SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL4 No4
DECEMBER 2020

ISSN 2587-4667

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

INFORMATION SECURITY ANALYSIS ALGORITHM IN CLOUD TECHNOLOGY

Jafarova Shalala Mehdi kizi, Ph.D
Sumgayit State University

ABSTRACT. There are different approaches to information security modeling in cloud technology. Unlike other modeling devices, the Petri network (PN) is a more universal device. This is justified by the fact that the information used is modeled by the PN and an assessment of security is made by analyzing the main properties of the PN outside the system.

KEYWORDS*: Security, server, browser, cloud service, provider, Petri network*

INTRODUCTİON

Here, processing technology, algebraic PN's are used to analyze the storage and protection of information. The main difference between the algebraic PN and the ordinary PN [4,5] is that it has the ability to perform full-value addition, subtraction, multiplication and residual division operations. The availability of these capabilities allows the ability to model the dynamic, discrete processes of the network to be compared with the first-order predicates of symbol logic. The practical advantages of such models make it possible to model multivariate polynomials and tabular functions.

The main advantage of algebraic PN and its various extensions is that it has more opportunities in the field of research and modeling of parallel processes. Given the formation of algebraic PS on the basis of closed categories with special properties, it is used in the synthesis of classical analysis and comparison methods of algebraic network systems as a mathematical modeling apparatus. This advantage allows the results of the modeling process to be widely applied in practice.

Fuzzy algebra PN is defined by the following five [1,2,3]:

$$N=(P \cup F, T, A, V, \mu_0{}^R),$$

here, $P=\{p_1,p_2,\ldots,p_n\}$ is a finite set of positions of type p; $F=\{f_1,f_2,\ldots,f_m\}$ - is a finite set of positions of type *f*; $T=\{t_1,t_2,\ldots,t_r\}$ is the finite set of transitions; *A*- finite alphabet*; V:[(P ∪ F)×T] ∪[T×(P ∪F)]→A**- is a description of the marked arcs that connect the positions with the links and the links with the positions; $\mu_0{}^R{:}P\cup F \to A^* \times [0,1]^{\ell}$ - A^* - is the initial marking of the positions of the words, A^* - *A* is a free monoid; ℓ*=card X^f (a), a∈P ∪F.*

Fuzzy algebra of PN the initial marking for each position is described by the following procession:

$$\mu_0^R(a)=\langle x_1x_2\ldots x_k, R(x_1)R(x_2)\ldots R(x_k)\rangle.$$

Fuzzy algebra in PN the permissibility of the passages is analogous to the rules of the algebraic PN and is determined by the first element of the procession. μ^R *(a)* Development of a t- transitions , which is allowed for marking $\mu_1^R(a)$ the first element of the procession is the algebra, which is analogous to the PN. The second element of the procession is calculated by the following formula:

$$R=(V(t,a))=min\{R(V(y,t))\,|\,y\in G^+(t)\},\quad a\in P\cup F$$

The activity of information security in cloud technology in accordance with the automation scheme is as follows:

To use the system, an authorized user obtains access by entering the password he has entered correctly. With the help of PN positions and links, it is possible to determine whether the user entered

this password correctly or not. When the system starts, the condition is checked, and if the password is entered by a real user, the system is opened for use. If the password is entered incorrectly, then the system is compromised by a malicious person. In this case, there will be no connection to the system and the system will not be opened for that malicious user. In this sequence, an automated system for modeling information security in cloud technology using fuzzy algebraic PN is created.

The operation and analysis algorithm of the fuzzy algebra PN is as follows:

1. The beginning of the algorithm

2. Plenty of links $(m+n)\times r$ dimensional $G^-=[(F\cup P)\times T]$ creation of input incident matrix:

$$g_{ji}^- = \begin{cases} s, & \text{if to } j \text{ is } i \text{ there is an arrow directed to the transition} \\ \varepsilon, & \text{else} \end{cases}$$

there, $i=\overline{1,r}$, $j=1,m+n.$ $j=1,m$ when, f arcs of type position, $j=m+1,\overline{m+n}$ when, p the arcs of the type position are expressed.

3. Plenty of links $r\times(m+n)$ dimensional $G^+=[T\times(F\cup P)]$ creation of output incident matrix:

$$g_{ji}^+ = \begin{cases} s, & \text{if to } j \text{ is } i \text{ there is an arrow directed to the transition} \\ \varepsilon, & \text{else} \end{cases}$$

here, $i=\overline{1,r}$, $j=\overline{1,m+n}.$ $j=\overline{1,m}$ while, f arcs of type position, $j=\overline{m+1,m+n}$ while, p the arcs of the type position are expressed.

4. The distribution function of the set of transitions $r\times(m+n)$ dimensional W^- creation of input membership matrix:

$$W_{ji}^- = \begin{cases} W(s), & \text{if to } j \text{ is } i \text{ there is an arrow directed to the transition} \\ 0, & \text{else} \end{cases}$$

here, $i=\overline{1,r}$, $j=\overline{1,m+n}$, $W(s) \in [0,1]$.

5. $1\times(m+n)$ ölçülü μ creation of initial marking:

$$\mu_j = \begin{cases} s, & \text{if the position is marked s word} \\ \varepsilon, & \text{if the position is not marked} \end{cases}$$

here, $j=\overline{1,m+n}$. $\mu_j(j=\overline{1,m})$ elements determine the positioning of the f-type position, $\mu_j(j=\overline{m+1,m+n})$ the elements determine the p-position positioning.

6. Creation of the matrix of the degree of belonging of the distribution function of the initial marker:

$$e_j = \begin{cases} W(\mu_j), & \text{if } j\text{- position is marked} \\ 0, & \text{if } j\text{- position is not marked} \end{cases}$$

here, $j=\overline{1,m+n;}$ $W(\mu_j)\in[0,1]$.

7. Search for a permitted passage. Every $t_i(i=\overline{1,r})$ the processing condition for the transition is checked:

a) G^- all input positions of the t_i transition from the input matrix are assigned. All $g_{ji}^- \neq \varepsilon(j=1,m)$, for is g_{ji}^- to is μ_j the presence of a left striker is conditionally checked:

$n_1 = card(g_{ji}^-)$ the length of the elements is calculated and from the first position of the elements of μ_j marking $p=copy(\mu_j, 1, n_1)$ the word is selected. If $p \neq g_{ji}^-$, to index i unit increases $i=i+1$ and the transition to the item is made 7.b.

b) All $g_{ji}^- \neq \varepsilon (j = \overline{m+1, m+n})$ a mirror word is compiled for: $\tilde{\mu}_j = \varepsilon$ və $n_1 = card(\mu_j)$, $\tilde{\mu}_j = \tilde{\mu}_j \circ copy(\mu_j, k, 1), \ k = \overline{n_1, 1}$ characters are moved according to the formula;

c) $g_{ji}^-, (j = \overline{m+1, m+n})$ in the mirror is checked to see if the word is left-handed: is $n_1 = card(g_{ji}^-)$ to $\tilde{\mu}_j$ from the first position of the word mirrored $p=copy(\mu_j, 1, n_1)$ the word is selected. If $p \neq g_{ji}^-$, to i index $i=i+1$ unit increases.

8. If $i>r$ to a deadlock is reported, else the transition to the item is made 9.

9. The transition to the item is made 7.a.

10. Calculation of the elements of the new marking matrix:

$$\mu_j^{'} = \begin{cases} copy(\mu_j, n_1 + 1, m_1 - n_1) \circ g_{ij}^+, j = \overline{1, m}; \\ copy(\mu_j, 1, m_1 - n_1) \circ g_{ij}^+, j = \overline{m+1, m+n}, \end{cases}$$

here, $m_1 = card(\mu_j), n_1 = card(g_{ji}^-).$

11. New marking is accepted after the current marking: $\mu_j = \mu_j^{'}, (i = \overline{1, m+n})$

12. Creating a matrix of the degree of belonging of the distribution function of the new marker:

a) The distribution function of the set of transitions W^+ calculation of the elements of the output degree matrix:

$$W^+(i,k) = min\left[W^-(j,i)^{\ell}\right] \text{ all } W^-(j,i) \neq 0, \quad \text{here, } i = \overline{1,r}; k = \overline{1, m+n};$$

all $W^-(j,i) \neq 0$, here, $i = \overline{1,r}; k = \overline{1, m+n}$;

b)

$$e_j = \begin{cases} W^+(j,k), & \text{əgər } \mu_j \neq e, \\ 0, & \text{əgər } \mu_j = e; \end{cases} \qquad j = \overline{1, m+n}; \ell = card(\mu_n).$$

here,

13. The transition to the item is made 7. The process continues until the desired marker is obtained.

14. The end of the algorithm.

REFERENCES

1. Aalst W. The Application of Petri Nets to Workflow Management. // The Journal of Circuits, Systems and Computers,Vol. 8, No. 1,1998, p.21-66.

2. Akhmedov M.A., Mustafaev V.A., Huseynzade Sh.S. Presentation and analysis of fuzzy rules productions using a modiffed fuzzy Petri nets / The 5th International Conference on Control and optimization With Industrial applications. 27 - 29 Auqust 2015. pp.184-186.
3. Frank A. Using relation algebra for the analysis of Petri Nets in a CASE tool based approach ./ Software Engineering and Formal Methods, Proceedings of the Second International Conference, Dortmund Univ., Germany, 2002, p. 396 - 405.
4. Gillam, Lee. Cloud Computing: Principles, Systems and Applications / Nick Antonopoulos, Lee Gillam. — L.: Springer, 2010. — 379 p. — (Computer Communications and Networks). — ISBN 9781849962407
5. Mell, Peter and Grance, Timothy. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. NIST (20 October 2011)

Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 5-9 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

QUANTUM COMPUTER ATTACKS ON SYMMETRIC AND ASYMMETRIC CRYPTOSYSTEMS.

მაქსიმ იავიჩი - კავკასიის უნივერსიტეტი

Maksim Iavich – Caucasus University

გიორგი წიკლაური – ევროპული სკოლა

Giorgi Tsiklauri – European School

ნუგო ამონაშვილი - ვლადიმირ კომაროვის თბილისის ფიზიკა-მათემათიკის N199 საჯარო სკოლა

Nugo Amonashvili - Vladimir Komarov Tbilisi School of Physics and Mathematics N199

რატი ტაბიძე - ქალაქ თბილისის კერძო სკოლის ბრიტანიკა

Rati Tabidze – Private School of Tbilisi

ნიკა ფანქველაშვილი - ვლადიმირ კომაროვის თბილისის ფიზიკა-მათემათიკის N199 საჯარო სკოლა

Nika Panqvelashvili - Vladimir Komarov Tbilisi School of Physics and Mathematics N199

გიორგი კვერნაძე - 61 საჯარო სკოლა

Giorgi Kvernadze – 61st Public School

ABSTRACT: This article analyzes at how Symmetric and Asymmetric cryptosystems and how they can be broken with the usage of quantum computers. The article also delves into who this is truly a problem for and what can be done to curb it. The paper covers the Integer Factorization Problem, Discrete Logarithm Problem, Grover's Algorithm, and Shor's Algorithm.

KEYWORDS: *Qubit, Symmetric Encryption, Asymmetric Encryption, Public Key, Private Key.*

აბსტრაქტი: ეს სტატია აანალიზებს, თუ როგორ მუშაობს სიმეტრიული და ასიმეტრიული კრიპტოსისტემები და როგორ შეიძლება მათი გატეხვა კვანტური კომპიუტერის გამოყენებით. გარდა ამისა, ეს სტატია განიხილავს, თუ ვისთვის წარმოადგენს ეს საფრთხეს და რა ზომებია მისაღები საშიშროების ასაცილებლად. სტატიაში განხილულია მთელი რიცხვების ფაქტორიზაციის პრობლემა, დისკრეტული ლოგარითმის პრობლემა, გროვერის ალგორითმი და შორის ალგორითმი.

საკვანძო სიტყვები: *ქიუბიტი, სიმეტრიული დაშიფვრა, ასიმეტრიული დაშიფვრა, საჯარო გასაღები, კერძო გასაღები.*

INTRODUCTION

Quantum computers are devoloping fast, however with those advantages come potential threats, but just how big are those threats? We often hear of how Quantum Computers will be able to do amazing and terrifying things such as predict the future, model the universe, and break all the encryptions we know, but how much of that is true? In this article we will examine the last claim and to what extent we need to worry about it. While the claim does have some truth to it, it is also quite hyperbolic and not completely accurate, this is because while certain encryptions are quite succeptible to Quantum Computers and must be replaced, others are much more resistant and need little to no enhancement to take on Quantum threats.

SYMMETRIC AND ASYMMETRIC ENCRYPTION

Symmetric Encryption

One key which must be kept secret is shared between users in this method and is used for both encryption and decryption. Often used as the method for bulk encryption.

$E_K(M)=C$

$D_K(C)=M$

Where M is the message, C is the encrypted message, K is the key, and E and D the encryption and decryption algorithms, respectively, E and D must be inverse functions such that $E_k(D_k(x))=x$.

Pros:

1. It is much faster than Asymmetric encryption.

2. If a large key size is used it is extremely resistant to brute force attacks.

Cons -

1. Leaks information with each usage and thus keys must be cycled.

2. Can only be used for ensuring secrecy and not authenticity.

Examples of symmetric cryptography are DES, AES, RC5, RC6. DES was the most commonly used block cipher in the world in the early days of computers. It encrypts 64-bit data using a 56-bit key. But with the advancement of technology, this method has become vulnerable to attacks. So people have tried alternatives like AES. AES is faster and more powerful than DES.

However the main disadvantage of Symmetric cryptosystems is that the keys must be exchanged in a secure manner before it can be used, and if the keys are not yet held by both parties it is impossible to deliver the keys to each other in a secure manner thus another system for delivering the keys is required. This is where Asymmetric encryption comes in.

Asymmetric Encryption

Asymmetric encryption is also known as public key cryptography. With this method, two keys are utilized which each decrypt the other's encryption. The first is a public key known by everyone and the second a private key known only to one user. This method was developed to address two key

issues. How to share information securely without having to meet up in person to exchange keys, and how to verify that the information comes from the correct user.

There are two main areas of application of asymmetric cryptography:

1. Open key encryption - Only those who have a private key can decrypt text with open key encryption. That is, anyone can send secret information to the key holder. If there are N persons in the network, only N-1 key pairs are required to exchange information between them. Open keys are freely interchangeable or placed in a common database.

2. Digital Signature - Anyone can decrypt the text encrypted with a secret key, i.e. anyone can refer to a common database of public keys and make sure that this information was indeed encrypted, signed, by the sender.

Having an open key poses an additional problem, system users need to be sure that the open key really belongs to the owner and has not been altered. This is achieved by creating an open key infrastructure where one key holder (certificate issuer) confirms to others (by digital signature) that their keys are owned.

These two methods are often used together in the most common usage of Asymmetric encryption, sharing the private keys for the faster Symmetric encryption. How this works in practice is each user sends the other their public key, then the user with the Symmetric key sends the other the key encrypted twice, first with the recipient's public key, and then with their own private key, then the recipient uses their private key to decrypt it, ensuring secrecy, and then the sender's public key, ensuring the key is from the correct sender.

Asymmetric encryption commonly utilizes one of two mathematical problems: The Integer Factorization Problem, and The Discrete Logarithm Problem. The Integer Factorization problem deals with the fact that once you multiply two large prime numbers it is extremely difficult for classical computers to factor the multiple back into the two large numbers. The Discrete Logarithm Problem is that it is similarly difficult for clasical computers to find the discrete logarithm of a number in a multiplicative cyclic group.

QUANTUM COMPUTERS AND THEIR ATTACKS ON SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

Difference between Quantum and Classical Computers

A classical computer performs operations using bits whose values can be 0 or 1. As for the quantum computer, it uses quantum bits, also known as qubits. Various physical objects can be used as quantum bits (i.e. individual photons, electrons ...). Let us consider the case of an electron as a quantum bit. Every electron has its own magnetic field, hence the spin. Place the electron in the magnetic field. Define two positions, spin up and spin down (similar to 1 and 0), according to the directions between the electron magnetic field and the external magnetic field. The main advantage of the quantum bit lies in the following, it can be both 1 and 0 in the at the same time. This is called quantum superposition. When determining the

instantaneous value of a quantum bit, we assume a value of 0 or 1, although prior to measurement it exists in both 0 and 1 states with certain coefficients (i.e. 64% probability of spin up or 1 and 36% probability of spin down or 0).

Compare two classical and two quantum bits. With two bits we can get four different options (00, 01, 10, 11). Classic bits can take only one value from a given four variants, while two quantum bits are all four of them with certain coefficients (α-00, β-01, γ-10, δ-11). As a result, to determine the state of this two-spin system, we would need four numbers (coefficients), while two numbers are sufficient to describe a two-classical system. Which means that two quantum bits contain information equivalent to four classical bits. A quantum bit of N contains the equivalent information of a 2N classical bit.

Quantum Computer attacks on Cryptosystems

As we have already seen in some respects the power of a quantum computer is significantly greater than that of a classical computer. Consequently the risk of hacking some ciphers increases. Consider one of the most common occurrences of asymmetric cryptography, encryption using RSA. Its sustainability is based on the fact that the factoring of "large numbers" is very difficult. When we refer to large numbers we are not talking about hundreds, thousands, or millions. We are talking about a 2048-bit number, which is equivalent to a 617-digit number in decimal systems. If we find an easy way to factorize such a large number, RSA will be rendered ineffective. We can also try every possible case, but it takes a long time on a classic computer. Yet for a quantum computer it represents nothing. If we had a 4099 ideally stable quantum bit computer, it would break the RSA-2048 in 10 seconds! To be fair, it should be noted that the most powerful quantum computer has 72 quantum bits (Google Bristlecone) with an error probability of 0.6%. Nevertheless, quantum computing is evolving day by day and is becoming more and more of a threat to cryptography.

Symmetric cryptosystems are in much less danger from quantum computer attacks than their Asymmetric counterparts as the best algorithm to break them, Grover's Algorithm provides only a quadratic speedup, while this is significant common systems such as AES-128 can deal with this by doubling their key size, AES-256 is acceptably safe against quantum attacks.

Asymmetric Cryptosystems on the other hand are in much more danger, Shor's algorithm gives exponential improvement over classical methods for both the Integer Factorization, and Discrete Logarithm problems and even increasing key size by large factors has too little of an effect to keep these systems Quantum-Proof.

What can be done?

Experts estimate that quantum computers will be strong enough to break encryptions within one to two decades, thus if you have information which must remain secret for longer than ten years it is important to start encrypting data with Quantum-Proof algorithms, AES-256 is strong enough to stand against Quantum Computers, and has already stood the test of time against classical computers, and thus is a good choice in the Symmetric encryption department, but what about Asymmetric encryption? While there are no fully tested Asymmetric cryptosystems which can hold their own against Quantum Computers IBM's CRYSTALS looks promising, it uses a lattice based mathematical problem at it's core where numbers are taken from a pool and added together, while for smaller sets it may seem simple to figure out which numbers were added together for larger sets it's nearly impossible to do so in a viable amount of time by classical computers, and Quantum Computers provide no advantage for solving this problem. There are also other organisations such as NIST working on proving the efficacy of a Quantum-Proof system.

Conclusion

While Quantum Computers are a real threat against classical encryptions there are recourses to take such as increased key size for Symmetric encryption and new algorithms for Asymmetric encryption. Thus while it is a problem it is not a panic-worthy one and should be handled effectively, without dropping everything else to work solely on it as other reputable organisations such as NIST and IBM are already working on viable solutions.

REFERENCES:

1. S.Bushwick - New Encryption System Protects Data from Quantum Computers - Scientific American, 2019
2. J.Lake - What is RSA encryption and how does it work? , comparitech 2018
3. V.Timofeev/iStock, How Do Quantum Computers Work? sciencealert
4. M.Brinon J.Daubin C.Derland P.Boito A.Bostan A.Poteaux M. Safey El Din Journées Nationales de Calcul Formel (JNCF) 2014 CIRM, Luminy.3 – 7 Novembre 2014
5. K.Martin, Waiting for quantum computing: Why encryption has nothing to worry about techbeacon
6. M. Iavich, S. Gnatyuk, A. Arakelian, G. Iashvili, Y. Polishchuk, D. Prysiazhnyy, Improved Post-quantum Merkle Algorithm Based on Threads, International Conference on Computer Science, Engineering and Education Applications, Springer, Cham, 454-464

Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 10-14 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

PSEUDO RANDOM NUMBER GENERATORS AND ITS USES

მაქსიმ იავიჩი - კავკასიის უნივერსიტეტი
Maksim Iavich – Caucasus University

გიორგი პაპავა სკოლა: 35-ე საჯარო სკოლა

Giorgi papava: 35 Public School
ნიკუშა ნადარაია სკოლა: სკოლა ლიცეუმ "მწიგნობართუხუცესი"
Nikusha Nadaraia. School "Mtsignobartukhutsesi"
გიორგი გოგუაძე სკოლა: 1 გიმნაზია
Giorgi Goguadze. School 1
ბექა პარასკებაშვილი სკოლა:154-ე საჯარო სკოლა
Beqa Paraskebashvili. 154 Public School

ABSTRACT: Growing interest and need in technology made it necessary to make complicated systems and entertainment sources right in your device. As suggested in the paper, many of the services use pseudorandom number generators as services. In this paper, it is described how PRNG started off and its use in the current modern world, as well as its vulnerabilities and Cryptographically secure PRNGs.

KEYWORDS: *pseudo random number generator, PRNG*

აბსტრაქტი: გაზრდილი ინტერესი ტექნოლოგიაში და კომპიუტერული მოწყობილობებისის პოპულარობა, იძულებულს გვხდის შევქმნათ დახვეწილი სისტემები და მრავალი სხვა რამ ჩვენი ყოველდღიური გამოყენების გაჯეტებზე. როგორც ამ კვლევაში არის აღწერილი, მრავალი სერვისი იყენებს PRNG-ს. კვლევაში არის აღწერილი ადრეული ნაბიჯები PRNG-ს და თუ რაში იყენებენ მას დღესდღეობით. ასევე ნახსენებია მისი სუსტი წერტილები და კრიპტოგრაფიულად უსაფრთხო PRNG-ები

PRNG

A PRNG (pseudorandom number generator) is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers. The PRNG-generated sequence is not truly random, because it is completely determined by an initial value, called the PRNG's seed (which may include truly random values). Although sequences that are closer to truly random can be generated using hardware random number generators, pseudorandom number generators are important in practice for their speed in number generation and their reproducibility.

PRNGs are central in applications such as simulations, electronic games and cryptography. Generating random numbers is an essential task in cryptography. Random numbers are necessary not only for generating cryptographic keys, but are also needed in steps of cryptographic algorithms or protocols (e.g. initialization vectors for symmetric encryption, password generation, nonce generation, ...). In a PRNG

with input, one only assumes that users can store a secret internal state and have access to a (potentially biased) random source.

EARLY STAGES OF PRNG

An early computer-based PRNG, suggested by John von Neumann in 1946, is known as the middle-square method. The algorithm is as follows: take any number, square it, remove the middle digits of the resulting number as the "random number", then use that number as the seed for the next iteration. For example, squaring the number "1111" yields "1234321", which can be written as "01234321", an 8-digit number being the square of a 4-digit number. This gives "2343" as the "random" number. Repeating this procedure gives "4896" as the next result, and so on. Von Neumann used 10 digit numbers, but the process was the same.

