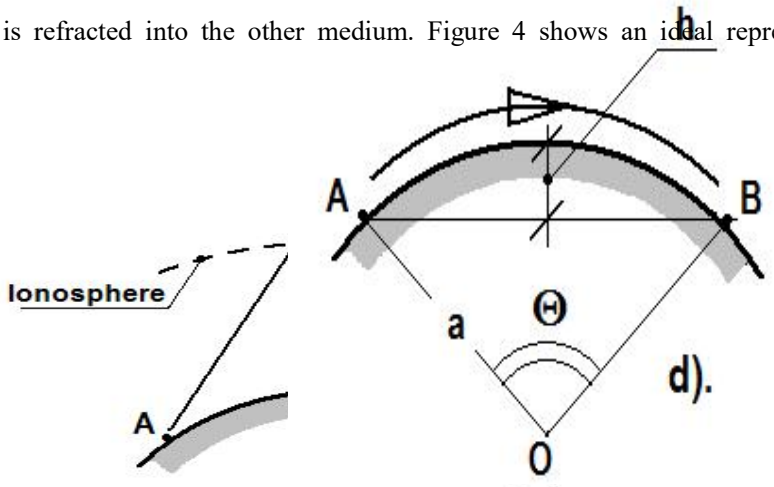



Fig. 4 showing a reflected radio wave [1]

A Scattered (Or Secondary) Radio wave. Scattered (or secondary) radio waves is referred as scattering, which it construes as related to reflection and could be referred to as diffuse reflection [6]. Its occurrence causes the energy of the radio wave to be distributed in all directions. According to [1], the phenomenon of scatter propagation through the irregularities of the ionosphere is peculiar to the VHF frequency band as shown in Figure 5.

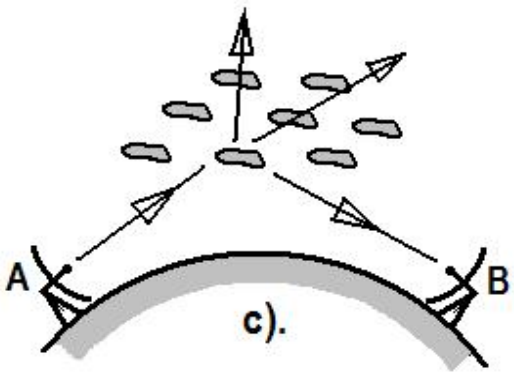



Fig. 5 Showing Scattered Radio Waves [1]

**Diffracted Radio Waves (Or Diffracted Waves).**

Diffracted radio waves is defined as electromagnetic wave that has been modified by an obstacle or spatial inhomogeneity in the medium by means other than a reflection or refraction [1]. [5] concurs with this assertion when it sees the phenomenon as occurring when the obstructing object is large compared to the wavelength of the radio wave. [1] sees it as occurring when $h \leq \lambda$ as shown in figure 6.

Fig 6 Showing Diffracted Radio Waves [1]

**2. Dynamics of Attenuating Factors prevalent in Radiowave Propagation**

Several attenuating factors are prevalent in radiowave propagation namely: Shadowing Effects, Multipath distortion, Picket Fencing, Path loss, Diffraction, Multipath Spread, Noise and Interference.

Shadowing Effect. "Shadowing" is the loss of field strength typically contributed to a diffracted wave emanating from an obstacle between transmitter antenna and receiver antenna [7, 8]. VHF and UHF waves exhibit a tendency of being attenuated with every rule of distance

This is just as ridges and hills could form shadows of VHF and UHF waves. The study, however, gave an exception concerning sharp ridges or other kinds of abrupt barriers usually caused by diffraction.

Multipath Distortion. Multipath distortion has to do with a situation where VHF and UHF waves are reflected off of dense surfaces like rocks or conductive earth, just like a beam of light can be reflected of a wall or a ceiling [2]. It sometimes occurs with several paths between a transmitting and receiving antenna as evinced in Figure 7.