A problem with the "middle square" method is that all sequences eventually repeat themselves, some very quickly, such as "0000". Von Neumann was aware of this, but he found the approach sufficient for his purposes and was worried that mathematical "fixes" would simply hide errors rather than remove them.

Von Neumann judged hardware random number generators unsuitable, for, if they did not record the output generated, they could not later be tested for errors. If they did record their output, they would exhaust the limited computer memories then available, and so the computer's ability to read and write numbers. If the numbers were written to cards, they would take very much longer to write and read. On the ENIAC computer he was using, the "middle square" method generated numbers at a rate some hundred times faster than reading numbers in from punched cards.

The middle-square method has since been supplanted by more elaborate generators.

A recent innovation is to combine the middle square with a Weyl sequence. This method produces high-quality output through a long period (see Middle Square Weyl Sequence PRNG).

Also In the second half of the 20th century, the standard class of algorithms used for PRNGs comprised linear congruential generators.Linear congruential generators (LCGs) are a class of pseudorandom number generator (PRNG) algorithms used for generating sequences of random-like numbers. The generation of random numbers plays a large role in many applications ranging from cryptography to Monte Carlo methods. The quality of LCGs was known to be inadequate, but better methods were unavailable.

PROBLEMS WITH PRNG

In practice, the output from many common PRNGs exhibit artifacts that cause them to fail statistical pattern-detection tests. These include:

- Shorter-than-expected periods for some seed states (such seed states may be called "weak" in this context);
- Lack of uniformity of distribution for large quantities of generated numbers;
- Correlation of successive values;
- Poor dimensional distribution of the output sequence;

- Distances between where certain values occur are distributed differently from those in a random sequence distribution.

Defects exhibited by flawed PRNGs range from unnoticeable (and unknown) to very obvious. An example was the RANDU random number algorithm used for decades on mainframe computers. It was seriously flawed, but its inadequacy went undetected for a very long time.

In many fields, research work prior to the 21st century that relied on random selection or on Monte Carlo simulations, or in other ways relied on PRNGs, were much less reliable than ideal as a result of using poor-quality PRNGs. Even today, caution is sometimes required, as illustrated by the following warning in the *International Encyclopedia of Statistical Science* (2010).

The list of widely used generators that should be discarded is much longer [than the list of good generators]. Do not trust blindly the software vendors. Check the default RNG of your favorite software and be ready to replace it if needed. This last recommendation has been made over and over again over the past 40 years. Perhaps amazingly, it remains as relevant today as it was 40 years ago.

consider the widely used programming language Java. As of 2017, Java still relies on a linear congruential generator (LCG) for its PRNG, which are of low quality.

One well-known PRNG to avoid major problems and still run fairly quickly was the Mersenne Twister, which was published in 1998. Other higher-quality PRNGs, both in terms of computational and statistical performance, were developed before and after this date; these can be identified in the List of pseudorandom number generators

An Ethereum lottery game, 1000 Guess, had a vulnerability that it generated predictable random numbers. This game decides a winner by a random number when the number of players who bet on the contract reaches to the predetermined number. The contract generated the random number using Sha256() function with private variables and the current block variables, such as block.timestamp, block.coinbase and block.difficulty. However, they are easily readable. First Private variable is accessible by using web3.eth.getStorageAT command. Second, it is well known that block variables can be easily manipulated by malicious miners. So hackers certainly capitalized on it and got a lot of profit from the service.

CRYPTOGRAPHICALLY SECURE PRNGS

A PRNG suitable for cryptographic applications is called a *cryptographically secure PRNG* (CSPRNG). A requirement for a CSPRNG is that an adversary not knowing the seed has only negligible advantage in distinguishing the generator's output sequence from a random sequence. In other words, while a PRNG is only required to pass certain statistical tests, a CSPRNG must pass all statistical tests that are restricted to polynomial time in the size of the seed. Though a proof of this property is beyond the current state of the art of computational complexity theory, strong evidence may be provided by reducing the CSPRNG to a problem that is assumed to be hard, such as integer factorization. In general, years of review may be required before an algorithm can be certified as a CSPRNG.

Some classes of CSPRNGs include the following:

- stream ciphers
- block ciphers running in counter or output feedback mode
- PRNGs that have been designed specifically to be cryptographically secure, such as Microsoft's Cryptographic Application Programming Interface function CryptGenRandom, the Yarrow algorithm (incorporated in Mac OS X and FreeBSD), and Fortuna
- combination PRNGs which attempt to combine several PRNG primitive algorithms with the goal of removing any detectable non-randomness
- special designs based on mathematical hardness assumptions: examples include the *Micali–Schnorr generator*, Naor-Reingold pseudorandom function and the Blum Blum Shub algorithm, which provide a strong security proof (such algorithms are rather slow compared to traditional constructions, and impractical for many applications)
- generic PRNGs: while it has been shown that a (cryptographically) secure PRNG can be constructed generically from any one-way function, this generic construction is extremely slow in practice, so is mainly of theoretical interest.

It has been shown to be likely that the NSA has inserted an asymmetric backdoor into the NIST certified pseudorandom number generator Dual_EC_DRBG

Most PRNG algorithms produce sequences that are uniformly distributed by any of several tests. It is an open question, and one central to the theory and practice of cryptography, whether there is any way to distinguish the output of a high-quality PRNG from a truly random sequence. In this setting, the distinguisher knows that either the known PRNG algorithm was used (but not the state with which it was initialized) or a truly random algorithm was used, and has to distinguish between the two.The security of most cryptographic algorithms and protocols using PRNGs is based on the assumption that it is infeasible to distinguish use of a suitable PRNG from use of a truly random sequence. The simplest examples of this dependency are stream ciphers, which (most often) work by exclusive-or-ing the plaintext of a message with the output of a PRNG, producing ciphertext. The design of cryptographically adequate PRNGs is extremely difficult because they must meet additional criteria. The size of its period is an important factor in the cryptographic suitability of a PRNG, but not the only one.

ACKNOWLEDGEMENT

The work was conducted as a part of SPG-19-133 financed by Shota Rustaveli National Science Foundation of Georgia.

CONCLUSION

According to our research, we confirm that PRNG is truly extremely useful and reliable to use. From computer science to Gambling, It is relevant in various industries, But you should always use the secure PRNG algorithms to ensure that your business doesn’t collapse because of the parasites that want to exploit you. As the technology advances PRNG will advance too, and we will get closer and closer to true randomness.

REFERENCES:

1. Y. Dodis, D.Pointcheval, S. Ruhault, D. Vergnaud , D. Wichs Security Analysis of Pseudo-Random Number Generators with Input: /dev/random is not Robust ? eprint.iacr.org 2013
2. J.Song, Attack on Pseudo-random number generator (PRNG) used in 1000 Guess, an Ethereum lottery game (CVE-2018–12454) medium.com 2018
3. R.Saucier Computer Generation of Statistical Distributions (1st ed.). Aberdeen, MD. Army Research Lab. . (2000).
4. G Iashvili, Y Polishchuk, D Prysiazhnyy, Improved Post-quantum Merkle Algorithm Based on Threads, Advances in Computer Science for Engineering and Education III 1247, 454

Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 15-23 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

OPEN-SOURCE INTELLIGENCE.

ინფორმაციის ღია წყაროებში მოპოვება.

გიორგი იაშვილი - კავკასიის უნივერსიტეტი
Giorgi Iashvili – Caucasus University
რეზიკო ჩალაძე (N20-ე საჯარო სკოლა)
Reziko Chaladze (N20 public school)
დავით ბეგაშვილი (N87-ე საჯარო სკოლა)
Davit Begashvili (N87 public school)
ვიქტორია საგრადიანი (N157 საჯარო სკოლა)
Viktoria Sagradian (N157 public school)
ლუკა სანარსკი (N199 საჯარო სკოლა)
Luka Sanarski (N199 public school)

ABSTRACT: In the following article you will learn about the usage of open-source intelligence. How dangerous it could be to leak wrong information or how it could be used in ethical hacking. In addition, known attacks using similar techniques will be discussed. Finally you will see recommendations to better protect our identity.

აბსტრაქტი: მოცემულ სტატიაში თქვენ გაეცნობით ინფორმაციის ღია წყაროებიდან მოპოვებას და მათ გამოყენებას. თუ რა საფრთხის შემცველი შეიძლება გახდეს არასწორი ინფორმაციის გაჟონვა ან როგორ შეიძლება ის გამოვიყენოთ ეთიკურ ჰაკინგში. ამასთანავე განხილული იქნება მსგავსი ტექნიკით განხორციელებული ცნობილი შეტევები. საბოლოოდ კი შეხვდებით რეკომენდაციებს საკუთარი იდენტობის უკეთესად დასაცავად.

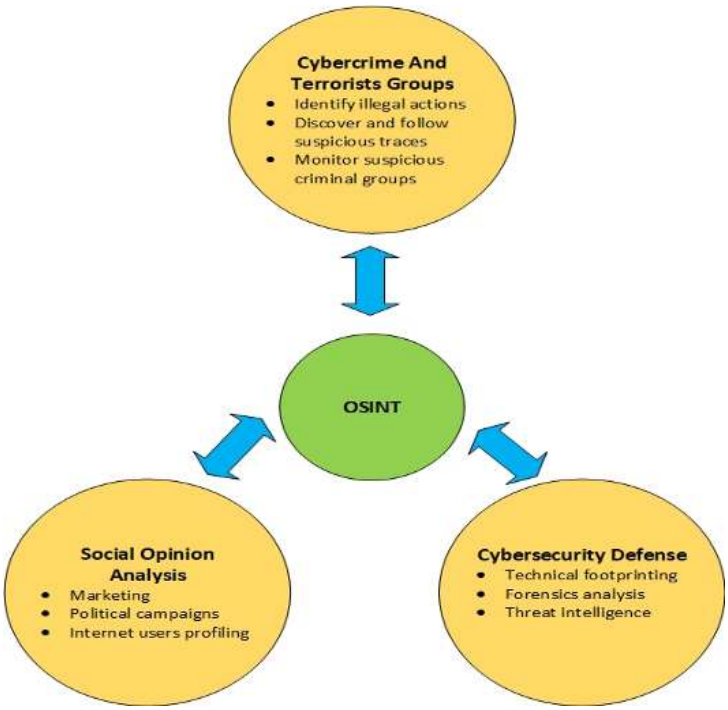
KEYWORDS: *open-source intelligence, social engineering, OSINT, informational leaks*

საკვანძო სიტყვები: *ღია წყაროებში ინფორმაციის მოპოვება, სოც. ინჟინერია, OSINT, ინფორმაციის გაჟონვა*

შესავალი

ტექნოლოგიურმა განვითარებამ შეცვალა ადამიანის ცხოვრების სტილი და ინტერესები. გააუმჯობესა კომუნიკაციის საშუალებები და ინტერნეტთან წვდომა. მეცნიერების აზრით 2030 წლისთვის ადამიანთა 90% გამოიყენებს ინტერნეტს(დაწყებული 6 წლიდან და ზევით). ინტერნეტმა უკვე ფართო დანიშნულება მიიღო, რომელიც ადამიანის ცხოვრებას დღითი-დღე ამარტივებს. პოპულარული გახდა სოციალური ქსელები სადაც ადამიანები წერენ საკუთარი თავის შესახებ, უზიარებენ ერთმანეთს ფოტოებს, ვიდეოებს, სიახლეებს და ა.შ. მომხმარებლები პირად ინფორმაციას საჯაროდ დებენ: სახელი, გვარი, საკონტაქტო ნომერი, საკონტაქტო მეილი, მიღებული განათლება, სამუშაო ადგილი და ა.შ. მაგრამ ამ ინფორმაციის გაზიარებისას ადამიანთა უმრავლესობა ვერ აანალიზებს მისგან გამოწვეულ შესაძლო პრობლემებს. თუ როგორ შეიძლება იყოს ეს ინფორმაცია მათ საზიანოდ გამოყენებული. ხოლო სანამ ამ თემაზე გადავალთ საჭიროა კარგად გავაანალიზოთ რა არის **ღია წყაროებში არსებული ინფორმაცია(OSINT)**.

ღია წყაროებში არსებული ინფორმაცია(OSINT) ეს არის საჯაროდ ხელმისაწვდომი ინფორმაციის მოპოვება, ანალიზი და ექსპლუატაცია მრავალმხრივი მეთოდების გამოყენებით. ის შეიძლება მოძიებული იყოს ინტერნეტშიც და მის გარეთაც(ტელევიზია, რადიო, გაზეთები, ჟურნალები, სტატიები და ა.შ).



როგორც ამერიკის შეერთებული შტატების თავდაცვის სამინისტრო ამბობს:

„ღია წყაროში არსებული ინფორმაცია(OSINT) არის ინფორმაცია, რომელიც წარმოებულია საჯაროდ ხელმისაწვდომი ინფორმაციისგან და არის შეგროვებული, ექსპლუატირებული და გავრცელებული შესაბამის აუდიტორიებში კონკრეტული ინფორმაციული მოთხოვნის გადასაჭრელად.“

ამასთანავე ინფორმაციის გაჟონვის ერთ-ერთი წყარო შეიძლება იყოს სოციალური ინჟინერია. სოც. ინჟინერიაარის ფსიქოლოგიური მანიპულაცია და შეტევა , რომლის დროსაც გარეშე პირი სისტემაზე ან ქსელზე მონოპოლირების მოპოვების მიზნით ანხორციელებს მოტყუების სხვადასხვა გზით მომხმარებლის გამოკითხვას და შემდეგ მიღებული ინფორმაციის გამოყენებას.

OSINT – ი შეგვიძლია დავყოთ რამოდენიმე პირობით ეტაპზე:

- იმის გარკვევა, რომ ინფორმაცია არის ღია წვდომაში
- ინფორმაციის მოგროვება
- ინფორმაციის ანალიზი ან/და გამოძიება

ინფორმაციის მოგროვების რამდენიმე ხერხი არსებობს

- პასიური მოგროვება

ეს არის OSINT – ში ყველაზე გამოყენებადი ინფორმაციის მოგროვების მეთოდი. რეალურად, მონაცემთა მოგროვების ნებისმიერი სქემა უნდა იყენებდეს პასიურ მეთოდს, რადგან OSINT – ის ერთ-ერთი მთავარი დანიშნულებაა ინფორმაციის მხოლოდ ღია წყაროებიდან მოგროვება.

- საშუალოდ პასიური მოგროვება

ტექნიკური თვალსაზრისით, ინფორმაციის მოგროვების ამ ხერხში ზოგადი ინფორმაციის მისაღებად, სამიზნე სერვერთან იგზავნება შეზღუდული ოდენობის ტრაფისი. გაგზავნილი ტრაფიკი მაქსიმალურად ცდილობს დაემსგავსოს ჩვეულებრივ ინტერნეტ ტრაფიქს. ეს კეთდება იმისათვის, რომ სისტემამ სერვერზე ინფორმაციის მოგროვების აქტივობა ვერ აღმოაჩინოს. ამ შემთხვევაში არ ხდება სამიზნის სიღრმისეული შესწავლა, ყველა ქმედება ტარდება ზედაპირულად.

- აქტიური მოგროვება

ამ შემთხვევაში საჭიროა უშუალო ურთიერთქმედება სისტემასთან. ამ პროცესის დროს მსხვერპლი ხვდება, რომ სისტემაში ხდება ინფორმაციის მოგროვება. აქტიური მოგროვების პროცესი მოიცავს ღია პორტების სკანირებას, ინფორმაციის მიღებას მსხვერპლის IT ინფრასტრუქტურის შესახებ, მოწყვლადობების სკანირებას, ისეთების როგორიცაა სისტემის გაუნახლებელი ვერსიები, ვებ სერვისის სკანირებას და ა.შ. ეს ტრაფიკი აისახება სისტემაში როგორც საეჭვო ან მავნე ქმედება და იქნება დაფიქსირებული მსხვერპლის IDS – ის ან IPS – ის მიერ. სოციალური ინჟინერიის თავდასხმაც შეიძლება ჩაითვალოს აქტიური ინფორმაციის მოგროვების მაგალითად.

- ამასთანავე სოციალურ ქსელებში ხშირად დიდი კვალი იტოვება ჩვენი პირადი ინფორმაციის შესახებ როგორიცაა: ტელეფონის ნომერი,მეილი,საცხოვრებელი ადგილი,ოჯახის წევრები და სხვა.

როდესაც ჩვენ კონკრეტული პიროვნება გვყავს სამიზნედ მისი პირადი ინფორმაცია შეიძლება ერთ კონკრეტულ რომელიმე სოც. ქსელში არ ჰქონდეს

და სხვა სოც. ქსელში დარჩენილი იყოს ის ინფორმაცია რაც ჩვენ გვჭირდება მის შესახებ ამისთვის გამოიყენება ხელსაწყო https://checkusernames.com/ რომლის საშუალებითაც

ჩვენ სახელი და გვარით ვეძებთ სხვადასხვა სოციალურ ქსელებში, თუ მაგალითად facebook ზე არაქვს დატოვებული კონკრეტული ინფორმაცია შეიძლება ეს ინფორმაცია სხვა რომელიმე სოც.ქსელში ქონდეს დატოვებული

და ამიტომ საჭიროა მისი სხვა სოციალური ქსელების დათვალიერება.

ღია წყაროში მოპოვებული ინფორმაციის გამოყენება

ღია წყაროში უამრავი ინფორმაციის მოპოვებაა შესაძლებელი მაგრამ მათი გამოყენება ორგვარად შეიძლება. ინფორმაციის გამზიარებლის სასიკეთოდ ან პირიქით მათსავე საზიანოდ.

რა იგულისხმება ინფორმაციის გამზიარებლის სასიკეთოდ გამოყენებაში?! ეს არის სოციალურ მედიაში მომხმარებლის მიერ საკუთარ თავზე გაზიარებული ინფორმაცია რომელიც შეიძლება შეიცავდეს განათლების დონეს, სამუშაო გამოცდილებას და ა.შ. ეს დიდ კომპანიებს კი ყავთ HR რომელიც ზუსტად ამ მეთოდის გამოყენებით ეძებს სამომავლოდ თანამშრომლებს ანდაც ამომავალ ტალანტებს.

მეორე მხრივ, OSINT შესაძლოა იყოს გამოყენებული ბოროტმოქმედების მიერ, რომლებიც აგროვებენ ინფორმაციას პოტენციური მსხვერპლის შესახებ და მიღებულ მონაცემებს შემდგომ სხვადასხვა ტიპის თავდასხმისთვის იყენებენ. მსგავსი ქმედების ერთ-ერთ მაგალითად შეიძლება ჩაითვალოს სოციალური ინჟინერია, რომლის გამოყენების დროსაც ბოროტმოქმედი ახდენს ფსიქოლოგიურ ზეწოლას პოტენციურ მსხვერპლზე, სასარგებლო ან სენსიტიური ინფორმაციის მისაღებად (მაგ. პაროლი ან საბანკო მონაცემები).

სოციალური ინჟინერიის განხრები და მათი ანალიზი

- **სოციალური ინჟინერიის განხრებია:**

Phishing, Spear Phishing, Vishing , Pretexting, Baiting, Tailgating, Quid pro quo. აქ განვიხილავთ რამდენიმე მათგანს.

- **Vishing (Voice Phishing)**

სოციალური ინჟინრები შეიძლება ყველგან იყვნენ ინტერნეტში. Vishing-ის დროს იყენებენ ტელეფონს. ტელეფონის საშუალებით ფიშერები სათაღლითოდ იყენებენ IVR ტექნიკას (Interactive Voice Response). ისინი ხელახლა ქმნიან იმ ხმას, სატელეფონო საჟღერადო ტონს, რომლებიც განეკუთვნებიან ბანკებს ან სხვადასხვა კომპანიებს. თავდამსხმელი თხოვს მსხვერპლს შეიყვანოს პირადი ინფორმაცია, რის შემდეგაც იმახსოვრებენ პინ კოდებს, ანგარიშის პაროლებსა და სხვა და სხვა ინფორმაციას.

- **Baiting**

Baiting არის სოციალური ინჟინერიის ერთ-ერთი განხრა. ამ დროს თავდამსხმელი ტოვებს დაინფიცირებულ CD დისკებს ან USB-ებს, საჯარო ადგილებში იმ იმედით რომ რომელიმე გამვლელი აიღებს ცნობისმოყვარეობის გამო და გამოიყენებს თავის მოწყობილობაზე. მაგალითად ქმნიან დისკს რომელსაც ახატავენ რაიმე პოპულარული ბრენდის ლოგოს, წერენ იგივე საინსტალაციო ფაილს ოღონდ სინამდვილეში ვირუსებით სავსეს. შემდეგ, მათ ტოვებენ ბარებში, მეტროს, ავტობუსის ან ტაქსის სკამებზე. მსხვერპლი აერთებს ნაპოვნ მოწყობილობას თავის მანქანაზე და ჰგონია რომ 100$-იანი პროგრამა უფასოდ იშოვა მაგრამ სინამდვილეში ის საკუთარ მოწყობილობაზე წვდომას აძლევს ბოროტმოქმედს.

- **Tailgating**

ერთ-ერთი ფართოდ გავრცელებული სოციალური ინჟინერიის განხრაა Tailgating (piggybacking). Tailgating არის ფიზიკური უსაფრთხოების დარღვევა როდესაც ადამიანი რომელსაც არ აქვს შესვლის უფლება მიყვება ადამიანს რომელსაც აქვს საშვი დაცულ ადგილას

შესასვლელად. მაგალითად შეიძლება კარი დაუჭიროს თავდამსხმელს თანამშრომელმა და ასე შეუშვას. თუ ეს კომპანია დიდია დიდი ალბათობაა იმისა რომ შემოჭრილი ადამიანი გეგონება თანამშრომელი, სწორედ ამიტომ ასეთი თავდასხმები ხშირად წარმატებული არის.

- **Quid pro quo**

ერთ-ერთი სოციალური ინჟინერიის განხრაა Quid pro quo. ამ დროს ხალხს სთავაზობენ ტექნიკურ დახმარებას. ისინი შემთხვევითობის პრინციპით ურეკავენ რომელიმე კომპანიის თანამშრომელს და ეუბნებიან რომ რაღაც პრობლემის გამო უკავშირდებიან. ზოგჯერ ეძლევათ საშუალება მსხვერპლს გააკეთებინონ ის რაც მოუნდებათ. Quid pro quo ასევე შეიცავს რაღაც დახმარების გაწევას სამიზნისთვის რომ მიიღონ პირველ რიგში ნდობა ხოლო შემდეგ საჭირო ინფორმაცია. მაგალითად თავდამსხმელი ცდილობს მოაგვაროს მსხვერპლის რომელიმე პრობლემა. ასევე შეიძლება იყოს რაიმე მატერიალური შეთავაზება რომელიც გულისხმობს საჩუქარს ინფორმაციის სანაცვლოდ.