In much the same vein, [3] outlines four major propagation paths: "surface wave", "space wave", "tropospheric" and "ionospheric." While the study sees the ionospheric path as important to medium-wave (MW) and HF propagation, it sees it as insignificant for VHF, UHF or microwave propagation.

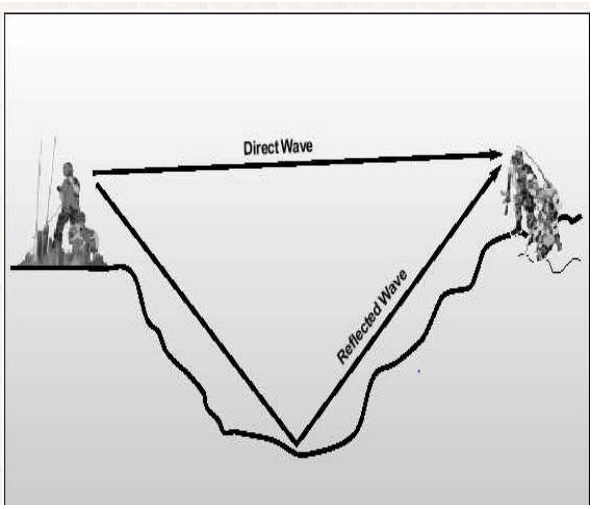



Fig. 7: Showing wave reflections caused by multipath distortion [2]

Figure 7 shows a direct LOS path between two radios that is inclusive of a reflected path from the bottom of a valley between them. The two paths are of different length with the direct path being the shorter of the two. And since radio waves travel at a constant velocity, the direct path wave arrives at the receiver before the reflected path. Thus, the same broadcast information reaches the receiver at two different times. It is much like echoes in an acoustically poor room. It is hard to understand what is being said if the echoes are close enough to each other.

Picket Fencing. Picket fencing is a form of multipathing that is common to vehicular mounted radios [2]. Its occurrence is usually associated with interference or reflections of signals from man-made objects such as buildings, houses, and other structures. Picket fencing is prevalent with VHF and UHF.

Path Loss. Path loss is the loss in power density experienced by a wave as it traverses the path between the transmitter and the receiver [9]. It is also major component in the analysis and design of the link budget of a telecommunication system [10].

Diffraction. Diffraction is an exception to the rule where ridges and hills form shadows of VHF and UHF radio waves [2]. It occurs when VHF and UHF waves are subjected to having a portion of their waves bend around on reaching very sharp ridges and continue propagation as if a very low power radio was placed at the top of the ridge. Figure 8 shows VHF and UHF Diffraction.

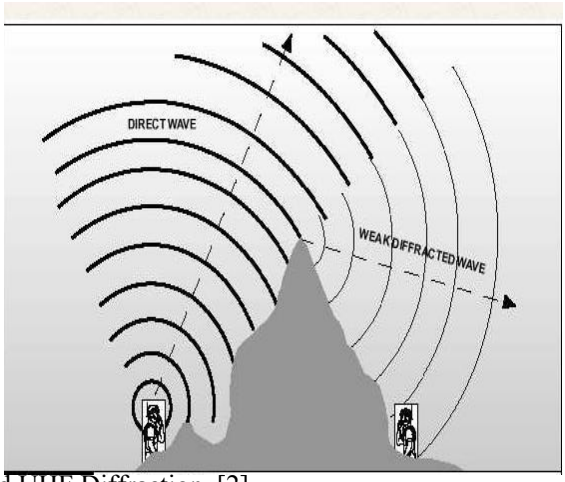



Fig. 8: Showing VHF and UHF Diffraction. [2]

Multipath Spread. Multipath spread is defined as the range of timed differences that it takes for radio signals to reach the receiving antenna when they arrive from several routes, which may include one or more sky wave paths and/or a ground-wave path [2]. This effect according to the study could be minimized by selecting a frequency that is as close as possible to the maximum usable frequency (MUF).