„საუკეთესო თავდაცვა არის კარგი OSINT"

დღესდღეობით ხშირი გახდა საჯაროდ გაზიარება ამა თუ იმ პროგრამის სისუსტეების შესახებ. ალბათ ადამიანი იფიქრებს: „რა არის ამაში ცუდი, ისინი გვაჩვენებენ რომ ანახლებენ პროგრამას და ზრუნავენ მომხმარებლის დაცულობასა და კომფორტზე." მართალიც იქნება მაგრამ აქ არის ერთი დიდი მაგრამ. არსებობს ხალხის კატეგორიაც რომელიც ვერ ახერხებს ამ განახლების ინსტალაციას და არჩევს ძველ ვერსიაზე დარჩენას. სისუსტის გაზიარებით შეიძლება ითქვას რომ ჰაკერს ლანგრით ვართმევთ შეტევის გზას ან იდეას. თავდამსხმელი მარტივად გამოიყენებს ამ სისუსტეებს და შეძლებს ან მომხმარებლის კომპიუტერზე წვდომის მიღებას ან მომხმაებლის პირადი ინფორმაციის ნახვას ანდაც ყველაზე უარეს შემთხვევაში ამ პროგრამის მონაცემთა ბაზებზე წვდომას.

ამიტომ როდესაც ზოგიერთი კომპანია ხმარებაში უშვებეს განახლებას, აიძულებეს მომხმარებელს რომ მათ მხარესაც განახლდეს პროგრამა რათა არ მოხდეს მსგავსი ინციდენტები.

ყველა დროის 3 საუკეთესო შეტევა სოც. ინჟინერიით

1. **ტოიოტა, 2019**

2019 წელს ტოიოტა ბოშოკუ კორპორაციაზე მოხდა თავდასხმა სოც ინჟნერიის გამოყენებით. ჰაკერების მსხვერპლი გახდა აუტო ნაწილების მიმწოდებელი. მას გაუგზავნეს საქმიანი მეილი

რომლის დახმარებითაც მსხერპლი დარწმუნეს რომ ადრესატის საბანკო ანგარიშის ინფორმაცია შეეცვალა. საბოლოოდ კი ტოიოტამ 37მილიონი ამერიკული დოლარით იზარალა.

2. ამერიკის დემოკრატიული პარტია, 2016

ერთ-ერთი დასამახსოვრებელი სოც. ინჟინერიის შეტევა მოხდა 2016 წელს აშშ-ში საპრეზიდენტო არჩევნების წინ. რომელმაც არჩევნების შედეგზეც იმოქმედა და დონალდ ტრამპს დაეხმარა გამარჯვებაში.

ჰაკერებმა შექმნეს ტყუილი ანგარიშები რომლითაც დემოკრატიული პარტიის წევრებს გაუგზავნეს ლინკი უჩვეულო საქმიანობის გამო. ამის შემდეგ კი მათ მიიღეს წვდომა ასობით მაილზე და მათზე არსებულ მგრძნობიარე ინფორმაციაზე.

3. RSA, 2011

RSA არის საჯაროდ ცნობილი კრიპტოსისტემა რომელიც უზრუნველყოფს მონაცემების დაცულად მიმოცვლას. 2011 წელს მათ მოუწიათ 66 მილიონი დოლარის დახარჯვა დაცვის სისტემისათვის. ამის მიზეზი კი გახდა ერთ-ერთი თანამშრომლისათვის ექსელის ფაილის გაგზავნა სახელით ,,სამუშაო გეგმა“. რომელიც შეიცავდა ვირუსს და გზა გაუხსნა ჰაკერებს.

როგორ უნდა დავიცვათ თავი

- **წესი #1:** დავაყენოთ ძლიერი პაროლები და უმჯობესი იქნება თუ 3 თვეში ერთხელ შევცვლით პაროლებს.
- **წესი #2:** Facebook - ზე თქვენი კონფიდენციალურობის პარამეტრების არჩევისას გახადეთ თქვენი პოსტები ხილვადი მხოლოდ თქვენი მეგობრებისათვის. დარწმუნდით, რომ თქვენი დასტურის გარეშე თქვენს გვერდზე არ გამოჩნდება პოსტები, რომლებზეც მონიშნული ხართ.
- **წესი #3:** კარგი იქნება თუ დამალავთ თქვენს საცხოვრებელ მისამართს, ტელეფონის ნომერს, ელექტრონული ფოსტის მისამართს და სხვა მონაცემებს (ან არასდროს შეიყვანოთ ისინი რადგან Facebook ხშირად მას მესამე პირებს ჰყიდის).
- **წესი #4:** შეზღუდეთ თქვენი პროფილის მოძებნის შესაძლებლობა და მონიშნეთ ,,მხოლოდ მეგობრები“. ყოველთვიურად წაშალეთ თქვენი Facebook მიმოწერის კონტენტი. იმ შემთხვევაში, თუ პროფილს მოგპარავენ, ვერ შეძლებენ სენსიტიური ინფორმაციის მოპოვებას თქვენი პირადი მიმოწერიდან.

- **წესი #5:** გამორთეთ პერსონალიზებული რეკლამები (Personalized ads).
- **წესი #6:** თქვენი სმარტფონით გადაღებული ფოტოები ბევრ სენსიტიურ მონაცემს შეიცავს მათი გადაღების დროისა და ადგილის შესახებ. თუ შესაძლებელია, არ გააზიაროთ ისინი პირდაპირ სოციალურ მედიაში ან გამორთეთ თქვენი ფოტოების ადგილმდებარეობა. გარდა ამისა, შეამცირეთ ფოტოს ზომა და დაარედაქტირეთ ის (რაც დააზიანებს ფოტოს მეტამონაცემებს).
- **წესი #7:** LinkedIn ხშირად გამოიყენება პერსონალური მონაცემების შესაგროვებლად. თუ თქვენთვის საჭიროა აღნიშნული ქსელის გამოყენება, განათავსეთ მხოლოდ საჯაროდ არსებული ინფორმაცია. გადაამოწმეთ რა ინფორმაცია გაქვთ აქამდე გაზიარებული LinkedIn-ზე.
- **წესი #8:** გაითვალისწინეთ, რომ ყველაფერი, რასაც სოციალურ მედიაში აქვეყნებთ, „ვირტუალურად წაუშლელ“ ინფორმაციად იქცევა, რომელიც თქვენს მოწინააღმდეგეებს გამოადგებათ გამოქვეყნებიდან წლების შემდეგ. შესაბამისად, არ გამოაქვეყნოთ თქვენი სახლის, თქვენი შვილებისა და ახლო მეგობრების ან ნათესავების ფოტოები. გირჩევთ, რომ გადახედოთ ყველა თქვენს ფოტოს Facebook-ზე, Twitter-ზე და Instagram-ზე და წაშალოთ ისეთები, რომლებიც გამოავლენენ იმ ადგილების ან ადამიანების იდენტობას, რომლების გსურთ, რომ დაიცვათ.
- **წესი #9:** დაუთმეთ რამდენიმე საათი თქვენს შესახებ იმ ინფორმაციის ამოსარჩევად, რომელიც, თქვენი აზრით, პირადი ან სენსიტიურია და მოძებნეთ ის Google-ის მეშვეობით, რათა დარწმუნდეთ, რომ სადმე არ გამოჩნდება. ამგვარი მოქმედებით ასევე გაიგებთ, თუ რა ინფორმაციაა საჯაროდ ხელმისაწვდომი ღია წყაროებში თქვენს შესახებ.
- **წესი #10:** გააქტიურეთ Google Alerts შეტყობინების ფუნქცია, რომელიც ელ-ფოსტაზე გამოგიგზავნით შეტყობინებებს, თუ თქვენი სახელი (ან თქვენი სახელის, თანამდებობის, ან თქვენი თანამშრომლის კომბინაცია) რომელიმე ვებსაიტზე ჩნდება. შედეგები არ მოიცავს სოციალურ მედიას.

Acknowledgement

The work was conducted as a part of SPG-19-133 financed by Shota Rustaveli National Science Foundation of Georgia.

ბიბლიოგრაფია

1. R. Layton P. Watters - Automating Open Source Intelligence – 2015
2. N. A. Hassan, R. Hijazi - Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence, 2018
3. A., Babak, B., P. Saskia, S., Fraser - Open Source Intelligence Investigation, 2016

Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 24-27 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

KEY IN CRYPTOGRAPHY AND THEIR IMPORTANCE FOR SECURITY

გასაღები კრიპტოგრაფიაში და მათი მნიშვნელობა უსაფრთხოებისთვის

მაქსიმ იავიჩი - კავკასიის უნივერსიტეტი

Maksim Iavich – Caucasus University

საბა ჩალაძე. N192 საჯარო სკოლა

Saba Chaladze. N192 public school

დავით ღელაღუტაშვილი. N199 საჯარო სკოლა

Davit Ghelaghutashvili. N199 public school

დაჩი გრძელიშვილი.

Dachi Grdzelishvili.

ალექსი ბერიშვილი. N199 საჯარო სკოლა

Aleksi Berishvili. N199 public school

თორნიკე კუმელაშვილი. N199 საჯარო სკოლა

Tornike Kumelashvili. N199 public school

საკვანძო სიტყვები: *კრიპტოგრაფია, გასაღები, უსაფრთხოება*

KEYWORDS: *cryptography, key, security*

აბსტრაქტი: აღნიშნულ სტატიაში, ჩვენ გავეცანით გასაღების გამოყენების ძირითად პრინციპებს კრიპტოგრაფიაში და მის მნიშვნელობას უსაფრთხოებაში. ჩვენ, ასევე, მიმოვიხილეთ RSA ალგორითმი, რომელიც გამოიყენება თანამედროვე კომპიუტერებში, შეტყობინების დაშიფრვისა და განშიფვრისათვის.

ABSTRACT: In this paper, we went over the basic principles of key usages in cryptography and its importance in security. We also reviewed the RSA algorithm, which is used by modern computers to encrypt and decrypt messages.

INTRODUCTION

Encryption is a process that encodes a message or file so that it can be only be read by certain people. Encryption uses an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble, or decrypt, the information. The message contained in an encrypted message is referred to as plaintext. In its encrypted, unreadable form it is referred to as ciphertext.

Basic forms of encryption may be as simple as switching letters. As cryptography advanced, cryptographers added more steps, and decryption became more difficult. Wheels and gears would be combined to create complex encryption systems. Computer algorithms have now replaced mechanical encryption.

What is an encryption key

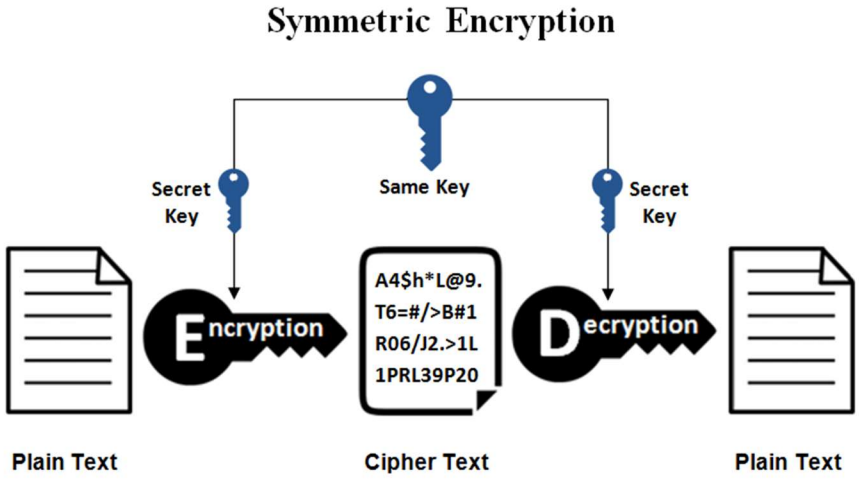
An encryption key is typically a random string of bits generated specifically to scramble and unscramble data. Encryption keys are created with algorithms designed to ensure that each key is unique and unpredictable. The longer the key constructed this way, the harder it is to break the encryption code.

Two types of encryption algorithms can be used by the encryption key server: symmetric algorithms and asymmetric algorithms.

Symmetric-key encryption

Symmetric-key algorithms use the same keys for both encryption and decryption. The keys may be identical or there may be a simple transformation to switch between the two states. The Caesar and ROT13 ciphers above both use a symmetric-key.

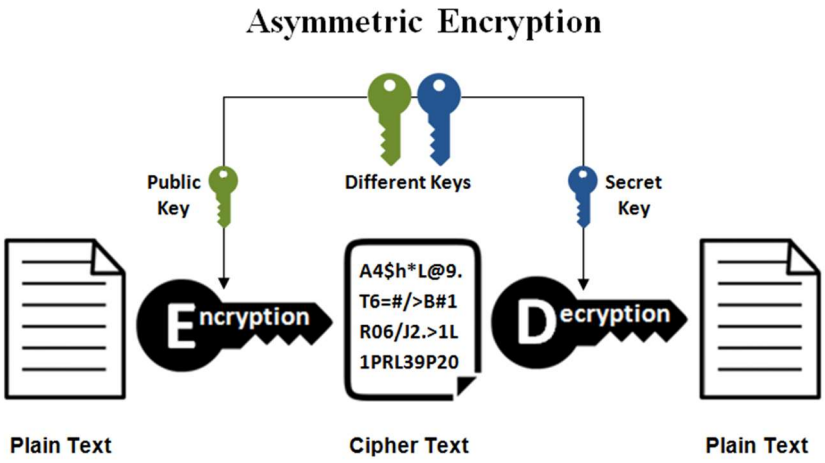
The key acts as a shared secret between two (or more) parties that can be used to send private information that cannot be read by anyone without a copy of the key. The main drawback here is the chicken and egg problem of sharing the secret key. Without a secure channel the key cannot be shared, but without the key no secure channel can be created. In times past this meant meeting in the real to swap a physical copy of the key, the only way to secure against anyone listening in. However, in 1976 a new method was published, allowing this to be done securely online.



Asymmetric-key encryption

Asymmetrical encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that only you know. A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the

internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.



RSA Algorithm

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name RSA algorithm.

RSA works by generating several different encryption keys.Two of those encryption keys are based on large prime numbers.Some math is done on these prime numbers using a one-way function — a mathematical operation that is easy to perform but which cannot be reversed if the answer and only some of the starting information is known. This gets a shared value which allows one of the prime numbers and it to be distributed as a public key, and one of the numbers and it to be kept secret and used as the private key.

Messages encrypted with the private key can easily be decrypted by the public key, which demonstrates that the person who did so holds the private key. This is used for signing messages.

Messages encrypted with the public key can only be decrypted by the private key — this allows the encrypted message to be transmitted over unsecured methods.

Key Security's Importance

Why is key security so important? To explain, let's look at a fundamental principle of cryptography, the so-called Kerckhoff's principle. According to this, security of a cryptosystem is not dependent on the security or confidentiality of any of its parts, but on the key(s) and the key(s) only. Consequently, a communication security problem is essentially a key management problem, as maintaining key security falls into the very definition of key management. Thus, good design of a cryptosystem, which should basically guarantee the complexity of its security, should eventually boil down to the efficient protection of a few cryptographic keys. There are three elements into which key security is divided:key confidentiality or key secrecy, key authenticity or verification of key sender identity, authorized use of the key or permissible use of the key

Cracked: 30 Year-Old Cryptography System

Dublin City University (DCU) researchers, Neill Costigan, PhD student at DCU and funded by the Irish Research Council for Science, Engineering and Technology (IRCSET) and Prof Michael Scott member of the Science Foundation Ireland (SFI)-funded Shannon Institute of Cryptography, have successfully cracked a crypto system published thirty years ago by coding theorist Robert J McEliece.

The crack which was accomplished using resources at the SFI-Funded Irish Centre for High End Computing was announced at the Post-Quantum Cryptography conference in Cincinnati, USA on Saturday 18 October.

Quantum computers will break current public key algorithms such as RSA. McEliece's system is not affected by quantum computers and is a leading candidate for future public-key cryptography. The successful attack shows that the originally proposed key sizes for McEliece's system are too small and need to be increased.

The DCU success was part of a coordinated attack by cryptographers in five countries. The attack was led by Prof Tanja Lange and Christiane Peters (Eindhoven Technical University, TU/e) and Prof Daniel J Bernstein (University of Illinois at Chicago), who recently published a paper claiming that a practical attack on McEliece's system was feasible with their new software.

Costigan and Scott ran the software at ICHEC for 8000 CPU hours and achieved the first break on Wednesday 2nd October 2008. Other countries ran the software for a total of 200000 CPU hours but did not have the luck of the Irish.

Acknowledgement

The work was conducted as a part of SPG-19-133 financed by Shota Rustaveli National Science Foundation of Georgia.

REFERENCES:

1. What is Encryption & How Does It Work? medium.com 2017.
2. T.Anton, The need to manage both symmetric and asymmetric keys, cryptomathic.com. 2019
3. Giorgos-Nektarios Panayotidis, The Role of the Key in Cryptography & Cryptosystems, study.com
4. Symmetric vs. Asymmetric Encryption – What are differences?, ssl2buy.com
5. M Iavich, G Iashvili, A Gagnidze, L Nachkebia, S Khukhashvili, THE ANALYSIS OF THE DIFFERENCE OF 4G AND 5G SECURITIES, Scientific and practical cyber security journal

Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 28-34 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

INFORMATION WAR IN UKRAINE

Volodymyr Khoroshko, National Aviation University, Doctor in Technical Sciences, Professor, Kyiv,
Volodymyr Artemov, National Aviation University, Doctor of pedagogical sciences, Professor, Kiev,
Ivan Opirskyi, Lviv Polytechnic National University, Doctor in Technical Sciences, Associate Professor,
Nikolay Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor, Kyiv, Ukraine
Ihor Ivanchenko, National Aviation University, PhD in Engineering Science, Associate Professor Kyiv, Ukraine

ABSTRACT: Today, the information war is a total phenomenon where it is impossible to determine its beginning and end. This is the existence of a struggle between states with the help of information weapons, that is, it is open and hidden targeted informational influences of states on each other in order to gain an advantage in the material sphere, where informational influences are influences by means of such means, the use of which allows you to achieve your goals. Four approaches to the definition of information war are described, containing political, legal, socio-economic, and psychological actions, involving the capture of the enemy's information space, the destruction of his communications, deprivation of means of transmitting messages, etc., as well as conceptual issues and the basics of network-centric theory control systems and the organization of military operations and cyber actions or cyber war. The implementation of the cybernetic approach strategy for organizing actions during military operations was studied to obtain the maximum effect from the impact on three areas - moral, mental, physical, and the sufficiency of such an approach to increase the mobility, accuracy and firepower of weapons was determined. Also investigated the effect on the most vulnerable objects using the system of the cybernetic approach, which allowed to assess its application in modern conditions of development of strategy and tactics of the struggle in the information field.

KEYWORDS: *informational-psychological influences, informational warfare, informational weapons, informational field, strategy, cybernetic warfare, cyber actions*.

At all stages of human civilization development, information was both the most important object and a means of fighting between people, nations, and states. Individual facts of influence on a wide audience can be revealed throughout the history of society. It is clear that in different periods, the intensity of the use of certain influence methods, as well as the perfection of its organization, are very different.

The politics of information warfare and the use of information influences emerged from the earliest times, but it should be noted that a systematic study of these phenomena only began in the twentieth century. However, the first attempts to investigate these topics took place in ancient times. Among the scholars of ancient times we should mention the works of Aristotle [1], Sun Tzu [2]. In the Renaissance, N. Machiavelli worked on this problem, publishing the book "The Prince" [1]. It is well-known fact that Princess Olga took trip from Kiev to Constantinople, but neither Byzantine nor Russian sources explain the reason and purpose of such a long journey. The realization of informational influences (concealment of information; its partial submission and others) was recorded by the chronicler in the territory of Ukraine during the times of Kievan Rus. The militant prince Svyatopolk reported in advance about his campaign, but kept the direction and forces he planned to use in secret. This was done to start the panic in the state of the enemy troops and quickly defeat him [3]. In the nineteenth century. K. von Clausewitz addressed the issue of information confrontation in the book "On War" [4]. During the XX-XXI centuries. many scientists from all over the world have been very productive in these issues and have achieved considerable success. The first documented research on the theory of information warfare is the work of Martin Libicki "What is Information Warfare?" Great contribution to the development of information warfare has been made by American scientists: Z. Brzezinski, D. Boyd, D. Warden, V. Linda, A. Sebrovski, D. Garstka, J. Stein, G. McLuyen, and also Russian: S. Rastorguev , S. Kara-Murza, A. Manojlo, I. Panyarin, S. Makarenko

and others. In addition, among Ukrainian researchers the following should be noted: G. Pohentsov, O. Litvinenko, V.V. Ostroukhova, V. Lipkanya, L.F. Kompantsev, R. Grishchuk and others.

The term “information warfare” introduced Chinese theorist Shen Wenguan [5,6]. And one of the first to write about the phenomenon of information wars publicly was M. McLuhan in 1960. Even then, it was known that the Cold War is being waged with the help of information technology, since it has been fought with the help of advanced technologies during the whole war.

It should be noted that the hybrid war was the invention of Eugene Messner, a White Guard colonel who was chief of staff at the Cornillian Division. He developed the theory of rebellion-war. In 1967, he published a book called “The Third World Theory”, in Argentina. The General Staff of the Soviet Union began to implement and develop this concept in the late 70's - early 80's of the XX century. In fact, consideration of hostilities and their organization from the standpoint of military cybernetics were formulated by M. Ogarkov during these years. Russia has adopted this concept and is now using it [6].

Information warfare is a total phenomenon where it is impossible to determine its beginning and end. It is the existence of a struggle between states with the help of information weapons, that is, it is open and hidden purposeful informational influences of the states against each other, in order to gain advantage in the material sphere, where the informative influences are influences by such means, the use of which allows to achieve the intended goals.

In [8] it is noted that there are now 4 approaches to the definition of information war:

- The first approach treats it as a set of political-legal, socio-economic, psychological actions that involve seizing the enemy's information space, destroying its communications, depriving the means of communication, and other similar purposes;
- In the second approach, information warfare is the most acute form of confrontation in the information space, where the qualities of interaction such as uncompromising, high intensity of dispute and short duration of intense rivalry are of paramount importance;
- in the third approach, information war is interpreted as a form of providing and conducting military force through the most modern electronic means;
- The fourth approach identifies information wars as cyber wars.

For the first time, the conceptual questions and foundations of the theory of the network-centric system of management and organization of combat and cyber-war were implemented in the US military doctrines "Joint Vision 2010", "Joint Vision 2020". The main aspects of taking a state under external control for the realization of its interests by suppressing the will of the victim population and government to resist through the use of a wide range of innovative technologies that are comprehensively applied were described in a 1989 article by William Linds “The Face of War, Changing: on the way to the fourth generation ”[9]. Major in the fourth-generation wars, according to Linda's views, is the fault of cultures, the initiation, support and nourishment from the outside, and the organization within the state of psychological and information pressure on its population and leadership, taking them under external control and management, creating the conditions for their emergence and promotion. growth in the country of socio-economic chaos and the very depletion of military, financial and other resources [9].

Targeted all-inclusive aggressive attacks on traditional cultural, historical and other values of the population, on the reputation of the most effective leaders of state and state-military administration. Creating conditions to harm education, culture, education of citizens. Starting "low intensity conflicts" with the participation of external, internal and theoretical forces on the victim territory.

The implementation and strategy of the cybernetic approach (Boyd's cybernetic cycle) to organize actions during military operations to maximize the impact on three areas (moral, mental, physical) was carried out by John Boyd during Operation Desert Storm in 1991. He considered war as a combination

of these three components: the destruction of the will of the enemy, the undermining of the common faith and common views; actions to distort and create perceptions of the enemy of reality based on misinformation and to create misconceptions about the situation; the destruction of the enemy's physical resources (weapons, manpower, infrastructure and supplies). At the same time, he proposed to consider all actions of his forces and the forces of the enemy within the cybernetic cycle, which has four processes in its structure: observation, orientation, decision, action ("Boyd's loop"), which, according to the author, reproduces itself and is self-regulating [9].

Based on the works of Boyd and his followers, the following tenets of the theory of OODA (Observe - observe, Orient - orient, Decide - decide, Act - action) [7]:

1. Counterparty military activities (combat operations) are carried out in the same cyber cycles of OODA.

2. The main elements of the OODA cycle are as follows:

- observation - gathering information from internal and external sources;
- orientation - formation of a set of possible plans (options) and evaluation of each of them according to a set of criteria;
- decision - choosing the best action plan for practical implementation;
- action - practical implementation of the chosen action plan.

3. The OODA cycle is a model of military activity of individuals and organizations for war and conflict of all levels (tactical, operational and strategic).

4. Directions for winning (gaining competitive advantage):

- reduction of the OODA cycle execution time;
- improving the quality of decisions made in the cycle.

5. Increasing the speed of all four elements of the OODA cycle is the main way to achieve victory.

Among the four stages of the OODA cycle, three are directly related to information processing and computer technology. The fourth stage (action) is generally "kinematic" and involves the movement in space, defense and defeat of the enemy on the basis of combat.

In order to maintain the timeframes of the OODA cycle of action of their forces and to provide a higher tempo of battle, it is necessary to accelerate all four stages of the cycle that are being implemented. Throughout the twentieth century, all efforts by scientists, engineers, and the military have been directed toward improving weapons and technology in the kinematic portion of the OODA loop. These efforts have resulted in increased mobility, accuracy and firepower of the weapons. However, at the present stage, the technological boundary of the kinematic part of the OODA cycle has come - more powerful weapons inflict acceptable acceptable damage, while faster and more secure weapons platforms and means of delivery deliver a striking target to the target. Due to this, there is a need to improve other stages of the OODA cycle.

Since the first three stages of the OODA cycle are directly related to the processes of gathering, distributing, comprehending, analyzing, and making decisions based on the information obtained, the faster the information is collected, distributed, analyzed, and perceived, the faster the decision is made. Speed and correctness of decision making are most important in today's real combat. This gave impetus to the development of the concept of network-centered military activity.

The issues of systematic disruption of government and the functioning of the state were proposed and implemented during the preparation of Operation Desert Storm in 1991 by Colonel US Air Force. He

developed a systematic, cybernetic approach to modern combat operations, calling it "effect-based operations" that took into account J. Boyd's developments and further developed the cybernetic concept of a network-centric organization of actions with elements of systems restriction theory. According to this concept, there are five main segments: the armed forces, the population, infrastructure, life support systems, military and political leadership - vital to any state. Each state has its unique places in them - vulnerabilities ("centers of gravity". Their correct identification and destructive impact on them leads to the effect of systemic "paralysis" of the state in certain spheres or as a whole.

The central ring of such a system is its most vulnerable object (Fig. 1). Less vulnerable objects in degree, but no less important in value are closer to the outer ring. It is worth noting that J. Warden states that each component has its centers of gravity [10].

Impact on such centers causes changes in the management processes of the objects of influence and consequently affects the whole system. Typical of such a theory is that the degree of influence of the center of gravity on the whole system depends on the degree of its closeness to the central ring. According to J. Warden's theory, the objects of influence are the connections between the rings and the connections within the rings themselves. Thus, the differentiation of subjects or objects of influence on the rings allows them to identify those that are related to the critical cybernetic infrastructure. It is this differentiation that allows them to be perceived as a coherent whole. This ensures that objects (entities) with critical cyber infrastructure are first exposed and then broken. And the tools or means of influence are political, informational, economic and military, which affect objects or centers of gravity.

At the heart of J. Warden's model is the state's military and political leadership, national leaders, which are a critical component of the national security architecture and surrounded and protected by four other rings. The second ring is the system of life support, production, factories, banks, which during the war are vital for the functioning of the military-industrial complex. State infrastructure - roads, railways, power lines - create a third ring. The fourth ring is the society (population), and the last, fifth outer ring is the armed forces [7, 10].

This model is implemented as the scheme "war from the middle to the outside." However, the US scheme works well in conflict zones where the armed forces are viewed by the local population as an external aggressor.

In contrast to this model, Russia has for a long time received support from the local population in the Crimea and significant military formations of the Black Sea Fleet, which were never perceived as an enemy (Fig. 2).

Russia has exerted a long-lasting and consistent influence on the population of the ARC in order to perceive Russian servicemen as defenders of the population and to correct a "historical mistake" regarding Crimea's belonging to Ukraine. Then began to exert influence on the leadership of the Autonomous Republic of Crimea and the city of Sevastopol, and after that - mass information and psychological influence on the personnel of the Armed Forces of Ukraine. The main objects of the transport infrastructure and the life support system were taken under control. The efforts of the Russian Federation to launch a campaign for the introduction of the Armed Forces into the Crimea were accompanied by actions that had all the characteristics of an information and psychological operation prepared and thought out for the purpose, measures and consequences of an information and psychological operation aimed primarily at a Russian audience and, on the other hand, Ukrainian and Western audiences [6]. , 11, 12].

The "hybrid war" tactics applied by Russia in the Crimea were also extended to the southeastern regions of Ukraine (Fig. 3).

The main impact was focused on populated regions. The next influences were government infrastructure and life support systems, respectively. The fourth and fifth circles of influence were the Armed Forces and the military-political leadership of Ukraine [11, 13].

The peculiarity of conducting information-psychological operations in Russia in the south-east of Ukraine is the constant search and use of up-to-date information drives capable of forming the necessary civic opinion. Recently, there has been a tendency to expand its influence on areas previously uncharacteristic of information confrontation, namely the revision of the history of statehood of Ukraine and Russia and interconfession relations.

It should be noted that the information war against Ukraine is aimed not only at loosening the situation inside the country, but also at creating a negative image of Ukraine in the world. This process started in 2005 during the first gas war. At the time, Ukraine was successfully portrayed as a dishonest, and at least dubious, gas transporter, despite the fact that for decades Ukraine had never allowed the disruption of natural gas supplies to Europe. Significantly, at the same time as these accusations, Russia emphasized the need to build gas pipelines alternative to the Ukrainian system. In addition, Ukraine's allegations of gas theft were not substantiated by specific facts [14].

It should be noted that in recent years Ukraine has become the target of powerful information attacks from Russia. Among the most striking examples of such a war is the imposition of the idea of federalization, giving the Russian language the status of a second state language. At different times the list of leading topics, such as the problems of the Black Sea Fleet, the problems of the fuel and energy complex, the problems of the Crimea, as well as the activities of political organizations such as the Right Sector, UNA-UNSO, changed.

For the first time, Ukraine was defeated in this war by spreading and misrepresenting that Ukraine was incapable of holding and servicing nuclear weapons, resulting in Ukraine voluntarily losing its nuclear status, losing its influence in the international arena.

And then there were the cluster scandal, gas wars between Ukraine and Russia, allegations of selling Kolchug to Iraq, and weapons in the Russian-Georgian war. It should be noted that in the years of independence, Ukraine has never worked ahead, took an active position, and always defended itself against information and psychological attacks.

It should be noted that what has been done by Russian media technologists on the territory of Ukraine in recent years has often not been considered as a threat to national security, and the demand of the Ukrainian population for Russian television programs has not caused fears of the Ukrainian authorities that their review will eventually lead to destructive and destabilizing influence on the consciousness of citizens, and through their consciousness - to change the attitude towards Ukraine itself.

And it is really clear that Russia does not spare the finances for the information war, provides information that the state is falling apart, that Ukraine is run by radicals, fascists, “Banderas”, Nazis, junta, who are committing mass riots, vandalism, and the most terrible - they are killing people on the streets, burning Communist houses , "Regionals" and Russian-speaking citizens.

Today the Russian-Ukrainian information war is open. However, Russia also conducts information attacks and actions against other states.

Yes, advocacy companies were previously seen as an ideological tool for promoting concepts. For the first time, Russia's propaganda campaign was also viewed as promoting the idea of a Russian peace. The new quality is that it is not only an advance of ideology, but also a tool of war. In addition, it was not clear until recently what Russian propaganda was. Now the picture has cleared up, it is a multifunctional tool with the highest level of expertise, which involves not only trolls operating in Europe, the US and most in Russia, but also a large group of experts who perform in-depth analysis of

urgent situations and respond very quickly to them. And it is an analysis of both psychological, political and military.

Only now have the European Union countries begun to wake up. They began to realize that in 1981 they had practically completed their activities to counteract the Soviet Union on the information front.

The House of Lords of the British Parliament noted that intelligence and foreign policy analytics of the West had lost the war to Russia, underestimating the directions of its development, and only events in the Crimea and the Donbass made it possible to understand that nothing had changed. Russia has inherited the entire system of the Soviet Union and very well uses information as an element of state power, while the West has actually disarmed itself.

In addition, it appears that the influence on the Western media and institutions is actually exercised by Russia. It also bribes tens of millions of dollars from journalists and European politicians. And this is without taking into account projects that have been converted into propaganda tools - television, radio, newspapers, online publications, as well as a large number of institutes operating in the USA, Europe and other places. In addition, individual arrangements and agreements with lobbyists.

Therefore, the SERA project was created in the European Union to identify information-psychological attacks and impacts, control, collect, analyze and repel or to bring Russian propagandists to the clean water in Europe. The program brings together leading journalists, activists and media analysts from European countries who use their expertise to develop an analytical tool to effectively address Russian misinformation at the strategic, conceptual and institutional levels [15].

Thus, an incredibly powerful information war is being waged on Ukraine. Therefore, it is necessary to develop a strategy and tactics for fighting in the information field.

In addition, it should be borne in mind that in modern conditions the nature of the armed struggle has changed significantly - it has become a "hybrid war".

The emphasis of the armed struggle is shifting towards the practical implementation of information technology. At the same time, information and psychological operations, attacks, actions and actions are becoming increasingly important in achieving political and military goals.

Underestimation of the capabilities of information and psychological weapons, counteracting influences and features of a particular territory can be fatal in the further aggravation of the military and political situation around Ukraine.

REFERENCES

1. Korolko, VG. 2000. “Fundamentals of Public Relations” - M. - K .: Refsl-beech - Wackler. - 528 p.

2. Sun Tzu. 2002. *Treatises on military art.* - M: LLC ATS Publishing House, St. Petersburg: Tezza fantastica. - 260 p.

3. Guz, A.M. *History of information protection in Ukraine and leading countries of the world*. 2007 - K: CST. - 864 p.

4. K. von Clausewitz. 2007 *On war* - M: Exmo. - 260 p.

5. Belska, T.V. 2014. “Information-psychological war as a way of influencing civil society and public policy” / TV Belska // *Technologies and mechanisms of public administration,* no. 3.: 49-56.

6. Zelinsky, S.A. 2008. *Information-psychological impact on the mass consciousness*. - St. Petersburg: Scythia. - 403 p.

7. Pirtskhalava, L.G. 2019. “Information confrontation in modern conditions: a monograph” / LG. Pirtskhalava, V.A. Khoroshko, Yu.E. Khokhlacheva, M.E. Shelest - To: Comprint CPU, - 226 p.

8. Spyga, P.S. 2014 “Fundamentals, technologies and patterns of information war” / PS Spiga, R.M. Rudnik // Problems of International Relations, vol. 8, - p. 326-339.

9. Danik, Yu.G. 2018. “High-tech aspects of national security and defense” // Communications and Networks. Telecom, October - p. 58-69.

10. Grischuk, R.V. 2010. *Fundamentals of Cyber Security* - Zhytomyr: ZhNAEU. - 636 p.

11. Pevtsov, G.V. 2015. “Information-psychological operations of the Russian Federation in Ukraine: models of influence and directions of counteraction” *// Science and Defense*, no. 2: 28-32.

12. Tolubko, V.B 2004. *Information security of the state in the context of combating information wars*. - K: NAOU,. - 176 p.

13. Gorbulin, V.P. 2017. World Hybrid War: The Ukrainian Front / For the General. - K: NISD,. - 496 p.

14. Magda, E. 2014. “Challenges of hybrid warfare: information impact” // *Scientific Notes of the Institute of Legislation of the Verkhovna Rada of Ukraine*, No.5: 138-142.

15. SERA. n.d. “Information and psychological confrontation in Ukraine” Accessed on January 21, 2019
http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/14459

Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 35-61 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების დამუშავებაზე ზედამხედველი ორგანოები და მათი უფლებამოსილება საქართველოსა და ევროკავშირში

SUPERVISORY AUTHORITIES FOR PROCESSING OF IDENTIFICATION DATA FOR ELECTRONIC COMMUNICATION AND THEIR POWERS IN GEORGIA AND THE EUROPEAN UNION

ილია ხუციშვილი „ნიუ ვიჟენ“ უნივერსიტეტი - სამართლის სკოლის დოქტორანტი
Ilia Khutsishvili
LEPL - Academy Of The Ministry Of Internal Affairs Of Georgia- Master's Academic Degree of Law
New Vision University - The Ph.D Programme in Law, Doctoral Student

ანოტაცია*

ნებისმიერი დემოკრატიული სახელმწიფოსათვის მნიშვნელოვანია სამართალდამცავი ორგანოების მიერ ფარული საგამოძიებო მოქმედებების განხორციელების კანონირერების კონტროლი ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემებზე წვდომის პროცესში.

საქართველოს კონსტიტუციის მე-15 მუხლი იცავს ადამიანის პირადი ცხოვრების ერთ-ერთ ყველაზე სენსიტიურ სფეროს - პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებას მასში სახელმწიფოსა და კერძო პირების მიერ დაუსაბუთებელი და უსაფუძვლო ჩარევისაგან. შესაბამისად საქართველოს კონსტიტუციით გარანტირებულია პირის პირადი ცხოვრების ხელშეუხებლობის დაცვის უფლება და იგი ადგენს ფორმალურ, პროცესუალურ წინაპირობას აღმასრულებელი ხელისუფლებისთვის, რომ არ მოხდეს ამ უფლებათა შეზღუდვა სასამართლოს ზედამხედველობის გარეშე.

პირადი ცხოვრების ხელშეუხებლობის უფლებაც შეიძლება შეიზღუდოს დემოკრატიულ სახელმწიფოში აუცილებელი, კონსტიტუციით გათვალისწინებული ლეგიტიმური მიზნების მისაღწევად, ამასთან იმ პირობის სავალდებულო დაცვით, რომ უფლებაში ჩარევა მიზნების მიღწევისთვის აუცილებელი და პროპორციული გზით მოხდება.

აღნიშნული უფლების დაცვა კიდევ უფრო აქტულური ხდება როდესაც საქმე ეხება სამართალდამცავი ორგანოებისა მიერ ფარული საგამოძიებო მიზნებისათვის ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების დამუშავებას.

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

სამართალდამცავი ორგანოები აღმასრულებელი ხელისუფლების ერთ-ერთ უმნიშვნელოვანეს სისტემას წარმოადგენს, რომლის ძირითად ფუნქციებს დანაშაულის პრევენცია/აღკვეთა, საზოგადოებრივი უსაფრთხოებისა და მართლწესრიგის დაცვა განეკუთვნება. დასახული ამოცანების შესასრულებლად სამართალდამცავ უწყებებს კანონმდებლობით მინიჭებული აქვთ ფარული საგამოძიებო საქმიანობის განხორციელება, აქედან გამომდინარე, არსებობს მათი არასათანადოდ გამოყენების რისკი, ამიტომ მათი საქმიანობის ეფექტიანი ზედამხედველობა მნიშვნელოვნად განსაზღვრავს ადამიანის უფლებების დაცვას, მასში დაუსაბუთებელი და უსაფუძვლო ჩარევებისაგან.

საკითხის აქტუალობიდან გამომდინარე, ნაშრომის ფარგლებში განხილულია საქართველოში სამართალდამცავი ორგანოების მიერ ფარული საგამოძიებო მოქმედებების განხორციელების პროცესში ზედამხედველი ორგანოების უფლებამოსილების ფარგლები და ასევე ევროპის მონაცემთა დაცვის საბჭოს უფლებამოსილება ევროკავშირის მასშტაბით პერსონალურ მონაცემთა დაცვის კონტროლის კუთხით.

საკვანძო სიტყვები: *პერსონალური მონაცემი, წვდომა, დამუშავება, ზედამხედველობა;*

ABSTRACT

Control on legality of the covert investigative actions by the law enforcement agencies is important for any democratic state in accessing the electronic communications identifying data.

Article 15 of the Constitution of Georgia protects one of the most sensitive areas of human personal life - rights to personal and family privacy, personal space and privacy of communication, which is inviolable from any unjustified interference by the State and private individuals. Accordingly, the Constitution of Georgia guarantees the right to protection of the privacy of a person and establishes a formal, procedural precondition for the executive authority not to restrict these rights without judicial supervision.

The right to inviolability of privacy may also be restricted in the democratic state for the attainment of the legitimate aims envisaged by the Constitution, but with the obligatory observance of the condition, that interference with the rights for achievement the goal shall be effected in a manner necessary and proportionate.

The protection of this right becomes even more urgent when it comes to the processing of electronic communication identifying data by law enforcement agencies for the covert investigative goals.

Law enforcement agencies are permitted by law to carry out operative and covert investigative activities, thereby there is the risk of their inappropriate use, so effective supervision of their activities significantly supports the protection of human rights from unjustified and ungrounded interference.

Given the urgency of the issue, the paper deals with the scope of the powers of supervisory bodies in the conduct of covert investigative activities by law enforcement agencies in Georgia as well as the powers of the European Data Protection Council with regard to the control of personal data protection throughout the EU.

KEYWORDS: *personal data, access, processing, supervision;*

შესავალი

ნებისმიერი დემოკრატიული სახელმწიფოსათვის მნიშვნელოვანია სამართალდამცავი ორგანოების მიერ ფარული საგამოძიებო მოქმედებების განხორციელების კანონირერების კონტროლი პერსონალურ მონაცემთა დამუშავებისას და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემებზე წვდომის პროცესში. საერთაშორისო დონეზე ევროკავშირმა პერსონალურ მონაცემთა დაცვის ძირითადი საკითხების კოდიფიცირება და განხორციელების ცალკე მექანიზმების რეგლამენტირება 1981 წლის „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ კონვენციის მიღებით განახორციელა (108-ე კონვენცია).[1]

108-ე კონვენცია ვრცელდება პერსონალურ მონაცემთა დამუშავების ყველა სფეროზე და მისი დებულებები მიმართულია პერსონალურ მონაცემთა საერთო დამუშავების რეგულირებისკენ. შესაბამისად, 108-ე კონვენცია ვრცელდება მონაცემთა დაცვაზე სამართალდამცავ სფეროში. აღნიშნული კონვენციის რატიფიცირება საქართველოს პარლამენტმა მოახდინა 2005 წელს.[2] 2001 წელს კი მიღებულ იქნა 108-ე კონვენციის დამატებითი ოქმი „საზედამხედველო ორგანოებისა და მონაცემთა საზღვართშორისი ნაკადების შესახებ“,[3] რომლის რატიფიცირება[4] საქართველოს პარლამენტმა მოახდინა 2013 წელს.

2008 წლის ნოემბერში მიღებულ იქნა ევროსაბჭოს ჩარჩო გადაწყვეტილება “სისხლის სამართლებრივ საკითხებზე პოლიციასა და სასამართლოს შორის თანამშრომლობის ფარგლებში დამუშავებულ პერსონალურ მონაცემთა დაცვის შესახებ”, რომელიც ჩანაცვლდა

---

1 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.01.1981,<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37> [წვდომის თარიღი: 02.11.2020];

2 საქართველოს პარლამენტის დადგენილება „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ კონვენციის რატიფიცირების თაობაზე, საკანონმდებლო მაცნე, 28/10/2005;

3 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, Strasbourg, 08/11/2001, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181>[წვდომის თარიღი: 02.11.2020];

4 საქართველოს პარლამენტის დადგენილება „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს კონვენციის დამატებითი ოქმის (ზედამხედველობით ორგანოებთან და მონაცემთა ტრანსსასაზღვრო გადადინებასთან დაკავშირებით) რატიფიცირების თაობაზე, საკანონმდებლო მაცნე, 27/07/2013;

2016 წლის ევროპარლამენტისა და ევროსაბჭოს 2016/680 დირექტივით. [5] აგრეთვე ჩარჩო გადაწყვეტილება 1987 წლის 17 სექტემბრის ევროპის საბჭოს მინისტრთა კომიტეტის NR (87)15 რეკომენდაცია, რომელიც არეგულირებს პოლიციის სფეროში პერსონალურ მონაცემთა გამოყენებას.[6]

1995 წლის 24 ოქტომბერს მიღებულ იქნა ევროპული პარლამენტისა და საბჭოს დირექტივა 95/46/EC „პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამ მონაცემთა თავისუფალი გადაადგილების შესახებ“,[7] (ჩანაცვლდა 2016 წლის რეგულაციით),[8] რომელიც თავისი არსით განავრცობს 1981 წლის „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ კონვენციის განმარტებებსა და დებულებებს. აღნიშნულ ცვლილებებს შემდგომში მოჰყვა ევროპარლამენტისა და ევროსაბჭოს 1997 წლის დირექტივის 97/66/EC მიღება „სატელეკომუნიკაციო სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების ხელშეუხებლობის დაცვის შესახებ“,[9] რომელიც ჩანაცვლებულ იქნა 2002 წლის „პირადი ცხოვრებისა და ელექტორნული კომუნიკაციების შესახებ დირექტივით“,[10] ხოლო შემდეგ კი 2009/136/EC დირექტივით შევიდა მასში ცვლილებები.[11]

---

[5] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016L0680>[წვდომის თარიღი: 06.11.2020];

[6] The Council of Europe, Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, <https://rm.coe.int/168062dfd4#_ftn1> [წვდომის თარიღი: 02.11.2020];

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046> [წვდომის თარიღი: 02.11.2020];

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504> [წვდომის თარიღი: 02.11.2020];

[9] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, 15 December 1997, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31997L0066> [წვდომის თარიღი: 02.11.20;

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 12 July 2002, [წვდომის თარიღი: 02.11.2020];

[11] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), <https://eur-lex.europa.eu/legal-content/EN/TXT/ELI/?eliuri=eli:dir:2009:136:oj> [წვდომის თარიღი: 02.11.2020];

აღნიშნულიდან გამომდინარე, უნდა ითქვას, რომ პერსონაურ მონაცემთა დამუშავებაზე და მისი დამუშავების კანონიერების კონტროლის მხრივ საკმაოდ მნიშვნელოვანია საერთაშორისო აქტები და რეგულაციები, რომელთა ნაწილის რატიფიცირებაც მოახდინა საქართველოს პარლამენტმა.