Noise and Interference. Receiver noise and interference comes from both external and internal sources [2]. While the internal noise originated from within the circuits of the receiver, other sources of noise within the radio that are of prominence are the power supplies and frequency synthesizers. External noise, however, comes from sources outside the radio and often exceeds internal receiver noise. The study went on to outline natural and man-made sources of noise and went on to highlight the VHF and UHF bands as being above atmospheric noise. Unintentional radio interference and intentional radio interference were also highlighted; with "collocation interference" as being typical of the former, while using "jamming" or deliberate interference as an example of the latter.

### 3. Radiowave Propagation Models

Radiowave propagation model is defined as an empirical mathematical formulation for characterization of radio wave propagation as a function of frequency, distance and other conditions [11, 12, 13 and 14].

It plays an important role in planning analysis and optimization of radio network. Hence, the imperative of developing effective propagation models for wireless communication systems. Radio Propagation models are not only used as mitigation measures, but used to predict the behavior of radio propagation in different environments. [15] categorized radio propagation models as falling into three categories, namely:

- Statistical Models
- Deterministic Models and
- Empirical Models.

3.1 Statistical Propagation Models. Their study outlines statistical propagation models as originally devised to provide estimations of signal field strengths (or signal power) in cases where there is insufficient knowledge of the terrain profile. Being models derived from data obtained from extensive measurements in different environments, they require a limited number of parameters (eg. effective antenna height, time and/or location variability, type of ground).

3.2 Deterministic (Geometrical) Propagation Models.

Their study outlines Deterministic models as making use of the laws governing electromagnetic wave propagation with a view to estimating the field strength(or signal power)directly from the path profile(which has to do with terrain and clutter between the transmitter and receiver). They are usually site specific and can be associated with indoor or outdoor propagation environments. Notable examples of it are the Fresnel model, Recommendation ITU-R P.525-2/526-4.

3.3 Empirical Propagation Models .Their study outlines Empirical path loss models as incorporating the benefits of deterministic and statistical models and is widely used for the planning and optimization of cellular networks. This model takes all environmental influences implicitly regardless of whether they could be separately recognized or not.

Their creation is hinged on fitting appropriate mathematical functions to extensive sets of measured path loss data with no due regard to base these functions on physical models of dominant propagation mechanisms. Wireless, Propagation and Network Engineers sees the simplicity and computational efficiency of this model as its main advantage.[16] and [17] sees the possibility of splitting empirical models into two subcategories namely, time dispersive and non-time dispersive; with the time dispersive models providing information about time dispersive characteristics of the channel such as delay spread of the channel during multipath. Examples of it are: Free space, Okumura-Hata, Cost 231, Ericsson propagation models, Recommendation ITU-RP. 1546, Okumura, Egli, ECC-33, SUI, Lee, Macro, COST-231-Walfisch-Ikeagami and Dual-slope, etc.

## REFERENCES:

1. Armoogum .V., Soyjaudah K.M.S., Mohamudally N., & Fogarty T., (2010). Propagation Models and Their Applications in Digital Television Broadcast Network
2. Design and Implementation. Trends in Telecommunications Technologies, pp 165-185.
3. Sauders S.R., (2005). Antenna and Propagation for Wireless Communication Systems. Wiley.
4. IEEE (2018). IEEE Standard Definitions of Terms for Radio Waves Propagation. IEEE Antenna and Propagation Society. New York, USA, IEEE Std 211
5. Biebuma J.J., & Omijeh B.O., (2013). Path loss Model Using Geographic Information System (GIS). International Journal of Engineering and Technology, vol. 3(3), pp 269-275.
6. Rick T., & Mathar R., (2007). Fast Edge Diffraction-Based Radiowave Propagation Model for Graphics

7. Hardware. Proceeding Of The 2nd IEEE International ITG Conference On Antenna (INICA), Munich, Germany.

8. Parmar K. J., & Nimavat V.D., (2015). Comparative Analysis of Path Loss Propagation Models on Radio Communication. International Journal of Innovative Research of Computer and Communication Engineering, vol. 3(2), pp 840-844.

9. Bolli .S., & Khan M.Z.A., (2015). A Novel LMMSE Based Optimized Perez-Vega Zamanillo Propagation Path Loss Model In VHF/UHF Bands For India. Progress in Electromagnetic Research, vol. 63, pp 17-33.

10. Popoola J.J., & Adesanya A.T., (2018). A Versatile Wave Propagation Model for Very High Frequency Broadcasting Band in Vegetation and/or Rocky Environment. International Journal of Engineering Science and Application, vol. 2(1), pp 18-26.

11. Temaneh- Nyah C., & Nepembe J.,(2014). Determination of a Suitable Correction Factor to a Radio Propagation Model for Cellular Wireless Network Analysis. Fifth International Conference on Intelligent

12. Systems, Modelling and Simulation, IEEE Computer Society, pp 175-182.

13. Anderson H.R., (2003). Fixed Broadband Wireless System Design: The Creation Of Global Mobile Communication, John Wiley & Sons, Inc., New York, NY.

14. Sharma P.K & Singh R.K., (2010). Comparative Analysis of Propagation Path Loss Models with Field Measured Oata, International Journal of Engineering, Science and Technology, vol. 2(6), pp 2008-2013.

15. Poonle A.A., & Owolabi O.J., (2019). Path Loss Modelling Of UHF Radio Wave Propagation in Ado-Ekiti, Nigeria. ABUAD Journal of Engineering Research and Development (AJERD), vol. 2(1), pp 90-102.

16. Ogbulezie J.C., Akonjom N.A., Ojomu S.A., Ezugwu A.O., & Igajah I.E., (2016). A Review of Path Loss Models for Uhfradiowaves Propagation: Trends and Assessment. International Journal of Research in Engineering and Science, vol 4(7), pp 67-75.

17. Sati G., & Singh S., (2014). A Review on Outdoor Propagation Models in Radio Communication. International Journal of Computer Engineering & Science, vol. 4(2), pp 64-68.

18. Garah. M., Djouane .L., Oudira .H., & Hamdiken .N., (2016). Indonesian Journal of Electrical Engineering and Computer Science. vol. 3(1), pp 126-135.

19. [22]Mardeni .R, & Kwan K.F., (2010). Optimization of Hata Propagation Prediction Model in Suburban Area in Malaysia. Progress in Electromagnetic Research C, vol. 13, pp 91-106.

20. Ebhota C.V., Isabona J., & Srivastava V.M., (2018). Base Line Knowledge on Propagation Modelling and Prediction Techniques in Wireless Communication Networks. Journal of Engineering and Applied Sciences, vol. 13(7), pp 1919-1934.

21. Nazmat T.S.B., Nasir. F., Segun I.P., Muhammed A.S., Abdulkarim A.O., & Carlos T.C., (2018). Path Loss Predictions For Multi-Transmitter Radio Propagation In VHF Bands Using Adaptive Neuro-Fuzzy Interference System. Engineering Science and Technology, an International Journal, Elsevier, pp 679-691.

22. Milanovic .J., Rimac-Drlje S., & Mayerski .I., (2010). Radio Wave Propagation Mechanisms And Empirical Models For Fixed Wireless Access Systems, Technical Gazette, pp 43-52.

23. Sarkar T.K., Zhong J., Kim K., Medouri A., & Salazar-Palma M., (2003). A Study of Various Propagation Models for Mobile Communication, IEEE Antennas and Propagation Magazine, vol. 45(3), pp 51-82.

24. Rappapot T.S.,(2002). Wireless Communication Principles and Practice, 2nd Edition, New York. Pearson Education.

**Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 73-76 ISSN 2587-4667**
**Scientific Cyber Security Association (SCSA)**

**УДК 004.056.5(075.8).**

# ПРОБЛЕМА ОБЩЕГО АНАЛИЗА ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

# THE PROBLEM OF GENERAL ANALYSIS OF INFORMATION PROTECTION IN THE INFORMATION SYSTEM

**Д. Басшықызы, старший преподаватель, НАО Каспийский университет технологий и инжиниринга им. Ш. Есенова, г Актау, Казахстан**
**D. Bashygyzy, Senior Lector, NAO Caspian University of Technology and Engineering named after Sh. Yessenova, Aktau, Kazakhstan**