1. საქართველო

მას შემდეგ რაც 2014 წლის 1 აგვისტოს საქართველოს პარლამენტმა მიიღო ახალი საკანონმდებლო პაკეტი ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით, ძირეულად გარდაიქმნა მოცემული სფეროს მარეგულირებელი კანონმდებლობა. განხორციელებული ცვლილებების შედეგად საქართველოს სისხლის სამართლის საპროცესო კოდექსს დაემატა ახალი თავი – ფარული საგამოძიებო მოქმედებები.[12]

ფარული მეთვალყურეობის ღონისძიებების განხორციელებაზე, რომელიც მოიცავს სისხლის სამართლის საპროცესო კოდექსით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებებსა და „კონტრდაზვერვითი საქმიანობის შესახებ“ საქართველოს კანონით გათვალისწინებულ კონტრდაზვერვითი საქმიანობის სპეციალურ ღონისძიებებს,[13] პასუხისმგებელია სახელმწიფო უსაფრთხოების სამსახურში არსებული საჯარო სამართლის იურიდიული პირი - ოპერატიულ-ტექნიკური სააგენტო, რომელსაც ექსკლუზიური უფლებამოსილება გააჩნია სატელეფონო კომუნიკაციის ფარულ მიყურადებასა და ჩაწერაზე, კავშირგაბმულობის არხიდან ინფორმაციის მოხსნასა და ფიქსაციაზე და საფოსტო-სატელეგრაფო გზავნილის კონტროლზე.

სსიპ-საქართველოს ოპერატიულ-ტექნიკური სააგენტო, ზემოაღნიშნულ ფარულ საგამოძიებო მოქმედებებთან ერთად აგრეთვე ახორციელებს „კონტრდაზვერვითი საქმიანობის შესახებ“ საქართველოს კანონით გათვალისწინებულ ელექტრონულ თვალთვალსა და სტრატეგიული და ინდივიდუალური მონიტორინგის ღონისძიებებს.

სამართალდამცავი ორგანოების საქმიანობა, რომელიც დაკავშირებულია დანაშაულის გამოძიებასთან, სამართალდარღვევის აღკვეთასთან, სისხლისსამართლებრივი დევნის განხორციელებასთან და ეხება ადამიანის კონსტიტუციით გარანტირებული უფლებების სფეროში ჩარევას, საჭიროებს არა მარტო სამართლებრივ ლეგიტიმაციას, არამედ ამ საქმიანობათა განხორციელების დროს მათი კანონიერების კონტროლსა და ზედამხედველობას. შესაბამისად, სახელმწიფო ვალდებულია გამორიცხოს ძალაუფლების უზურპაციის საფრთხე და უზრუნველყოს აღნიშნული რისკების დაბალანსება კონტროლის

[12] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, თავი XVI[1] ფარული საგამოძიებო მოქმედებები, საკანონმდებლო მაცნე, 09/10/2009;

[13] „კონტრდაზვერვითი საქმიანობის შესახებ“ საქართველოს კანონი, მე-9 მუხლი, საკანონმდებლო მაცნე, 11/11/2005;

საკმარისი მექანიზმებით, რომელიც ხორციელდება ისეთი ორგანოების მეშვეობით როგორებიცაა პროკურატურა, სასამართლო, სახელმწიფო ინსპექტორის სამსახური.

1.1 სასამართლო ზედამხედველობა

ოპერატიულ-სამძებრო ღონისძიებების ჩატარებაზე სასამართლო კონტროლი რეგულირდება „ოპერატიულ-სამძებრო საქმიანობის შესახებ" საქართველოს კანონით. აღნიშნულ აქტებში გაწერილია პროცედურები და ის ვადები, რომლის განმავლობაშიც ოპერატიულ-სამძებრო ღონისძიების განმახორციელებელმა ორგანომ უნდა მიმართოს სასამართლოს.

ოპერატიულ-სამძებრო ღონისძიების ჩატარების შესახებ შუამდგომლობაში უფლებამოსილი პირი მიუთითებს კონკრეტულ ვადას, რომელიც საჭიროა ამა თუ იმ ოპერატიულ-სამძებრო საქმიანობის ჩასატარებლად. მოსამართლე კი მისი შინაგანი რწმენის შესაბამისად მსჯელობს როგორც საქმიანობის ჩატარების, ისე ვადის მიზანშეწონილობაზე.[14]

რაც შეეხება ფარული საგამოძიებო მოქმედებას, იგი ტარდება მოსამართლის განჩინებით. განჩინებას პროკურორის მოტივირებული შუამდგომლობის საფუძველზე იღებს გამოძიების ადგილის მიხედვით რაიონული (საქალაქო) სასამართლოს მოსამართლე,[15] გარდა იმ შემთხვევისა, როდესაც სახელმწიფო-პოლიტიკური თანამდებობის პირის, მოსამართლის და იმუნიტეტის მქონე პირის მიმართ უნდა ჩატარდეს ფარული საგამოძიებო მოქმედება, ასეთ შემთხვევაში ფარული საგამოძიებო მოქმედება შეიძლება ჩატარდეს საქართველოს უზენაესი სასამართლოს მოსამართლის განჩინებით, საქართველოს გენერლაური პროკურორის ან მისი მოადგილის მოტივირებული შუამდგომლობის საფუძველზე.

შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანო: ა) სისხლის სამართლის საპროცესო კოდექსის (სსსკ-ის) 143^1 მუხლით გათვალისწინებული ფარული საგამოძიებო მოქმედების იმ ტერიტორიაზე განხორციელების უზრუნველსაყოფად, სადაც საქართველოს იურისდიქცია ვრცელდება, ვალდებულია გამოიყენოს კომუნიკაციის რეალურ დროში მოპოვების სტაციონარული ან ნახევრად სტაციონარული ტექნიკური შესაძლებლობა,

---

[14] საკონსტიტუციო სასამართლოს №1/1/625, 640 გადაწყვეტილება საქმეზე: საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო", ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო", ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია", ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება" და ააიპ „ადამიანის უფლებათა ცენტრი" საქართველოს პარლამენტის წინააღმდეგ, 2016 წლის 14 აპრილი;

[15] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, 143^3-ე მუხლი, ფარული საგამოძიებო მოქმედების ჩატარების წესი, საკანონმდებლო მაცნე №1772, 09/10/2009;

აგრეთვე გეოლოკაციის რეალურ დროში განსაზღვრის სტაციონარული ან/და არასტაციონარული ტექნიკური შესაძლებლობა.[16]

მოსამართლე პროკურორის შუამდგომლობისა და მისი დასაბუთებისთვის საჭირო, თანდართული მასალის სასამართლოში წარდგენიდან არაუგვიანეს 24 საათისა განიხილავს შუამდგომლობას სსსკ-ის 112-ე მუხლით დადგენილი წესით. მოსამართლეს შეუძლია შუამდგომლობა ზეპირი მოსმენის გარეშე განიხილოს.

მოსამართლე შუამდგომლობას ზეპირი მოსმენით, პროკურორის მონაწილეობით, დახურულ სასამართლო სხდომაზე განიხილავს და განჩინებით იღებს გადაწყვეტილებას ფარული საგამოძიებო მოქმედების ჩატარების ნებართვის გაცემის შესახებ ან მისი ჩატარების ნებართვის გაცემაზე უარის თქმის შესახებ.[17] განჩინება დგება 4 ეგზემპლარად, რომელთაგან ერთი რჩება სასამართლოში, ორი გადაეცემა შუამდგომლობის წარმდგენ პროკურორს ან შესაბამისი საგამოძიებო ორგანოს უფლებამოსილ წარმომადგენელს, რომელთაგან ერთი მიეწოდება შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს და ერთი განჩინება, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, სასამართლოს მიერ მიეწოდება პერსონალურ მონაცემთა დაცვის ინსპექტორს.

მოსამართლის განჩინების ეგზემპლარები შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს და პერსონალურ მონაცემთა დაცვის ინსპექტორს წარედგინება განჩინების გამოტანისთანავე, დაუყოვნებლივ, მაგრამ არაუგვიანეს 48 საათისა, მატერიალური (დოკუმენტური) სახით.

აქედან გამომდინარე, სამართალდამცავი ორგანოების მიერ ოპერატიულ-სამძებრო და ფარული საგამოძიებო მოქმედებების განხორციელება დაუშვებელია სავალდებულო სასამართლო კონტროლის გარეშე, რომელიც არსებობს ორ შემთხვევაში, სასამართლოს წინასწარი ნებართვის ან გადაუდებელი აუცილებლობისას სასამართლოს შემდგომი კონტროლის სახით.[18]

როგორც საკონსტიტუციო სასამართლო გადაწყეტილებაში განმარტავს,[19] „გადაუდებელი აუცილებლობა“ გულისხმობს ისეთ შემთხვევებს, როდესაც თანაზომიერების პრინციპზე დაყრდნობით, კონსტიტუციით გათვალისწინებული საჯარო ინტერესის მიღწევა, რეალურად არსებული ობიექტური მიზეზების გამო, შეუძლებელია კერძო ინტერესების

---

[16] იქვე, 143[3]-ე მუხლი, ფარული საგამოძიებო მოქმედების ჩატარების წესი, საკანონმდებლო მაცნე №1772, 09/10/2009;

[17] იქვე, 143[3]-ე მუხლი, მე-5 ნაწილი, საკანონმდებლო მაცნე №1772, 09/10/2009;

[18] საკონსტიტუციო სასამართლოს №2/1/484 გადაწყვეტილება საქმეზე: „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე თამარ ხიდაშელი საქართველოს პარლამენტის წინააღმდეგ“, ქ. ბათუმი, 2012 წლის 29 თებერვალი;

[19] საკონსტიტუციო სასამართლოს პირველი კოლეგიის №1/3/407 გადაწყვეტილება საქმეზე: „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე-ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ“, ქ. ბათუმი, 2007 წლის 26 დეკემბერი;

დაუყოვნებლივი, მყისიერი შეზღუდვის გარეშე. ამასთან, ძალზე მკაფიო, ნათელი და ცალსახა უნდა იყოს, რომ კონსტიტუციის ფარგლებში საჯარო ინტერესის სხვაგვარად დაცვის მცირედი ალბათობაც არ არსებობს. გადაუდებლობა მიუთითებს დროის სიმცირეზე, რაც უფლების შესაზღუდად მოსამართლის ბრძანების მოპოვების საშუალებას არ იძლევა და საჭიროებს დაუყოვნებლივ მოქმედებას.“

აქედან გამომდინარე, სამართალდამცავი ორგანოების საქმიანობა, რომელიც ეხება ადამიანის უფლებების შეზღუდვასა და კონკრეტულ უფლებაში ჩარევას, ექვემდებარება სასამართლო კონტროლს წინასწარ ან შემდგომ ეტაპებზე. ამგვარი რეგულაციის მიზანია დაიცვას ნებისმიერი პირი ძირითად უფლებებსა და თავისუფლებებში თვითნებური და შეუზღუდავი ჩარევისგან.

ადამიანის უფლებათა სფეროში ჩარევისთვის კანონით გათვალისწინებული მოსამართლის ბრძანების სავალდებულო პირობა ემსახურება კონკრეტული ოპერატიულ-სამძებრო თუ ფარული საგამოძიებო მოქმედებების წინასწარი კონტროლის უზრუნველყოფას დამოუკიდებელი და ნეიტრალური სასამართლოს მიერ. რაც მიმართულია ხელისუფლების მხრიდან ძალაუფლების ბოროტად გამოყენების თავიდან აცილებისაკენ.[20]

სასამართლო კონტროლის ერთ-ერთ ფორმად მიჩნევა აგრეთვე საქართველოს უზენაესი სასამართლო, რომელიც ადგენს ფარული საგამოძიებო მოქმედებების რეესტრს,[21] სადაც აისახება ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული სტატისტიკური ინფორმაცია, კერძოდ: ფარული საგამოძიებო მოქმედებების ჩატარებასთან დაკავშირებით სასამართლოებში შესული შუამდგომლობების და სასამართლოთა მიერ მათზე მიღებული განჩინებების შესახებ ინფორმაცია, აგრეთვე ოპერატიულ-სამძებრო ღონისძიების შედეგად მოპოვებული მასალის განადგურების თაობაზე ინფორმაცია, რომელიც არ ეხებოდა პირის დანაშაულებრივ საქმიანობას, მაგრამ შეიცავდა ცნობებს მისი ან სხვა პირის პირადი ცხოვრების შესახებ.[22] საქართველოს უზენაესი სასამართლო ვალდებულია ყოველი წლის ბოლოს გამოაქვეყნოს აღნიშნული ინფორმაცია.

---

[20] საკონსტიტუციო სასამართლოს პრეცედენტული გადაწყვეტილებები №1/1/625, 640, საქმეზე: საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“, ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ, 2016 წლის 14 აპრილი;

[21] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, 143^{10}-ე მუხლი, ფარული საგამოძიებო მოქმედებების რეესტრი, საკანონმდებლო მაცნე №1772, 09/10/2009;

[22] იქვე, 143^{8}-ე მუხლი, პირველი ნაწილი, საკანონმდებლო მაცნე №1772, 09/10/2009;

1.1.1 ზედამხედველი მოსამართლის ინსტიტუტი

2018 წლის 21 ივლისს მიღებულ იქნა საქართველოს კანონი „სახელმწიფო ინსპექტორის სამსახურის შესახებ",[23] რომელიც ითვალისწინებს სამართალდამცავი ორგანოს წარმომადგენლის, მოხელის ან მასთან გათანაბრებული პირის მიერ ჩადენილ, ადამიანის წამებასთან, წამების მუქარასთან, არასათანადო მოპყრობის სხვა ფორმებთან ან ადამიანის უფლებათა სხვა მძიმე დარღვევებთან დაკავშირებულ დანაშაულთა ეფექტიანი გამოძიების უზრუნველსაყოფად დამოუკიდებელი საგამოძიებო მექანიზმის ჩამოყალიბებას.

აღსანიშნავია, რომ აღნიშნული კანონით სახელმწიფო ინსპექტორის სამსახურის საგამოძიებო უფლებამოსილება სრულად ამოქმედდა 2019 წლის 1 ივლისიდან. „სახელმწიფო ინსპექტორის სამსახურის შესახებ" საქართველოს კანონის მიღებამ გამოიწვია ასევე ცვლილება სისხლის სამართლის საპროცესო კოდექსშიც, მაგალითად: კოდექსის იმ ნორმებში, რომლებიც უკავშირდება პერსონალურ მონაცემთა დაცვის ინსპექტორს, მის ნაცვლად მიეთითება სახელმწიფო ინსპექტორი ან სახელმწიფო ინსპექტორის აპარატი, ასევე, სსსკ-ში გაჩნდა ტერმინი -ზედამხედველი მოსამართლე.[24]

სსსკ-ის მე-3 მუხლის 32^1-ე ნაწილის თანახმად, ამ კოდექსის XVI^1 თავის მიზნებისთვის, ზედამხედველი მოსამართლე არის საქართველოს უზენაესი სასამართლოს თავმჯდომარის მიერ განსაზღვრული საქართველოს უზენაესი სასამართლოს მოსამართლე, რომელიც სახელმწიფო ინსპექტორის სამსახურის მიერ წარმოებულ სისხლის სამართლის საქმეებზე ამ კოდექსით დადგენილი წესით და დადგენილ ფარგლებში აკონტროლებს: ა) ამ კოდექსის 143^1 მუხლის პირველი ნაწილის „ა" ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების სტაციონარული ტექნიკური შესაძლებლობის გამოყენებით ჩატარებას კონტროლის ელექტრონული სისტემითა და კონტროლის სპეციალური ელექტრონული სისტემით; ბ) ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებულ აქტივობებს ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკის კონტროლის ელექტრონული სისტემით; გ) ამ კოდექსის 143^1 მუხლის პირველი ნაწილის „გ" ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების და „ოპერატიულ-სამძებრო საქმიანობის შესახებ" საქართველოს კანონის მე-7 მუხლის მე-3 პუნქტის „ბ" ქვეპუნქტით გათვალისწინებული ღონისძიების განხორციელებას გეოლოკაციის რეალურ დროში განსაზღვრის კონტროლის სპეციალური ელექტრონული სისტემით.

---

[23] საქართველოს კანონი „სახელმწიფო ინსპექტორის სამსახურის შესახებ", საკანონმდებლო მაცნე, 21/07/2018

[24] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, მე-3 მუხლი, 32^1-ე პუნქტი, საკანოინმდებლო მაცნე №1772, 09/10/2009;

ამასთან, სახელმწიფო ინსპექტორის სამსახურის საგამოძიებო ქვემდებარეობა, „სახელმწიფო ინსპექტორის სამსახურის შესახებ" საქართველოს კანონის თანახმად,[25] ვრცელდება: ა) საქართველოს სისხლის სამართლის კოდექსის 144^1-144^3 მუხლებით, 332-ე მუხლის მე-3 ნაწილის „ბ" და „გ" ქვეპუნქტებით, 333-ე მუხლის მე-3 ნაწილის „ბ" და „გ" ქვეპუნქტებით, 335-ე მუხლით ან/და 378-ე მუხლის მე-2 ნაწილით გათვალისწინებულ დანაშაულზე, თუ იგი ჩადენილია სამართალდამცავი ორგანოს წარმომადგენლის, აგრეთვე მოხელის ან მასთან გათანაბრებული პირის მიერ; ბ) სამართალდამცავი ორგანოს წარმომადგენლის, აგრეთვე მოხელის ან მასთან გათანაბრებული პირის მიერ ჩადენილ სხვა დანაშაულზე, რომელმაც გამოიწვია პირის სიცოცხლის მოსპობა და რომლის ჩადენის დროს ეს პირი იმყოფებოდა დროებითი მოთავსების იზოლატორში ან პენიტენციურ დაწესებულებაში, ანდა ნებისმიერ სხვა ადგილას, სადაც სამართალდამცავი ორგანოს წარმომადგენლის, მოხელის ან მასთან გათანაბრებული პირის მიერ, თავისი ნების საწინააღმდეგოდ, აკრძალული ჰქონდა ადგილსამყოფელის დატოვება, ანდა აღნიშნული პირი სხვაგვარად იმყოფებოდა სახელმწიფოს ეფექტური კონტროლის ქვეშ.

როგორც აღინიშნა, სსსკ-ის მე-3 მუხლის 32^1-ე ნაწილის თანახმად, ზედამხედველი მოსამართლე აკონტროლებს სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის სტაციონარული ტექნიკური შესაძლებლობის გამოყენებით ჩატარებას კონტროლის ელექტრონული სისტემითა და კონტროლის სპეციალური ელექტრონული სისტემით. „საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ" საქართვლოს კანონის მე-2 მუხლის „ი" და „კ" ქვეპუნქტები განმარტავენ კონტროლის ელექტრონულ სისტემასა და კონტროლის სპეციალურ ელექტრონულ სისტემას.[26]

აღსანიშნავია, რომ სსსკ-ში 2018 წლის 21 ივლისს შეტანილი საკანონმდებლო ცვლილებების უმთავრეს მიზნად გამოცხადდა არასათანადო მოპყრობის სავარაუდო მსხვერპლთა დაცვა და ამ მიზნით მათი პროცესუალური უფლებებისა და გარანტიების გაფართოება. პროცესუალურ უფლებათა დაცვის მნიშვნელოვან გარანტიად კი გამოიკვეთა მოსამართლის როლის გაზრდა, რისი დადასტურებაცაა სსსკ-ში ზედამხედველი მოსამართლის ინსტიტუტის შემოტანა, რომელიც აკონტროლებს სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ჩატარებასა და შეუძლია შეაჩეროს აღნიშნული ფარული საგამოძიებო მოქმედება კანონით გათვალისწინებული კონკრეტული გარემოებების არსებობისას.

---

[25] საქართველოს კანონი „სახელმწიფო ინსპექტორის სამსახურის შესახებ", მე-19 მუხლის, პირველი პუნქტი, საკანონმდებლო მაცნე, 21/07/2018

[26] საქართველოს კანონი „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ", მე-2 მუხლის „ი" და „კ" ქვეპუნქტები, საკანონმდებლო მაცნე, 22/03/2017;

ზედამხედველი მოსამართლე გასცემს ელექტრონული თვალთვალის ღონისძიების ჩატარების შესახებ ბრძანებას და აკონტროლებს ღონისძიების აღსრულების პროცესს. ზედამხედველი მოსამართლე ადგენს ელექტრონული თვალთვალის განხორციელების ვადებს, მას აქვს უფლება შეაჩეროს ელექტრონული თვალთვალის ღონისძიება კონტროლის ელექტრონული სისტემის მეშვეობით.[27]

ზედამხედველ მოსამართლეს უფლება აქვს, სპეციალურ სამსახურს მოსთხოვოს ელექტრონული თვალთვალის ღონისძიების მიმდინარეობის შესახებ ინფორმაციისა და ელექტრონული თვალთვალის ღონისძიების შედეგად მოპოვებული ინფორმაციის წარდგენა.[28] ელექტრონული თვალთვალის ღონისძიების დასრულების შემდეგ, ზედამხედველ მოსამართლეს წარედგინება ანგარიში ელექტრონული თვალთვალის ღონისძიების შედეგად მოპოვებული ინფორმაციის შესახებ და უფლებამოსილი ორგანოს მიერ შედგენილი შესაბამისი ოქმის ეგზემპლარი სატელეფონო კომუნიკაციის ფარულ მიყურადებასა და ჩაწერას ზედამხედველი მოსამართლე აკონტროლებს ა) კონტროლის ელექტრონული სისტემით, ელექტრონული თვალთვალის ღონისძიების განხორციელების სამართლებრივი საფუძვლის შემოწმებითა და ბ) კონტროლის სპეციალური ელექტრონული სისტემით, ინიცირებულ/განხორციელებულ ბრძანებათა ლოგირების მონაცემების სამართლებრივ საფუძვლებთან შედარებით.

ამავე მიზნით, ზედამხედველი მოსამართლე აგრეთვე უფლებამოსილია გაეცნოს კონტროლის ელექტრონული სისტემითა და კონტროლის სპეციალური ელექტრონული სისტემით მიწოდებულ იმ აქტივობებს, შესაბამის სამართლებრივ დოკუმენტებს და ლოგირების მონაცემებს, რომლებიც ფარული საგამოძიებო მოქმედების ჩატარების მიზნით ხორციელდება.[29]

აღსანიშნავია, რომ გადაუდებელი აუცილებლობის შემთხვევაში შესაძლებელია კონტრდაზვერვითი საქმიანობის მიზნებისთვის ელექტრონული თვალთვალის დაწყება ზედამხედველი მოსამართლის ბრძანების გარეშე, თუმცა ამ შემთხვევაში სპეციალური სამსახური ვალდებულია დაუყოვნებლივ აცნობოს სასამართლოს და ელექტრონული თვალთვალის ღონისძიების დაწყებიდან 24 საათში მიმართოს მას შესაბამისი შუამდგომლობით.[30] იმ შემთხვევაში, თუ ზედამხედველი მოსამართლე შუამდგომლობის საფუძველზე არ გასცემს ელექტრონული თვალთვალის განხორციელების ნებართვას, ელექტრონული თვალთვალის ღონისძიება დაუყოვნებლივ უნდა შეწყდეს, ხოლო

---

[27] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, 143^6-ე მუხლი, მე-5^1 ნაწილი, საკანონმდებლო მაცნე, 09/10/2009;
[28] იქვე, 143^6-ე მუხლი, მე-14 ნაწილი, საკანონმდებლო მაცნე, 09/10/2009;
[29] იქვე, 143^3-ე მუხლი, საკანონმდებლო მაცნე, 09/10/2009;
[30] იქვე, 143^3-ე მუხლი, მე-6 ნაწილი, საკანონმდებლო მაცნე, 09/10/2009;

ელექტრონული თვალთვალის ღონისძიების შედეგად მიღებული/მოპოვებული ინფორმაცია უნდა განადგურდეს.[31]

1.2 საპროკურორო ზედამხედველობა

საპროკურორო ზედამხედველობის არსი მდგომარეობს ქვეყანაში კანონის უზენაესობის დაფუძნებასა და საზოგადოებრივი წესრიგის შენარჩუნებაში. პროკურატურის ორგანიზაციული სტრუქტურა მსოფლიოს სხვადასხვა ქვეყანაში ძირითადად ორის სახითაა გავრცელებული. პირველი სახის პროკურატურს წარმოადგენს სრულიად დამოუკიდებელ უწყებას, რომელიც არ შედის არც ერთი სამინისტროს დაქვემდებარებაში, მეორე სახის პროკურატურა კი უშუალოდ იუსტიციის სამინისტროს დაქვემდებარებაშია და ახორციელებს სამინისტროს მიერ მისთვის განსაზღვრულ უფლებამოსილებებს.

რაც შეეხება საქართველოში საპროკურორო ზედამხედველობას ოპერატიულ-სამძებრო და ფარულ საგამოძიებო მოქმედებებზე, საპროკურორო კონტროლის ფორმები დადგენილია როგორც სისხლის სამართლის საპროცესო კანონმდებლობით, ასევე „პროკურატურის შესახებ“ საქართველოს ორგანული კანონითა[32] და გენერალური პროკურორის შესაბამისი ბრძანებითაც,[33] რომლითაც განსაზღვრულია სამართალდამცავ ორგანოებში ოპერატიულ-სამძებრო ღონისძიებებზე საპროკურორო ზედამხედველობის განხორციელების წესები და ფორმები.

როგორც კონსტიტუციის, ისე „ოპერატიულ-სამძებრო საქმიანობის შესახებ” საქართველოს კანონის შესაბამისად, გადაუდებელი აუცილებლობის შემთხვევაში შესაძლებელია იმ სახის ოპერატიულ-სამძებრო და ფარული საგამოძიებო ღონისძიებების ჩატარება, რომლებიც ზღუდავენ ადამიანის უფლებებს ან შესაძლებელია შეზღუდონ. ასეთი ღონისძიებები ხორციელდება პროკურორის დადგენილებით, გადაუდებელი აუცილებლობის პირობებში, რომელიც ისევ სასამართლო და საპროკურორო ზედამხედველობის საგანს წარმოადგენს.[34]

სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“–„გ“ ქვეპუნქტებით გათვალისწინებული რომელიმე ფარული საგამოძიებო მოქმედების განხორციელების შემთხვევაში პროკურორი

---

[31] იქვე, 143[6]-ე მუხლი, მე-4 ნაწილი, საკანონმდებლო მაცნე №1772, 09/10/2009;

[32] საქართველოს ორგანული კანონი პროკურატურის შესახებ, საკანონმდებლო მაცნე, 30/11/2018;

[33] საქართველოს გენერალური პროკურორის №9 ბრძანება საქართველოს გენერალური პროკურატურის თავდაცვის სამინისტროში, იუსტიციის სამინისტროსა და სპეციალურ პენიტენციურ სამსახურში გამოძიების საპროცესო ხელმძღვანელობისა და ოპერატიულ-სამძებრო საქმიანობაზე ზედამხედველობის დეპარტამენტის დებულების დამტკიცების შესახებ, საკანონმდებლო მაცნე, 26/12/2019;

[34] საქართველოს კანონი „ოპერატიულ-სამძებრო საქმიანობის შესახებ“, VI თავი, საკანონმდებლო მაცნე, №1933, 30/04/1999;

ვალდებულია ფარული საგამოძიებო მოქმედების დადგენილებაში მითითებული დაწყების დროიდან არაუგვიანეს 24 საათისა მიმართოს რაიონულ (საქალაქო) სასამართლოს, რომლის სამოქმედო ტერიტორიაზედაც ჩატარდა/ტარდება აღნიშნული ფარული საგამოძიებო მოქმედება, ან გამოძიების ადგილის მიხედვით სასამართლოს შუამდგომლობით გადაუდებელი აუცილებლობისას ჩატარებული/მიმდინარე ფარული საგამოძიებო მოქმედების კანონიერად ცნობის შესახებ.

შუამდგომლობაში პროკურორმა უნდა დაასაბუთოს როგორც ზემოაღნიშნული მუხლის მე-2 ნაწილით გათვალისწინებული გარემოებების,[35] ისე იმ გარემოებების არსებობა, რომლებმაც განაპირობა ფარული საგამოძიებო მოქმედების მოსამართლის განჩინების გარეშე, გადაუდებლად ჩატარება/დაწყება. მოსამართლე პროკურორის შუამდგომლობას განიხილავს მისი სასამართლოსთვის წარდგენიდან არაუგვიანეს 24 საათისა, ზემოაღნიშნული მუხლის მე-5 ნაწილით დადგენილი წესით.[36]

შუამდგომლობის განხილვისას მოსამართლე ამოწმებს, შეესაბამება თუ არა ჩატარებული/მიმდინარე ფარული საგამოძიებო მოქმედება სსსკ-ის მოთხოვნებს, აუცილებელი იყო თუ არა აღნიშნული ფარული საგამოძიებო მოქმედების გადაუდებლად ჩატარება/დაწყება და განჩინებით იღებს ერთ-ერთ შემდეგ გადაწყვეტილებას: ა) ჩატარებული ფარული საგამოძიებო მოქმედების კანონიერად ცნობის შესახებ; ბ) მიმდინარე ფარული საგამოძიებო მოქმედების კანონიერად ცნობის და მისი ჩატარების ვადის არაუმეტეს 48 საათამდე გაგრძელების შესახებ.[37] ეს ვადა აითვლება პროკურორის დადგენილებაში მითითებული ფარული საგამოძიებო მოქმედების დაწყების დროიდან;გ) ჩატარებული/მიმდინარე ფარული საგამოძიებო მოქმედების უკანონოდ ცნობის, მისი შეწყვეტის, შედეგების გაუქმების და მის შედეგად მოპოვებული მასალის/ინფორმაციის განადგურების შესახებ.

გადაუდებელი აუცილებლობის შემთხვევაში ფარული საგამოძიებო მოქმედების ჩატარების შესახებ პროკურორის დადგენილებას, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, ფარული საგამოძიებო მოქმედების დადგენილებაში მითითებული დაწყების დროიდან არაუგვიანეს 12 საათისა პროკურორი ან პროკურორის დავალებით გამომძიებელი მატერიალური (დოკუმენტური) სახით წარუდგენს სახელმწიფო ინსპექტორის სამსახურს. სსს კოდექსის 143^1 მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების ჩატარების შესახებ პროკურორის დადგენილება, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, სააგენტოს მიერ მისი მიღებისთანავე მიეწოდება სახელმწიფო ინსპექტორის სამსახურს ელექტრონული ეგზემპლარის სახით, კონტროლის ელექტრონული სისტემის მეშვეობით.

---

[35] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, 143^1-ე მუხლი, მე-2 ნაწილი, საკანონმდებლო მაცნე №1772, 09/10/2009;

[36] იქვე, 143^3-ე მუხლი, მე-5 ნაწილი, საკანონმდებლო მაცნე №1772, 09/10/2009;

[37] იქვე, 143^3-ე მუხლი, მე-5 ნაწილი, საკანონმდებლო მაცნე №1772, 09/10/2009;

პროკურორის დადგენილების ელექტრონული ეგზემპლარის პროგრამულად მიწოდების დადასტურებისთანავე სააგენტო იწყებს სსს კოდექსის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებას. ამ ნაწილით გათვალისწინებული ელექტრონული ეგზემპლარის მიწოდების წესი მოქმედებს იმ შემთხვევაში, როდესაც გამოიყენება სტაციონარული ტექნიკური შესაძლებლობა. თუ შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოსთვის წარდგენილი გადაუდებელი აუცილებლობის შემთხვევაში ფარული საგამოძიებო მოქმედების ჩატარების შესახებ პროკურორის დადგენილება ბუნდოვანება-უზუსტობას შეიცავს, შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანო ამის თაობაზე დაუყოვნებლივ აცნობებს პროკურორს ან შესაბამისი საგამოძიებო ორგანოს უფლებამოსილ წარმომადგენელს.[38]

პროკურორი უზრუნველყოფს დადგენილებაში არსებული ბუნდოვანება-უზუსტობის აღმოფხვრას. ფარული საგამოძიებო მოქმედების კანონიერად/უკანონოდ ცნობის შესახებ მოსამართლის განჩინება დგება 4 ეგზემპლარად, რომელთაგან ერთი რჩება სასამართლოში, ორი გადაეცემა შუამდგომლობის წარმდგენ პროკურორს ან შესაბამისი საგამოძიებო ორგანოს უფლებამოსილ წარმომადგენელს, რომელთაგან ერთი მიეწოდება შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს, და ერთი განჩინება, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, სასამართლოს მიერ მიეწოდება სახელმწიფო ინსპექტორის სამსახურს.

სისხლის სამართლის საპროცესო კანონმდებლობა გარკვეულწილად ზღუდავს პროკურატურის უკანონო ქმედებებს იმ თვალსაზრისით, რომ არსებობს ყველა მტკიცებულების წარმომავლობის და მოპოვების კანონიერების გადამოწმების ვალდებულება, რათა თავიდან იქნეს აცილებული ამ მტკიცებულების ან მასზე დაყრდნობით მოპოვებული სხვა მტკიცებულებების დაუშვებლად ცნობა სისხლის სამართლის პროცესში. შესაბამისად, რეალურ დროში ინფორმაციის მოპოვება პერსონალურ სახელმწიფო ინსპექტორის სამსახურის მიერ კონტროლის გარეშე კანონით დადგენილი წესის გარეშე მოპოვებულ მტკიცებულებად ჩაითვლება, რაც განაპირობებს მის დაუშვებლობას სისხლის სამართლის პროცესში. ამასთან, საპროცესო კანონმდებლობით განსაზღვრულია იმ ინფორმაციის განადგურების წესი და პროცედურა, რომელიც სისხლის სამართლის პროცესში მტკიცებულებად არ გამოიყენება.[39]

[38] იქვე, 143[3]-ე მუხლი, მე-6 ნაწილი, საკანონმდებლო მაცნე, 09/10/2009;
[39] იქვე, 143[8]-ე მუხლი, საკანონმდებლო მაცნე, 09/10/2009;

1.3 სახელმწიფო ინსპექტორის სამსახურის ზედამხედველობა

,,ასოცირების შესახებ შეთანხმების“[40] ფარგლებში იმპლმენტაციის კუთხით საქართველომ იკისრა ვალდებულება დაცვის ისეთი სამართლებრივი დონის შემუშავებისა, რომელიც სულ მცირე შეესაბამება დირექტივასა და ასოცირების შესახებ შეთანხმების პირველი დანართით გათვალისწინებულ სხვა საერთაშორისო დოკუმენტებს. აქედან გამომდინარე 2011 წლის 28 დეკემბერს საქართველოს პარლამენტმა მიიღო საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“,[41] რომლის მიზანია პერსონალური მონაცემის დამუშავებისას უზრუნველყოს ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის დაცვა.

სწორედ ზემოაღნიშნული საერთაშორისო კონვენციები და ევროკავშირის დირექტივები გახდა საფუძველი იმისა, რომ რომ დღესდღეობით არსებული საკანონმდებლო მოწესრიგებით, საქართველოში სამართალდამცავი ორგანოების მიერ პერსონალურ მონაცემთა დამუშავება და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემებზე წვდომა სახელმწიფო ინსპექტორის სამსახურის ზედამხედველობის კომპეტენციას განეკუთვნება, რომელიც ახორციელებს პერსონალურ მონაცემთა დამუშავების კანონიერებისა და ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლს.[42]

„ელექტრონული კომუნიკაციების შესახებ” საქართველოს კანონის თანახმად, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემები არის მომხმარებლის მაიდენტიფიცირებელი მონაცემები; კომუნიკაციის წყაროს კვალის დადგენისა და იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის ადრესატის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის თარიღის, დროისა და ხანგრძლივობის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის სახის იდენტიფიცირებისათვის საჭირო მონაცემები; მომხმარებლის კომუნიკაციის აღჭურვილობის ან შესაძლო აღჭურვილობის იდენტიფიცირებისათვის საჭირო მონაცემები; მობილური

[40] საქართველოს საერთაშორისო ხელშეკრულება და შეთანხმება “ასოცირების შესახებ შეთანხმება ერთის მხრივ, საქართველოსა და მეორეს მხრივ, ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებს შორის”, საკანონმდებლო მაცნე, 27/06/2014;

[41] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, საკანონმდებლო მაცნე, 28/12/2011;

[42] საქართველოს კანონი „სახელმწიფო ინსპექტორის სამსახურის შესახებ“, მე-18 მუხლი, ფარული საგამოძიებო მოქმედებების ჩატარების და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლი, საკანონმდებლო მაცნე, 21/07/2018;

კომუნიკაციის აღჭურვილობის ადგილმდებარეობის იდენტიფიცირებისათვის საჭირო მონაცემები;[43]

სახელმწიფო ინსპექტორის მონაწილეობა ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემებზე წვდომის პროცესში ფარული საგამოძიებო და ოპერატიულ-სამძებრო საქმიანობის დროს წარმოადგენს აღნიშნული ქმედებების კონტროლის ერთ-ერთ მექანიზმს.[44]

2015 წლის 31 მარტს სისხლის სამართლის საპროცესო კოდექსში ამოქმედდა ნორმები,[45] რომლებიც ითვალისწინებდა ფარული საგამოძიებო მოქმედებების განხორციელების ორეტაპიანი ელექტრონული სისტემის დამკვიდრებას. სსსკ.-ის 2017 წლის 22 მარტამდე მოქმედი 143[4] მუხლის მეორე ნაწილის თანახმად, სატელეფონო საუბრის ფარულ მიყურადებასა და ჩაწერას უფლებამოსილი ორგანო ახორციელებდა ფარული საგამოძიებო მოქმედებების განხორციელების ორეტაპიანი ელექტრონული სისტემის მეშვეობით. სსსკ-ის მე-3 მუხლის 32-ე ნაწილი კი განმარტავდა ფარული საგამოძიებო მოქმედებების განხორციელების ორეტაპიანი ელექტრონული სისტემის ცნებას, ეს იყო ტექნიკურ და პროგრამულ გადაწყვეტილებათა ერთობლიობა, რომელიც გამორიცხავდა პერსონალურ მონაცემთა დაცვის ინსპექტორის ელექტრონული თანხმობის გარეშე სამართალდამცავი ორგანოს მონიტორინგის სისტემის მეშვეობით ობიექტის აქტივაციის შესახებ ბრძანების დამოუკიდებლად განხორციელების შესაძლებლობას.

აღნიშნული ძირითადად გულისხმობდა იმას, რომ ფარული საგამოძიებო მოქმედებების განსახორციელებლად სამართალადამცავ ორგანოს, სასამართლოს მხრიდან ნებართვის გარდა სჭირდებოდა ელექტრონული ნებართვა პერსონალურ მონაცემთა დაცვის ინსპექტორისგანაც. სატელეფონო საუბრის ფარულ მიყურადებასა და ჩაწერას კი ახორციელებდა საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ოპერატიულ-ტექნიკური დეპარტამენტი.[46]

2016 წელს, სხვა ნორმებთან ერთად საკონსტიტუციო სასამართლოში შეტანილ იქნა სარჩელი[47] სსსკ-ის 143[3] მუხლის მე-4 ნაწილის ნორმატიული შინაარსი, რომლის მიხედვითაც

---

[43] საქართველოს კანონი „ელექტრონული კომუნიკაციების შესახებ“, მე-2 მუხლის ჰ[62] ქვეპუნქტი, საკანონმდებლო მაცნე, 02/06/2005;

[44] საქართველოს კანონი „სახელმწიფო ინსპექტორის სამსახურის შესახებ“, მე-2 მუხლი და მე-18 მუხლები, საკანონმდებლო მაცნე, 21/07/2018;

[45] საქართველოს კანონი „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“, საკანონმდებლო მაცნე 2870-Iს, 30/11/2014;

[46] ხოდელი მ., სადისერტაციო ნაშრომი „სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით)“, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი იურიდიული ფაკულტეტი, 2019 წელი, გვ.245;

[47] საკონსტიტუციო სარჩელი №640 (საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო”, ააიპ „საერთაშორისო გამჭვირვალობა - საქართველო”, ააიპ

უფლებამოსილი სახელმწიფო ორგანოს მიერ ამ კოდექსის 143^1 მუხლის პირველი ნაწილის „ა" და „ბ" ქვეპუნქტებით გათვალისწინებული ფარული საგამოძიებო მოქმედებების ჩატარების უზრუნველსაყოფად კანონით განსაზღვრული უფლებამოსილი პირი იყენებდა კავშირგაბმულობისა და კომუნიკაციის ფიზიკური ხაზებიდან და მათი შემაერთებლებიდან, მეილსერვერებიდან, ბაზებიდან, კავშირგაბმულობის ქსელებიდან და კავშირგაბმულობის სხვა შემაერთებლებიდან ინფორმაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობას, აგრეთვე კომუნიკაციის აღნიშნულ საშუალებებთან განათავსებდა და ამონტაჟებდა სათანადო აპარატურას და პროგრამული უზრუნველყოფის მოწყობილობებს.

საკონსტიტუციო სასამართლომ დააკმაყოფილა აღნიშნული საკონსტიტუციო სარჩელი და არაკონსტიტუციურად ცნო საქართველოს კონსტიტუციის მე-16 და მე-20 მუხლის პირველ პუნქტთან მიმართებით (2016 წელს მოქმედი რედაქცია) საქართველოს სისხლის სამართლის საპროცესო კოდექსის მე-3 მუხლის 31-ე ნაწილი და ამავე კოდექსის 143^3 მუხლის მე-4 ნაწილი.[48] შესაბამისად, არაკონსტიტუციურად იქნა ცნობილი სახელმწიფო უსაფრთხოების სამსახურის ტექნიკური წვდომა სატელეკომუნიკაციო ოპერატორების ქსელებთან, რაც განაპირობებდა კომუნიკაციის მონაცემთა შეგროვებისა და მონიტორინგის შეუზღუდავ შესაძლებლობას.

2017 წლის 31 მარტამდე დაევალა საქართველოს პარლამენტს სატელეკომუნიკაციო ოპერატორების სერვერებზე პირდაპირი წვდომის შეზღუდვისა და კონტროლის გამკაცრების მიზნით შესაბამისი საკანონმდებლო ცვლილებების განხორციელება სისხლის სამართლის საპროცესო კოდექსში.[49]

2017 წლის 22 მარტის საკანონმდებლო ცვლილებებით გაუქმდა საკონსტიტუციო სასამართლოს გადაწყვეტილებით არაკონსტიტუციურად ცნობილი ფარული საგამოძიებო მოქმედებების განხორციელების ორეტაპიანი ელექტრონული სისტემა და პერსონალურ მონაცემთა დაცვის ინსპექტორს,* წინასწარი თანხმობის ნაცვლად, მიენიჭა ფარული

„საქართველოს ახალგაზრდა იურისტთა ასოციაცია", ააიპ „სამართლიანი არჩევნებისა და ემოკრატიის საერთაშორისო საზოგადოება" და ააიპ „ადამიანის უფლებათა ცენტრი" საქართველოს პარლამენტის წინააღმდეგ).

[48] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება, N 1/1/625, 640, საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები - გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო", ააიპ „საერთაშორისო გამჭვირვალობა - საქართველო", ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია", ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება" და ააიპ „ადამიანის უფლებათა ცენტრი" საქართველოს პარლამენტის წინააღმდეგ, ქ.ბათუმი, 14 აპრილი, 2016;

[49] განმარტებითი ბარათი საქართველოს კანონის პროექტზე სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ, https://info.parliament.ge/file/1/BillReviewContent/141417 [წვდომის თარიღი: 07.03.2020]

* 2019 წლის 1 ივლისიდან პერსონალურ მონაცემთა დაცვის ინსპექტორის ნაცვლად მიეთითება სახელმწიფო ინსპექტორის სამსახური, შესაბამისის საკანონმდებლო ცვლილებები განხორციელდა

საგამოძიებო მოქმედების განხორციელების კონტროლის ელექტრონული სისტემის მეშვეობით შეჩერების უფლება. შეიქმნა ახალი ორგანო საჯარო სამართლის იურიდიული პირი - საქართველოს ოპერატიულ-ტექნიკური სააგენტო (სააგენტო),[50] რომელიც სსსკ-ის მე-3 მუხლის 32-ე ნაწილის „ა"ქვეპუნქტის შესაბამისად, სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ჩატარების ექსკლუზიური უფლებამოსილების მქონე ორგანოა.[51] აღნიშნული სააგენტო არა მხოლოდ ფლობს ტექნიკურ საშუალებებს ფარული მოსმენების განსახორციელებლად, არამედ პასუხისმგებელია ამ სისტემის ფუნქციონირებაზე, რა მიზნითაც ის ქმნის შესაბამის პროგრამულ უზრუნველყოფას და განათავსებს ტექნიკურ საშუალებებს.