**АННОТАЦИЯ.** Все программы защищены от несанкционированного копирования, если в ней выполняется копия программы, позволяющая проверить саму программу, с целью определить, создана ли она с соблюдением всех необходимых технологий. Программа не может нормально работать, если нарушена технология создания копий. Таким образом, юридическое копирование приводит к использованию некоторой уникальной технологии создания копий. Любая копия или внутренний файл защищенной программы должен иметь «ключ " - один или несколько кодовых цифр. При проверке программа сравнивает ряд специфических признаков рабочей среды с предварительно закодированным ключом и по результатам сравнения формирует соответствующий знак. Таким образом, создание копии программы минимально: эта копия должна предоставить ключ, готовый к работе с реальным компьютером, чтобы быть работоспособной.

**КЛЮЧЕВЫЕ СЛОВА:** *информационная система, файл, программа, компонент, персонал*

**ABSTRACT**: All programs are protected from unauthorized copying if a copy of the program is executed in it, which allows you to check the program itself in order to determine whether it was created in compliance with all the necessary technologies. The program cannot work normally if the copying technology is violated. Thus, legal copying involves some unique copying technology. Any copy or internal file of a protected program must have a "key" - one or several code digits. When checking, the program compares a number of specific features of the working environment with a pre-encoded key and, based on the results of the comparison, forms the corresponding sign. Thus, the creation of a copy of the program is minimal: this copy must provide a dongle ready to work with a real computer in order to be functional.

**KEYWORDS:** *information system, file, program, component, personal*

Стандарт информационной безопасности создает основу для взаимодействия между производителями, потребителями и экспертами по квалификации продукции информационных технологий.

Важнейшие стандарты информационной безопасности (в хронологическом порядке): «критерии безопасности компьютерных систем Министерства обороны США (оранжевая книга. 1983)», «европейские критерии безопасности информационных технологий», «федеральные критерии безопасности информационных технологий США», "критерии единства безопасности информационных технологий".

Какими специфическими признаками может обладать компьютер, на котором работает программа, а именно программно - аппаратная среда.

Для IBM – совместимых ПК этими признаками могут быть:

1. тип ПК и тип операционной системы (версия);
2. Дата выхода и /или его контрольное соединение;

3. физическое место месяцев на дисковом носителе;
4. аппаратный состав;
5. наличие скрытых частей программы;
6. физические особенности носителя (в т. ч. дефекты).

Некоторые из этих признаков очень индивидуальны (например, физические особенности некачественного носителя), другие менее индивидуальны (тип ПК, версия друга). Программа может использовать один или несколько символов, чтобы проверить законность копии. Особое значение в этом случае имеет способ применения программы: если программа рассчитана на работу на конкретном ПК, выбираются одни метки, если она легко перемещается с одного компьютера на другой без потери работоспособности - выбираются другие. Назовем программы первого типа-стационарными, а второго - мобильными.

Во всех случаях проверка законности не должна влиять на быстрое действие программы или требовать от пользователя каких-либо дополнительных действий (например, может ли система, использующая пароль, считаться эффективной). Система защиты должна проверять копию, а не пользователя.

Эти проверки довольно просты, но не имеют высокой степени индивидуальности в том смысле, что могут быть сотни тысяч ПК одного типа, использующих одну и ту же ОС. Поэтому обычно эти проверки используются в сочетании с проверкой других отдельных симптомов и предназначены для защиты стационарных программ.

Тип ПК жазылған f0000: жазылған fffe записан в КОС по адресу,т. е. в байтах перед последним в мегабайтном адресном пространстве ПК. Значения этого байта могут быть следующими кодами (табл.1).

Таблица 2. Коды значений байта

| Код | Тип БД |
|---|---|
| FF | PC |
| FE | XT |
| FD | PCjr |
| FC | AT |

Проверка сроков выхода и контрольной суммы фур. Постоянное запоминающее устройство (пси) является неделимой составной частью любого IBM, объединенного с ПК. Состав НПС учитывает особенности реализации конкретных ПК и может отличаться от компьютеров каждого типа.

При этом в конце фур (по адресу$F000:$FFFS) обычно записывается срок ее выхода, поэтому даже для однотипных ПК (даже при наличии одной фирмы - изготовителя) контрольная сумма фур отличается на разных экземплярах ПК.

Дата выхода НПС находится по адресу SFOOO: $FFF5 и состоит из 8 смешанных байтов. Данные хранятся символически в формате MM/DD/YY (MM – символы номера месяца, DD – номер даты, YY –номер года), например «26.06.92». Эта проверка используется для защиты стационарных программ.

Хорошей индивидуальностью обладает физический номер кластера, который начинается на жестком диске с файлом с защищенной программой. Действительно, в аппаратно-программной среде ПК что-то другое (кроме состава оперативной памяти) динамично меняется, как и файловая структура жесткого диска. При создании легальной копии исходный номер кластера для файловой программы на жестком диске в общем случае будет случайным. Если при отправке программа проверит этот номер,то в большинстве случаев она легко обнаружит незаконное копирование.

Такой способ защиты нельзя считать идеальным по многим причинам. Проверка номера кластера выполняется не так просто, как проверка даты выхода и типа ПК. Но первоначальный недостаток заключается в другом: любое изменение места файла в пределах хотя бы одного каталога приводит к незаконности ранее установленной копии.

Программа может проверить эффективный объем оперативной памяти, наличие и объем расширенной памяти, тип центрального процессора и приблизительную скорость его работы, наличие математического сопроцессора, тип и количество дисководов для гибких дисков, параметры физического жесткого диска, количество логических дисков, тип и количество каналов для подключения внешних устройств. Каждая из этих характеристик может повторяться на тысячах других ПК, но все они достаточно индивидуальны в комплексе и поэтому могут с большим успехом использоваться для защиты стационарных программ [1].

Некоторые зарубежные фирмы выпускают электронные ключи для защиты мобильных приложений - несколько более дешевых устройств, которые подключаются к стандартному каналу последовательного или параллельного ввода – вывода перед отправкой защищаемого приложения. Электронные ключи реализуются на основе заказанных микросхем и осуществляют взаимодействие с защищенной программой в необходимом интерфейсе.

Для компьютеров класса IBM AT используется специальная энергоемкая КМОП - память, которая хранит полезную информацию о составе аппаратных средств ПК, в том числе – эффективную память. Информацию о периферийных устройствах формирует Equipm в КМОП-памяти.

Наиболее эффективным способом защиты (в основном для мобильных приложений) является создание и использование скрытых частей программы и/или особенности физических носителей информации.

Скрытые части программы-это область носителя диска, которая тем или иным способом связана с программой, но не записана в виде файлов ОС. В подавляющем большинстве случаев в программе нет необходимости искусственно создавать такие территории, так как они будут«за» любым файлом.

Не очень эффективный способ защиты заключается в создании и использовании дополнительных скрытых кластеров. Такие кластеры могут быть помечены как неверные или «потерянные» в FAT (т. е. не соответствующие ни одному зарегистрированному файлу). (Во всех случаях, независимо от того, находится ли ключ за файлом или в отдельном кластере, защита может быть легко нейтрализована, если копирование дискета «из блока в блок " используется с помощью системной утилиты DISKCOPY или аналогичных несистемных программ).

Лучшей способностью противостоять незаконному копированию обладает система защиты, основанная на учете индивидуализированных особенностей, прежде всего дискет в анализе неустранимых дефектов. В этом случае система проверки защиты «знает» список дефектных секторов оригинальной дискеты и пытается их отформатировать. Если после форматирования обмен информацией с сектором прошел правильно, то соответствующий сектор - без дефекта и, следовательно, мы намерены работать с нелегальной копией дискеты. Главное достижение этого способа защиты приводит к принципиальной невозможности создания дефекта, который не устраняется программными средствами на правильной дискете.