საქართველოს პარლამენტის მიერ სისხლის სამართლი საპროცესო კოდექსში განხორციელებული ცვლილებების შედეგად 143^3 მუხლის მე-5^1 ნაწილის თანახმად, სატელეფონო კომუნიკაციის ფარული მიყურადების შესახებ მოსამართლის განჩინების ელექტრონული ეგზემპლარის სახელმწიფო ინსპექტორისთვის პროგრამულად მიწოდების დადასტურებისთანავე სააგენტო იწყებს სატელეფონო კომუნიკაციის ფარულ მიყურადებასა და ჩაწერას. აღსანიშნავია, რომ ელექტრონული ეგზემპლარის მიწოდების აღნიშნული წესი მოქმედებს იმ შემთხვევაში, როდესაც გამოიყენება სტაციონარული ტექნიკური შესაძლებლობა.[52]

აღსანიშნავია, რომ სისხლის სამართლის საპროცესო კოდექსი განსაზღვრავს შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს ვალდებულებას, რომ სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის უზრუნველსაყოფად, სადაც საქართველოს იურისდიქცია ვრცელდება, გამოიყენოს კომუნიკაციის რეალურ დროში მოპოვების სტაციონარული ან ნახევრად სტაციონარული ტექნიკური შესაძლებლობა.[53]

საკანონმდებლო ცვლილებების შედეგად, სახელმწიფო ინსპექტორის სამსახურს, როგორც ფარული საგამოძიებო მოქმედებებზე ზედამხედველ ორგანოს, მიენიჭა საგამოძიებო მოქმედებების შეწყვეტისა და შეჩერების უფლებამოსილება.[54] კანონმდებლობით განისაზღვრა სახელმწიფო ინსპექტორის სამსახურის უფლებამოსილებები ფარული საგამოძიებო მოქმედებების ჩატარების კონტროლის სფეროში და სახელმწიფო ინსპექტორს მიენიჭა უფლებამოსილება განახორციელოს ფარული

საქართველოს სისხლის სამართლის საპროცესო კოდექსში, საკანონმდებლო მაცნე №3276-რს, 21/07/2018;

[50] საქართველოს კანონი „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ", საკანონმდებლო მაცნე, 22/03/2017;

[51] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, მე-3 მუხლის 32-ე ნაწილის „ა"ქვეპუნქტი, საკანონმდებლო მაცნე, 09/10/2009;

[52] იქვე, 143^3-ე მუხლი, მე-51 ნაწილი, საკანონმდებლო მაცნე, 09/10/2009;

[53] იქვე, 143^3-ე მუხლი, მე-4 ნაწილი, საკანონმდებლო მაცნე, 09/10/2009;

[54] საქართველოს კანონი „სახელმწიფო ინსპექტორის სამსახურის შესახებ", მე-16 მუხლი, საკანონმდებლო მაცნე, 21/07/2018;

საგამოძიებო მოქმედებების ჩატარების და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლი, ესენია: ა) კონტროლის ელექტრონული სისტემით – მონაცემთა დამუშავების კანონიერება; ბ) კონტროლის სპეციალური ელექტრონული სისტემით – მონაცემთა დამუშავების კანონიერება; გ) მონაცემთა დამმუშავებლის/უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერება (ინსპექტირება).[55]

2. ევროკავშირი

დამოუკიდებელი ზედამხედველობა მონაცემთა დაცვის ევროპული კანონმდებლობის მნიშვნელოვანი კომპონენტია. როგორც ევროკავშირის, ისე ევროპის საბჭოს კანონმდებლობის მიხედვით, პერსონალურ მონაცემთა დამუშავების კონტექსტში ფიზიკურ პირთა უფლებებისა და თავისუფლებების დასაცავად, დამოუკიდებელი საზედამხედველო ორგანოს არსებობა აუცილებელია. ვინაიდან პეროსნალურ მონაცემთა დაცვა სულ უფრო და უფრო რთულდება ციფრული ტექნოლოგიების განვითარებასთან ერთად, შესაბამისად იზრდება საზედამხედველო ორგანოების როლი.

ევროკავშირში დამოუკიდებელი საზედამხედველო ორგანოების არსებობა პერსონალურ მონაცემთა დაცვის უფლების ერთ-ერთ ყველაზე მნიშვნელოვან ელემენტად მიიჩნევა. მას ძირითადად, ევროკავშირის კანონმდებლობა ითვალისწინებს. ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლის მე-3 პუნქტისა[56] და ევროკავშირის ფუნქციონირების შესახებ ხელშეკრულების (TFEU) მე-16 მუხლის მე-2 პუნქტის თანახმად,[57] პერსონალური მონაცემების დაცვა ფუნდამენტური უფლებაა, ხოლო მონაცემთა დაცვის დამუშავების წესებსა და კანონიერებას უნდა აკონტროლებდეს დამოუკიდებელი ორგანო. მონაცემთა დაცვის კანონმდებლობის შესრულების კუთხით, დამოუკიდებელი საზედამხედველო ორგანოს მნიშვნელობა აღიარებულია პრეცედენტულ სამართალშიც.

ევროპული კანონმდებლობა აწესებს დამოუკიდებელი ზედამხედველობის მოთხოვნას, როგორც მნიშვნელოვან მექანიზმს მონაცემთა ეფექტიანად დაცვისათვის. პირადი ცხოვრების ხელშეუხებლობის უფლების შეზღუდვისას, დამოუკიდებელი საზედამხედველო ორგანო მონაცემთა სუბიექტისთვის პირველი საკონტაქტო პირია. როგორც ევროკავშირის, ისე ევროპის საბჭოს კანონმდებლობის თანახმად, საზედამხედველო ორგანოს შექმნა სავალდებულოა. ორივე სამართლებრივი ჩარჩო ითვალისწინებს ამ ორგანოს

---

[55] იქვე, მე-18 მუხლი, საკანონმდებლო მაცნე, 21/07/2018;

[56] Charter of fundamental rights of the European Union, Article 8, Official Journal C 364 , 18/12/2000 P. 0001 – 0022, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000X1218%2801%29> [წვდომის თარიღი: 04.03.2020];

[57] Treaty on the Functioning of the European Union, Article 16, Official Journal C 326 , 26/10/2012 P. 0001 – 0390, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT> [წვდომის თარიღი: 04.03.2020];

უფლებამოვალეობათა ჩამონათვალს, რომელიც ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციაში (GDPR)[58] წარმოდგენილი სიის მსგავსია. ამგვარად, შეიძლება ითქვას, რომ საზედამხედველო ორგანოები ფუნქციონირებენ ერთნაირად, როგორც ევროკავშირის, ისე ევროპის საბჭოს კანონმდებლობის მიხედვით.

ევროკავშირის კანონმდებლობაში GDPR-ი ითვალისწინებს საზედამხედველო ორგანოთა კომპეტენციებსა და ორგანიზაციულ სტრუქტურას და ადგენს მოთხოვნას, რომ ისინი იყვნენ კომპეტენტურები და ჰქონდეთ რეგულაციით გათვალისწინებული ფუნქციების შესასრულებლად საჭირო უფლებამოსილება. საზედამხედველო ორგანო ეროვნულ კანონმდებლობაში ძირითადი უწყებაა, რომელიც უზრუნველყოფს შესაბამისობას ევროკავშირის მონაცემთა დაცვის კანონმდებლობასთან. მას აქვს არაერთი მოვალეობა და უფლებამოსილება, რომლებიც სცდება პროაქტიული და პრევენციული ზედამხედველობის ფარგლებს. ამ მოვალეობათა შესასრულებლად, საზედამხედველო ორგანოს უნდა ჰქონდეს სათანადო უფლებამოსილებები გამოძიების, დარღვევის გამოსწორებისა თუ კონსულტაციის გაცემის მხრივ, რომლებიც წარმოდგენილია GDPR-ის 57-ე და 58-ე მუხლებში,[59] კერძოდ: კონსულტაცია გაუწიოს მონაცემთა სუბიექტებსა და დამმუშავებლებს მონაცემთა დაცვის ყველა საკითხზე; დაამტკიცოს სტანდარტული სახელშეკრულებო პირობები, სავალდებულო ძალის მქონე კორპორატიული წესები, ან ადმინისტრაციული შეთანხმებები; გამოიძიოს დამუშავების ოპერაციები და საჭიროების შემთხვევაში, ჩაერიოს კიდეც; მოითხოვოს ინფორმაცია, რომელიც საჭიროა მონაცემთა დამმუშავებლის საქმიანობაზე ზედამხედველობისთვის; მონაცემთა დამმუშავებელს გამოუცხადოს გაფრთხილება ან საყვედური და გასცეს ბრძანება, რომ პერსონალურ მონაცემთა უსაფრთხოების დარღვევა ეცნობოთ მონაცემთა სუბიექტებს; გასცეს მონაცემთა შესწორების, დაბლოკვის, წაშლის ან განადგურების ბრძანება; დააწესოს დროებითი ან საბოლოო აკრძალვა მონაცემთა დამუშავებაზე, ან შესაბამის პირს დააკისროს ადმინისტრაციული ჯარიმა; საქმე განსახილველად გადასცეს სასამართლოს.[60]

ზემოაღნიშნული ფუნქციების განსახორციელებლად, საზედამხედველო ორგანოს ხელი მიუწვდებოდესა ყველა პერსონალურ მონაცემსა და ინფორმაციაზე, რომელიც საჭიროა მოკვლევის ჩასატარებლად, აგრეთვე, ნებისმიერ შენობაზე, სადაც მონაცემთა

---

58 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), Official Journal of the European Union L 119/1, < https://eur-lex.europa.eu/eli/reg/2016/679/oj>, [წვდომის თარიღი: 04.03.2020];

59 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 57 and Article 58, Official Journal of the European Union L 119/1, https://eur-lex.europa.eu/eli/reg/2016/679/oj [წვდომის თარიღი: 07.03.2020]

60 ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ. 227;

დამმუშავებელი რელევანტურ ინფორმაციას ინახავს. მართლმსაჯულების ევროპულ სასამართლოს (CJEU-Court of Justice of the European Union) თანახმად, საზედამხედველო ორგანოს უფლებამოსილებები უნდა განიმარტოს ფართოდ, რაც უზრუნველყოფს მონაცემთა დაცვის სრულ ეფექტიანობას ევროკავშირში.

Schrems-ის საქმეში მართლმსაჯულების ევროპულმა სასამართლომ, ევროკავშირსა და აშშ-ს შორის დაცვის საშუალებათა შეთანხმების (Safe Harbour Agreement) საფუძველზე, განიხილა აშშ-სთვის პერსონალური მონაცემების გადაცემის შესაბამისობა ევროკავშირის მონაცემთა დაცვის სამართალთან. საქმე ეხებოდა მასობრივ თვალთვალს აშშ-ს ეროვნული უსაფრთხოების სააგენტოს მხრიდან, რაც ედვარდ სნოუდენის სკანდალმა გამოააშკარავა. მართლმსაჯულების ევროპულმა სასამართლომ განმარტა, რომ ეროვნულ საზედამხედველო ორგანოებს, როგორც მონაცემთა დამუშავების დამოუკიდებელ მონიტორებს, აქვთ პერსონალურ მონაცემთა მესამე ქვეყნისთვის გადაცემის პრევენციის უფლება (მიუხედავად გადაწყვეტილებისა შესაბამისობის შესახებ), თუკი არსებობს გონივრული მტკიცებულება, რომ მესამე ქვეყანაში სათანადო დაცვა აღარ არის გარანტირებული.[61]

თითოეულ საზედამხედველო ორგანოს აქვს სათანადო კომპეტენცია საგამოძიებო უფლებამოსილების განხორციელებისა და ჩარევისათვის საკუთარი იურისდიქციის ფარგლებში. თუმცა, ვინაიდან მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის აქტივობები ხშირად კვეთს საზღვარს, თვითონ დამუშავება კი გავლენას ახდენს რამდენიმე წევრ სახელმწიფოში მყოფ მონაცემთა სუბიექტებზე, აქტუალური ხდება კომპეტენციათა გადანაწილება სხვადასხვა საზედამხედველო ორგანოს შორის.

GDPR-ის მიღებით, დეტალური წესები დაინერგა საერთაშორისო საქმეებში საზედამხედველო ორგანოების უფლებამოსილებასთან დაკავშირებით. რეგულაცია ადგენს „ერთი ფანჯრის პრინციპს“ და მოიცავს დებულებებს, რომლებიც სავალდებულოს ხდის სხვადასხვა საზედამხედველო ორგანოს შორის თანამშრომლობას. საერთაშორისო საქმეებზე ეფექტიანი თანამშრომლობისთვის, GDPR ადგენს წამყვანი საზედამხედველო ორგანოს შექმნის ვალდებულებას, მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის ძირითადი დამოუკიდებელი ზედამხედველობა ან ერთადერთი ადგილსამყოფელის მიხედვით.[62]

წამყვანი საზედამხედველო ორგანო, რომელიც საერთაშორისო საქმეებზე მუშაობს, მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ერთადერთი მარეგულირებელია საერთაშორისო დამუშავების პროცესში და კოორდინაციას უწევს სხვა საზედამხედველო

---

61 Judgment of the Court (Grand Chamber) of Maximillian Schrems v Data Protection Commissioner, Case C-362/14, 6 October 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362, [წვდომის თარიღი: 07.03.2020];

62 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 56 (1), Official Journal of the European Union L 119/1, https://eur-lex.europa.eu/eli/reg/2016/679/oj [წვდომის თარიღი: 07.03.2020]

ორგანოებთან თანამშრომლობას, კონსენსუსის მისაღწევად. თანამშრომლობა მოიცავს ინფორმაციის გაცვლას, ურთიერთდახმარებას მონიტორინგისა და გამოძიების პროცესში, ასევე, შესასრულებლად სავალდებულო გადაწყვეტილებათა მიღებას.[63]

ევროპის საბჭოს კანონმდებლობაში საზედამხედველო ორგანოთა კომპეტენციები და უფლებამოსილებები წარმოდგენილია მოდერნიზებული 108-ე კონვენციის მე-15 მუხლში და შეესაბამება მათთვის ევროკავშირის კანონმდებლობით მინიჭებულ უფლებამოსილებებს, როგორიცაა: გამოძიება და ჩარევა; ადმინისტრაციული სანქციის დაწესება გადაწყვეტილებათა გამოცემისა და კონვენციის დებულებათა დარღვევის შემთხვევაში; სასამართლო საქმისწარმოების დაწყება. ზოგადად, დამოუკიდებელ საზედამხედველო ორგანოებს აქვთ შემდეგი უფლებამოსილებებიც: რეაგირება მონაცემთა სუბიექტების მოთხოვნებსა და საჩივრებზე; საზოგადოების ცნობიერების ამაღლება მონაცემთა დაცვის კანონმდებლობის შესახებ; კონსულტაციის გაწევა მათთვის, ვინც ეროვნულ დონეზე იღებს გადაწყვეტილებას იმ საკანონმდებლო ან ადმინისტრაციულ ზომებზე, რომლებიც ითვალისწინებს პერსონალურ მონაცემთა დამუშავებას.

ევროპის მონაცემთა დაცვის საბჭო (EDPB) ერთ-ერთ მნიშვნელოვან როლს ასრულებს მონაცემთა დაცვის წესების ეფექტიანად და თანმიმდევრულად დანერგვაში ევროკავშირის მასშტაბით GDPR-ის თანახმად, ევროპის მონაცემთა დაცვის საბჭო (EDPB) შექმნილია როგორც ევროკავშირის ორგანო და სამართლის სუბიექტი.[64] საბჭო 29-ე მუხლის სამუშაო ჯგუფის სამართალმემკვიდრეა. ეს უკანასკნელი კი მონაცემთა დაცვის დირექტივის საფუძველზე შეიქმნა შემდეგი მიზნებით: კომისიისათვის კონსულტაციის გაწევა ევროკავშირის ნებისმიერ ღონისძიებაზე, რომელიც გავლენას ახდენს ფიზიკურ პირთა უფლებებზე პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების ხელშეუხებლობის კუთხით; დირექტივის ერთგვაროვანი დანერგვის ხელშეწყობა; და კომისიისთვის ექსპერტული მოსაზრების მიწოდება მონაცემთა დაცვის საკითხებზე. 29-ე მუხლის სამუშაო ჯგუფი შედგებოდა ევროკავშირის წევრი სახელმწიფოების საზედამხედველო ორგანოების, ასევე, კომისიისა და ევროკავშირის მონაცემთა დაცვის ზედამხედველის (EDPS) წარმომადგენლებისგან.

სამუშაო ჯგუფის მსგავსად, საბჭოს შემადგენლობაში არიან: თითოეული წევრი სახელმწიფოს საზედამხედველო ორგანოს ხელმძღვანელი, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, ან მათი წარმომადგენლები.[65] ევროკავშირის მონაცემთა დაცვის ზედამხედველი (EDPS) სარგებლობს თანაბარი ხმის უფლებით, გარდა დავების გადაწყვეტის

---

[63] იქვე, Article 60, Official Journal of the European Union L 119/1, https://eur-lex.europa.eu/eli/reg/2016/679/oj [წვდომის თარიღი: 07.03.2020];

[64] იქვე, Article 68, Official Journal of the European Union L 119/1, https://eur-lex.europa.eu/eli/reg/2016/679/oj [წვდომის თარიღი: 07.03.2020];

[65] იქვე, Article 68(3), Official Journal of the European Union L 119/1, https://eur-lex.europa.eu/eli/reg/2016/679/oj [წვდომის თარიღი: 07.03.2020];

შემთხვევებისა. ასეთ საქმეებში ევროკავშირის მონაცემთა დაცვის ზედამხედველს (EDPS) ხმის მიცემა შეუძლია მხოლოდ იმ პრინციპებსა და წესებზე გადაწყვეტილებათა მიღებისას, რომლებიც შეეხება ევროკავშირის ინსტიტუტებს და შეესაბამება GDPR-ით გათვალისწინებულ პრინციპებსა და წესებს. კომისიას უფლება აქვს, მონაწილეობა მიიღოს საბჭოს შეხვედრებსა და საქმიანობაში, ხმის მიცემის უფლების გარეშე.

საბჭო წევრებიდან ირჩევს თავმჯდომარეს (რომელიც წარმოადგენს საბჭოს) და თავმჯდომარის ორ მოადგილეს, უბრალო უმრავლესობით და 5-წლიანი ვადით. ამასთან, ევროპის მონაცემთა დაცვის საბჭოს (EDPB) აქვს სამდივნოც, რომელსაც უზრუნველყოფს ევროკავშირის მონაცემთა დაცვის ზედამხედველი (EDPS). იგი ანალიტიკურ, ადმინისტრაციულ და ლოგისტიკურ მხარდაჭერას უწევს საბჭოს.[66] ევროპის მონაცემთა დაცვის საბჭოს (EDPB) ფუნქციები დეტალურად არის აღწერილი GDPR-ის 64-ე, 65-ე და 70-ე მუხლებში და მოიცავს კომპლექსურ ფუნქციებს, რომელთა დაყოფაც შეიძლება 3 ძირითად კატეგორიად: თანმიმდევრულობა, კონსულტაცია და ხელმძღვანელობა.

აქედან გამომდინარე უნდა ითქვა, რომ ევროკავშირის მონაცემთა დაცვის სტანდარტები ეფუძნება ევროპის საბჭოს 108-ე კონვენციას, მონაცემთა დაცვის ზოგად რეგულაციასა და მონაცემთა დაცვის დირექტივას პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის. ასევე, ადამიანის უფლებათა ევროპული სასამართლოსა და ევროკავშირის მართლმსაჯულების სასამართლოს პრეცედენტულ სამართალს.

დასკვნა

აქედან გამომდინარე, უნდა ითქვას, რომ პერსონალურ მონაცემეთა დამუშავებაზე ზედამხედველობა დემოკრატიული სახელმწიფოს ერთ-ერთი უმნიშვნელოვანესი პრიორიტეტია. ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების დამუშავებაზე ზედამხედველობა საზოგადოებრივი ურთიერთობებისა და ტექნოლოგიური საშუალებების განვითარებასთან ერთად უფრო აქტუალური ხდება, მითუმეტეს როდესაც უფრო აქტულური ხდება როდესაც საქმე ეხება სამართალდამცავი ორგანოებისა და უსაფრთხოების სამსახურების მიერ ოპერატიულ-სამძებრო და ფარული საგამოძიებო მიზნებისათვის ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების დამუშავებას.

სამართალდამცავი ორგანოები აღმასრულებელი ხელისუფლების ერთ-ერთ უმნიშვნელოვანეს სისტემას წარმოადგენს, რომლის ძირითად ფუნქციებს დანაშაულის პრევენცია/აღკვეთა, საზოგადოებრივი უსაფრთხოებისა და მართლწესრიგის დაცვა

[66] იქვე, Article 71, Article 75, Official Journal of the European Union L 119/1, https://eur-lex.europa.eu/eli/reg/2016/679/oj [წვდომის თარიღი: 07.03.2020];

განეკუთვნება. აღნიშნული ამოცანების შესასრულებლად სამართალდამცავ უწყებებს კანონმდებლობით მინიჭებული აქვთ ფარული საგამოძიებო და ოპერატიულ-სამძებრო საქმიანობის განხორციელება, აქედან გამომდინარე, არსებობს მათი არასათანადოდ გამოყენების რისკი, ამიტომ მათი საქმიანობის ეფექტიანი ზედამხედველობა მნიშვნელოვნად განსაზღვრავს ადამიანის უფლებების დაცვას, მასში დაუსაბუთებელი და უსაფუძვლო ჩარევებისაგან.

ბიბლიოგრაფია

ნორმატიული მასალა:

1. საქართველოს კონსტიტუცია, საკონონმდებლო მაცნე, 24/08/1995;

2. საქართველოს საერთაშორისო ხელშეკრულება და შეთანხმება "ასოცირების შესახებ შეთანხმება ერთის მხრივ, საქართველოსა და მეორეს მხრივ, ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებს შორის", საკანონმდებლო მაცნე, 27/06/2014;

3. საქართველოს ორგანული კანონი „პროკურატურის შესახებ", საკანონმდებლო მაცნე, 30/11/2018;

4. საქართველოს სისხლის სამართლის საპროცესო კოდექსი, საკანონმდებლო მაცნე, 09/10/2009;

5. საქართველოს კანონი „ელექტრონული კომუნიკაციების შესახებ", საკანონმდებლო მაცნე, 02/06/2005;

6. საქართველოს კანონი „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ", საკანონმდებლო მაცნე, 22/03/2017;

7. საქართველოს კანონი „სახელმწიფო ინსპექტორის სამსახურის შესახებ", საკანონმდებლო მაცნე, 21/07/2018;

8. საქართველოს კანონი „ოპერატიულ-სამძებრო საქმიანობის შესახებ", საკანონმდებლო მაცნე, №1933, 30/04/1999;

9. საქართველოს კანონი „კონტრდაზვერვითი საქმიანობის შესახებ“, საკანონმდებლო მაცნე, №2097, 11/11/2005;

10. საქართველოს პარლამენტის დადგენილება „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ კონვენციის რატიფიცირების თაობაზე, საკანონმდებლო მაცნე, 28/10/2005;
11. საქართველოს პარლამენტის დადგენილება „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს კონვენციის დამატებითი ოქმის (ზედამხედველობით ორგანოებთან და მონაცემთა ტრანსსასაზღვრო გადადინებასთან დაკავშირებით) რატიფიცირების თაობაზე, საკანონმდებლო მაცნე, 27/07/2013;
12. საქართველოს გენერალური პროკურორის №9 ბრძანება საქართველოს გენერალური პროკურატურის თავდაცვის სამინისტროში, იუსტიციის სამინისტროსა და სპეციალურ პენიტენციურ სამსახურში გამოძიების საპროცესო ხელმძღვანელობისა და ოპერატიულ-სამძებრო საქმიანობაზე ზედამხედველობის დეპარტამენტის დებულების დამტკიცების შესახებ, საკანონმდებლო მაცნე, 26/12/2019;

უცხოენოვანი:

1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.01.1981,<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37> [წვდომის თარიღი: 02.11.2020];
2. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, Strasbourg, 08/11/2001, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181>[წვდომის თარიღი: 02.11.2020];
3. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016L0680>[წვდომის თარიღი: 06.11.2020];
4. The Council of Europe, Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, <https://rm.coe.int/168062dfd4#_ftn1> [წვდომის თარიღი: 02.11.2020];
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement

of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046> [წვდომის თარიღი: 02.11.2020];

6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504> [წვდომის თარიღი: 02.11.2020];
7. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, 15 December 1997, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31997L0066> [წვდომის თარიღი: 02.11.2020];
8. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 12 July 2002, [წვდომის თარიღი: 02.11.2019];
9. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), <https://eur-lex.europa.eu/legal-content/EN/TXT/ELI/?eliuri=eli:dir:2009:136:oj> [წვდომის თარიღი: 02.11.2020];
10. Treaty on the Functioning of the European Union, Article 16, Official Journal C 326 , 26/10/2012 P. 0001 – 0390, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT> [წვდომის თარიღი: 04.03.2020];
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), Official Journal of the European Union L 119/1, < https://eur-lex.europa.eu/eli/reg/2016/679/oj>, [წვდომის თარიღი: 04.03.2020];
12. Charter of fundamental rights of the European Union, Article 8, Official Journal C 364 , 18/12/2000 P. 0001 – 0022, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000X1218%2801%29> [წვდომის თარიღი: 04.03.2020];

სამეცნიერო ლიტერატურა

1. ხოდელი მ., სადისერტაციო ნაშრომი „სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით)“,

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი იურიდიული ფაკულტეტი, 2019 წელი, გვ.245;

2. ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, გვ.227;

სასამართლო გადაწყვეტილებები

1. საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება, N 1/1/625, 640, საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები - გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა - საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“, ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ, ქ.ბათუმი, 14 აპრილი, 2016;
2. საკონსტიტუციო სასამართლოს №2/1/484 გადაწყვეტილება საქმეზე: „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე თამარ ხიდაშელი საქართველოს პარლამენტის წინააღმდეგ“, ქ. ბათუმი, 2012 წლის 29 თებერვალი;
3. საკონსტიტუციო სასამართლოს პირველი კოლეგიის №1/3/407 გადაწყვეტილება საქმეზე: „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე-ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ“, ქ. ბათუმი, 2007 წლის 26 დეკემბერი;
4. Judgment of the Court (Grand Chamber) of Maximillian Schrems v Data Protection Commissioner, Case C-362/14, 6 October 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362, [წვდომის თარიღი: 07.03.2020];

Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 62-65 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

ATTACKS ON WIRELESS NETWORKS AND THEIR PREVENTIONS

უსადენო ქსელზე ორიენტირებული თავდასხმები და მათი პრევენცია

გიორგი იაშვილი -კავკასიის უნივერსიტეტი

Giorgi Iashvili – Caucasus University

გიორგი მელაძე - კომაროვი

Giorgi Meladze - Komarovi

გეგი ჩაჩიბაია -კომაროვი

Gegi Chachibaia-Komarovi

ლაშა ჯანჯალაშვილი - 1 კლასიკური გიმნაზია

Lasha Janjalashvili – 1 Classic Gymnasium

გეგა შავდათუაშვილი - აია -Gess

Gega Shavdatuashvili Gess

ABSTRACT. This article distinguishes between wireless (wifi) and wired networks, in particular, discusses the pros and cons of wireless and wired networks, and provides recommendations for their relatively more secure use.