Как видно из опыта, часть дискет (не менее 1%) состоит из заводских выходных дефектов, поэтому при большом выпуске коммерческих программ такие дефекты приходится создавать искусственно. Для этого иногда используют лазеры, а чаще – обычную булавку. После нескольких упражнений вы можете оставить царапину на слое носителя, когда угодно, или вы можете перевернуть дискету, чтобы сохранить работоспособность большей ее части. Но царапины и вмятины поверхности дискеты могут повредить головки некоторых носителей.

Под информационной безопасностью понимается поддержание инфраструктуры под случайным или предопределенным воздействием естественного или искусственного характера, грубо ущемляющего защиту информации и субъектов информационных отношений, в том числе владельца и пользователей информации, и поддержка инфраструктуры [2].

1. типичные атаки на операционные системы

Угроза-это потенциальная возможность реального нарушения информационной безопасности. Попытка осуществить угрозу называется нападением, а такого стремящегося – злоумышленником. Социальных злоумышленников называют источником угрозы.

Прежде всего, угроза исходит из-за наличия уязвимого места в защите информационных систем (например, возможность доступа посторонних лиц к крайне необходимому оборудованию или ошибке в программном обеспечении).

Типичные атаки:

1. сканирование файловой системы: злоумышленник сканирует файловую систему компьютера и пытается прочитать (или скопировать, или стереть) все файлы подряд.

2. Кража ключевой информации: в простейшем случае-злоумышленник видит пароль, набранный пользователем.

3. выбор пароля.

4.сбор мусора: во многих операционных системах информация, удаленная пользователем, физически не удаляется, помечается как удаленная. С помощью специальных программных средств эта информация (мусор) может быть впоследствии восстановлена. Сбор мусора может осуществляться не только на дисках, но и в оперативной памяти.

5. повышение полномочий: для реализации данной угрозы злоумышленник, используя ошибки в программном обеспечении операционной системы либо/или политике безопасности, получает больше полномочий, чем ему было предоставлено в соответствии с политикой безопасности. Обычно это происходит либо путем запуска программы от имени другого пользователя, либо переключением динамически загружаемой библиотеки. Эта угроза представляет большую опасность для операционных систем (UNIX), которые позволяют временно увеличить полномочия пользователя.

6. программный. В качестве средств вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (как правило - полоса пропускания сетей, вычислительные возможности процессоров и оперативной памяти). По расположению источника угрозы такое потребление подразделяется на локальное и отключенное. При сбое в конфигурации системы локальная программа монополизирует процессор или/или физическую память, снижая скорость выполнения других программ до нуля.

Одним из опасных способов атаки является проникновение вредоносного программного обеспечения в атакующую систему.

7.исключение штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы [3-5].

Защищенными называют ОС, рассматривающие средства защиты от основных классов угроз. Защищенная ОС обязательно должна содержать средства ограничения доступа пользователя к своим ресурсам, а также средства проверки подлинности пользователя, начиная работу с ОС. Кроме того, защищенная ОС должна содержать средства противодействия случайному или непреднамеренному выходу ОС из строя.

## ЛИТЕРАТУРА

1. Айтхожаева Е.Ж., И Син Фу Е.В. Язык программирования баз данных xBase. /Методические указания к лабораторным работам по дисциплинам «Системы баз данных», «Базы данных». / - Алматы: КазНТУ, 2006.
2. Айтхожаева Е.Ж., И Син Фу Е.В. Визуальное проектирование компонентов систем баз данных. /Методические указания к лабораторным работам по дисциплинам «Системы баз данных», «Базы данных». / - Алматы: КазНТУ, 2004.
3. Айтхожаева Е.Ж., Дрогнова Н.Ф., И Син Фу Е.В. Разработка приложений баз данных. /Методические указания к курсовой работе/ - Алматы: КазНТУ, 2005.
4. Sergiy Gnatyuk , Maksim Iavich , Giorgi Iashvili , Andriy Fesenko ENSURING EUROPEAN CIVIL AVIATION CYBERSECURITY, Scientific and practical cyber security journal, 2019
5. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019