აბსტრაქტი. მოცემული სტატია განასხვავებს უსადენო (wireless-wifi) და სადენიან (wired) ქსელებს, კერძოდ განიხილავს უსადენო და სადენიანი ქსელების უსაფრთხოების მინუსებს და პლიუსებს, ასევე მოცემულია რეკომენდაციები მათ შედარებით მეტად უსაფრთხოდ გამოყენებისთვის

საკვანძო სიტყვები: *Wireless-Wifi(უსადენო), Wired(სადენიანი).*

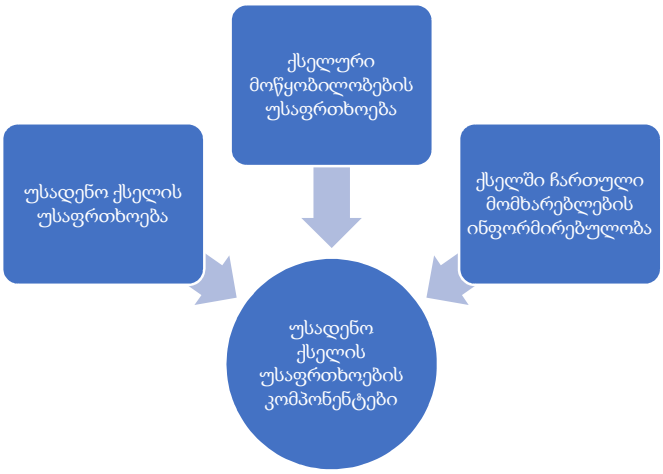
KEYWORDS: *Wireless-Wifi, Wired.*

შესავალი

XXI საუკუნე ტექნოლოგიების საუკუნეა, ტექნოლოგიის დაკავშირება სამყაროსთან კი სწორედ ქსელის გავლით ხდება. გამოყოფენ ქსელის 2 ძირითად კატეგორიას სადენიან (Wired) და უსადენო (Wireless) ქსელებს. ორივეს გააჩნია თავისი დადებითი და უარყოფითი მხარეები, რაც მომხმარებლის კომფორტულ ინტერესებზეა დამოკიდებული.

უსადენო ქსელის უსაფრთხოების კომპონენტები

უსადენო ქსელი იმდენად დაცულია, რამდენადაც უსაფრთხოა ქსელური მოწყობილობები და კომპიუტერები, ამასთან გათვითცნობიერებულია ამ ქსელში ჩართული ყველა მომხმარებელი. აქ საუბარი არ არის თუ რომელი უფრო მეტად მნიშვნელოვანია – საერთო ჯამში ზემოთქმული სამივე კომპონენტი ადგენს უსადენო ქსელის დაცულობის დონეს.



“wireless “ ქსელის მოწყვლადობის მთავარი კომპონენტია ქსელში ჩაბმული მოწყობილობების დაცულობა. მაგალითად შეგვიძლია ავიღოთ სისუსტეების შემცველი როუტერი, რომელსაც შეუძლია მთლიან ქსელს შეუქმნას საფრთხე, თუნდაც მოწყობილობაში არსებობდეს ძლიერი ფაიერვოლი და ამასთან უსაფრთხოების განახლებები.

ქსელური უსაფრთხოების კომპონენტებია ასევე კომპიუტერები და ის მოწყობილობები რომლებითაც ვუკავშირდებით ამა თუ იმ ქსელს. არსებობს უამრავი ქეისი სადაც დაუცველმა მოწყობილობამ დიდი რაოდენობის ზარალი მიაყენა ამა თუ იმ კომპანიას. მაგალითისთვის:

https://www.nytimes.com/2005/08/17/technology/virus-attacks-windows-computers-at-companies.html

ბოლო და ერთ-ერთი მნიშვნელოვანი კომპონენტია – მომხმარებელი – მოხმარებელმა საჭიროა ზუსტად იცოდეს, თუ როგორ გამოიყენოს wifi ქსელი უსაფრთხოდ, რადგან რისკი იმდენად მაღალია, რომ wifi-ს პაროლის გაზიარების შემთხვევაში შეუძლებელი ხდება ქსელი დაიცვა თუნდაც უახლესი ფაიერვოლით და როუტერით.

Wireless ქსელის უსაფრთხოების მთავარი გამოწვევები

უსადენო ქსელის ძირითადი შიდა და გარე გამოწვევები მოიცავს შემდეგს:

- უცხო პირები რომლებიც უსადენო ქსელის „გატეხვას“ ცდილობენ:
- Brute-Force შეტევა პაროლის ამოსაცნობად როგორც მოწყობილობაზე ისე WiFi-ზე
- შიფრაციის სისუსტეების გამოყენება
- მოწყობილობის სისუსტეების გამოყენება
- არასწორი კონფიგურაცია

- ფიშინგ შეტევა (მაგალითად, ზარი საფორთთან ასეთი შინაარსის ტექსტით, საკონფერენციო ოთახში ვარ და პაროლი დამავიწყდა. შემახსენეთ პაროლი თუ შეიძლება)

სტუმარი, რომელსაც WiFi სჭირდება

კომპანიის თანამშრომლები:

- ფიშინგ შეტევის ვერ გამოცნობა და მონაცემების გაცემა
- დავირუსებული ბარათების შეერთება კომპიუტერში და ვირუსების ქსელში გავრცელება
- მიღებული „ლეგიტიმური“, რეალურად ვირუსული ფაილების გახსნა
- ქსელში ჩართული მოწყობილობის ღიად დატოვება
- ქსელთან დაკავშირებული პორტატული (მობილური, ლეპტოპი) მოწყობილობის დაკარგვა

ქსელის დაცვა თანამედროვე მიდგომებით

ცხადია , რომ სადენიანი ქსელების შემთხვევაში, რისკი ფიზიკური კონტაქტისა უნდა იყოს მინიმუმამდე დაყვანილი. სადენიან ქსელზე წვდომის მოპოვება მხოლოდ ფიზიკურად დაკავშირებით შეიძლება და აშკარაა რომ ეს მისი უსაფრთხოების აუცილებელი და ყველაზე მთავარი შემადგენელი ნაწილია. მოწყვლად ადგილებში კი საჭიროა დაყენდეს სათვალთვალო სისტემები (კამერები).

სხვადასხვა რეკომენდაციებიდან გამომდინარე, რომ შევაჯამოთ რეკომენდირებულია რომ ერთ ცალკეულ კომპანიაში არსებობდეს ორი ან ორზე მეტი უსადენო ქსელი. ვინაიდან აუცილებელია თანამშრომლები, სხვა მომხმარებლებისგან იზოლირებულ ქსელში იყვენენ ჩაბმულნი.

ცალკეულ შემთხვევებში, ქსელების იზოლირებისთვის კომპანიები იყენებენ რამდენიმე უსადენო ქსელს, რომლებზეც მხოლოდ ადამიანთა კონკრეტულ ჯგუფებს აქვთ წვდომა.

თანამედროვე წვდომის წერტილებს გააჩნიათ - თაღლითი წვდომის წერტილების (rogue AP) აღმოჩენის, დაბლოკვისა და გათიშვის საშუალება. მაგალითისათვის კი მათ აქვთ საშუალება აღმოაჩინონ აუტორიზებული უსადენო ქსელის მსგავსი სახელის მქონე ჰაკერის მიერ ჩართული არააუტორიზებული უსადენო ქსელი და დაბლოკონ ის. რისკების შესამცირებლად, რეკომენდებულია ძველი Access Point-ების ახლით ჩანაცვლება.

ქსელური თავდასხმების პრევენცია

ქსელს უნდა იცავდეს თანამედროვე შესაძლებლობების მქონე ფაიერვოლი, ქსელური მოწყობილობები და კომპიუტერები დაცული იყოს, თანამშრომლები კი – ინფორმირებულნი. უფრო დეტალურად:

- ქსელური მოწყობილობები ფიზიკურად უნდა იყვნენ დაცული (რთულად ხელმისაწვდომ ადგილას);
- ქსელურ მოწყობილობებს უნდა გააჩნდეთ ძლიერი პაროლი, რომელიც არავითარ შემთხვევაში არ იქნება "Default";
- წვდომის წერტილები ისე უნდა იყოს განაწილებული რომ ტალღების გავრცელება რაღაც საზღვრებს მიღმა იზღუდებოდეს;
- WiFi იმდენად არის დაცული, რამდენადაც ძლიერია მისი შიფრაცია, პაროლი კი – გრძელი. ამიტომ WiFi-ს უნდა ჰქონდეს 10 ან მეტი სიმბოლოსგან შემდგარი რთული პაროლი, რომელიც დაცულია WPA2 (ან თუ მხარდაჭერა აქვს უახლესი WPA3) პროტოკოლით;
- დისტანციური კავშირის დროს, საჭიროა კომპანიის კუთვნილი, ან მის მიერ დაშვებული მომწოდებლის VPN-ის გამოყენება;
- ქსელურ მოწყობილობებზე განახლებები და პატჩები უნდა დაყენდეს დროულად;
- აუცილებელია შეღწევადობის ტესტირების ჩატარება წელიწადში ერთხელ მაინც;
- კომპანია დაცული უნდა იყოს ოფიციალურად შეძენილი ანტივირუსით;
- აუცილებელია თანამშრომლების ინფორმირებულობა და ტრენინგები ;
- მიუხედავად იმისა, რომ დიდ შრომას და ადამიანურ რესურს მოითხოვს მნიშვნელოვანია MAC მისამართის ფილტრაცია და ე.წ White List-ის შექმნა.

დასკვნა

მიმოვიხილეთ სადენიანი და უსადენო ქსელები, მათი დადებითი და უარყოფითი მხარეები, შევაჯამეთ მათი მნიშვნელობა დღევანდელობაში და მათი უსაფრთხოების აუცილებლობა, მათ შორის თუ რა ზომები უნდა გატარდეს თავდასხმების პრევენციისთვის.

Acknowledgement

The work was conducted as a part of SPG-19-133 financed by Shota Rustaveli National Science Foundation of Georgia.

ბიბლიოგრაფია

1. Computer Networking: A Top-Down Approach (6th Edition) – Kurose and Ross
2. Wireless Networks by Clint Smith and Daniel Collins (2014)
3. Wireless Networking Absolute Beginner's Guide by Michael Miller (2013)
4. S Gnatyuk, V Kinzeryavyy, M Iavich, D Prysiazhnyi, K Yubuzova, High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks, ICTERI Workshops, 657-668

Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 66-73 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

SECURITY ISSUES FOR DIGITAL TECHNOLOGY ENTREPRENEURSHIPS AND STARTUPS

Tinatin Mshvidobadze
Professor Gori State University (Georgia)

ABSTRACT: The unprecedented digital revolution has transformed the meaning and forms of entrepreneurship across the globe. In this article is proposed a conceptualization and characterization of three different phenomena: technology entrepreneurship, digital technology entrepreneurship, and digital entrepreneurship. Each of them has different origin and different emergence dynamics, and in most cases, they generate rather different trajectories for growth and technology evolution.
It is shown the different cybersecurity trends and threats for Startups.

KEYWORDS: *Entrepreneurship, startup, digital technologies, cybersecurity, sensors.*

INTRODUCTION

This article is focused on the identification and description of technology entrepreneurship in times of digitization. Based on current examples, we identify and describe characterizations of technology entrepreneurship, digital technology entrepreneurship, and digital entrepreneurship.

According to the MacInnis approach, we describe the different types of technology entrepreneurship and their characteristics. On this basis, we propose and discuss conceptual differentiation[1].

The overwhelming focus on technologies innovation might acquire an ambiguous meaning when related to startups [2]. Firms operating into the so-called traditional sectors of Western countries often exhibit higher growth rates than firms placed at the technological border.

The incoming of digital technologies in the realm of entrepreneurship represents a new challenge for entrepreneurs and policy makers. When applied to manufacturing, digital technologies (such as social media, mobile computing, data analytics, 3d printing, cloud, and cyber solutions) lead to a remodeling of productive patterns originating new market opportunities, higher revenue streams, faster time-to-market, enhanced service provision, and increased productivity [3]. Moreover, digital technologies also deeply modify the boundaries of products and processes, in doing so transforming the nature of uncertainty inherent entrepreneurial processes and outcomes, as well as the ways of dealing with such uncertainty. All these changing's are shifting the traditional way of creating and doing business, determining the emergence of a new specific type of entrepreneurship, the *digital entrepreneurship*[4]. specific digital knowledge base and ICT markets, the creation of digital business environments, an easier access to finance facilitations, the diffusion of digital skills, the creation of e-leadership, and the creation of entrepreneurial culture. These complex aims assume a heuristic and wide-ranging approach that, presumably, requests a reconsideration of the logic that leads to the emergence and development of startups operating in the digital setting.

The innovative and entrepreneurial critical processes become linked to the entire external environment, considered as a place of aggregation of individuals, companies, individual talents, institutions and support services. This feature is consistent with the needs of digital entrepreneurship, where the most important

productive factors are the availability of specialized personnel, of venture capitalists, and knowledge generation sources. To be placed in an ecosystem also could help all the memberships companies to obtain legislative rules that ensure, for example, the ownership of the innovations introduced and the cybersecurity of client companies, in doing so encouraging the adoption of the same technologies [5].

Implications for Digital Technology Entrepreneurship

A significant contribution to the definition of technology entrepreneurship as a field was made by Tony Bailetti [6]. His definition not only changed how organizations connect with users, but also transformed the importance of technology entrepreneurship.

Studies by Davidsson and Brush have shown that the type and nature of technology opportunities can be a key factor in driving the entrepreneurial process[7]. According to Nambisan, digital entrepreneurship is much closer to information systems' concepts of artefacts, platforms, and information infrastructure. Digital technology entrepreneurship refers to technology: its products are technological [8].

Table 1 provides some examples of entrepreneurial firms that can identify the differences between types of technology entrepreneurship. The proposed typology, as Drori points out, aims to connect traditional science-based technology entrepreneurship with university intellectual property[9] to new and rapidly developing Internet-based digital startups.

According to Fauchart, each of these types of firms may respond to specific entrepreneurial motivations towards their founders, which may reflect a combination of multiple entrepreneurial identities or specific dominant identities [10]. However, digital entrepreneurs are expected to be able to sell their players to a larger player, effectively transferring their customer base to the new firm.

Digital technology entrepreneurs, unlike digital entrepreneurs, do not rely solely on the innovative ecosystem. They strategically combine technological product knowledge with consumer know-how. From an academic perspective, researchers could use the different classifications of entrepreneurship to learn more about the personal motivations of entrepreneurs and their founding behaviours, financing preferences, etc.

Westerlund, Leminen, and Rajahonka [11] describe the example of new entrants in the Internet of Things (IoT) ecosystem, where the lack of structure and solid standards in the ecosystem increase the complexity of entrepreneurs’ decisions.

Typology	Example	
Technology Entrepreneurship	Fractus (www. Fractus.com)	Started as an academic spin-off, Fractus was a pioneer in the development of internal antennas for smartphones. They first attempted to commercialize their new antenna designs as a finished product, but then realized that it made more sense to just focus or R&D, patenting and licensing their technology to manufacturers and OEMs such as Nokia, Samsung, or Motorola.
	Oryzon Genomics (www.Orizon. Com)	Founded by bio-pharmaceutical researcher's Oryzon's first decade of operations was focused in offering genomics diagnostics. The company took-off in 2008 when it shifted its focus developing proprietary drug candidates and licensing to large pharmaceutical such as Roche.
	Rust Patrol (www.rustpatrol.com)	The technology was invented by a chemistry professor, and it offered a potential alternative a solution to address metal corrosion. A decade later, in 2014, two students joined the researcher to successfully start commercializing anti-corrosion products for industrial and consumer needs.
Digital Technology Entrepreneurship	Go pro (www. gopro .com)	Founded by surfer frustrated with the limited options he had to take nice action shots, Go pro become a manufacturer of action cameras and created a new category in the market. It is good example of user entrepreneurship.
	Fitbit (www. fitbit .com)	Started by a team IT professionals that identified the untapped potential of sensors and wireless technologies, it transformed from being a consumer electronics to a digital healthcare company.
	Tesla (www. tesla.com)	First a hobby electric car, it was one of the rare successful attempts to build an electric sports car from scratch. In a few decades, it has become a disruptor in the automotive industry, challenging the innovation pace and accelerating the technological development of electric vehicles.
Digital Entrepreneurship	Air bnb (www.airbnb.com)	What started as an idea to make a bit of money by renting space in an apartment, quickly become a popular site for people to share and find accommodation. After failing to attract business angels, it was only after being part of an acceleration program in 2009 that is started to gain traction as an accommodation-sharing platform
	Just Eat (www .just-eat.com)	An attempt to make takeaway ordering an option for al types of restaurants in 2001 was the birth of one of the largest networks of international restaurants that offers online ordering in an increasing number of countries around the world.
	Dropbox (www.dropboxs.com)	The idea of having a user's files synchronize in the cloud was behind in the digital storage company that has successfully competed with the largest software firms. Since 2009, when the competitive treat of the iCloud arose, they have managed to keep growing what was once a feature into a full product line for consumers and businesses.

Table 1. Examples of different types of technology and digital entrepreneurship

The successful I-Corps program (http://www.nsf.gov/i-corps), implemented by the National Science Foundation in the United States, it is a remarkable example of how digital technology entrepreneurship also activates new policies and support mechanisms. The digital core of new technologies allows for accelerated approaches to market validity and early growth.

One of the most quoted scholar, Audretsch DB. of entrepreneurship states that new firms do not always have an innovation propensity higher than incumbent firms, "even for a developed country such as the United States, only a very small fraction of new startups is really innovative" [12]. Without innovative capacity, in a contestable market, these firms have limited chance to grow.

As researchers agree to sustain that the entrepreneurial process is the result of a complex interaction between individuals, cultural, social, and environmental factors, the alternative that is intended to endorse and concentrate efforts on entrepreneurs/aspiring entrepreneurs who show the best business plans, the preeminent entrepreneurial features, and the ability to withstand market difficulties [13,14].

These entrepreneurs have the higher probability of founding and managing entrepreneurial ventures.

The concept of startup

Consistent with the pillar of Schumpeterian theories, the focus of a startup is expected to be on innovation. Innovation understood as a positive change compared to a pre-existing situation, therefore not only technological but also managerial, organizational, productive, or technical, that allows and sustains a company in the proposition of a profitable business model.

As reminded by Blank [15], a scalable startup created from the very beginning by founders who believe that their proposal could change the world.

A Consistent with Blank, a scale ups can be framed as fast growing startups that have already overcome some phases on which the activity of the startup is focused. A scale up stands out for some parameters attesting its success like market traction, 1–10 million € turnover annually, at least 1 million users (in the b2c), 20% growth in revenues or headcount for 3 years running after at least 10 people and $ 1 million in revenues, and 20% of the turnover from the foreign market [16].

The incoming of digital era certainly is a source of uncountable opportunities. A new wave of economic openings linked to the Industry 4.0, where digital platforms will be coupled and connected with sophisticated infrastructures of sensors, cyber-physical systems, and robots, is expected [17]. In this perspective, according to Brown and Mason [18], this possibility is linked to the capacity to create a specific business environment consistent with scale ups needs. Only when effectively planned, this framework provides consistent outcomes. In Italy, for instance, the low number of scale ups created is not believed to depend on the lack of quality startups but mainly on their need to move abroad to find sufficient risk capital investments for tackling scaling, as well as for the shortage of connections with external actors.

By Brown and Mason recommended, new policy measures are requested, as the environments in which scale ups prosper are distinct from those which have high rates of startups [19] .

To this purpose, the necessity to create a distinctive type of supportive economic and social framework emerges to establish steady and productive relationships among all the local stakeholders; to provide relational forms of support, instead of money-based facilities that have showed limited impact [20]; to attract different businesses funding resource targeted to the specific requirements of the businesses; to nurture the developing of the innovation system joining local customers end users, suppliers, universities, and so on ; to guarantee the recognition of unprotected and open sources innovations, respect on technological innovations and the protection of intellectual property rights; and to limit its action at regional or local level by Bosma NS, and Sternberg R. [21]. As by Isenberg DJ. The specific environments and specialized resource scale ups and HGFs need are usually defined in ecosystems[22].

An ecosystem for the emerging of scale ups

In the last decade, the *entrepreneurship ecosystem approach* has emerged as response for the propagation of scale ups and HGFs in general.

Evidence shows that ecosystems have typically emerged in places that already have an established and highly regarded knowledge base which employs significant numbers of scientists and engineers. Universities, research and corporate R&D laboratories are a primary source of skilled personnel who can found innovative startups [23]. Anyway, sometimes the substantive disconnection between universities and their surrounding local entrepreneurial and innovation ecosystem belittles entrepreneurial spillovers from universities.

Three types of services facilitating the process of business startup and growth by enabling new firms to focus on their area of expertise can be highlighted: specialist business services (law, marketing, accountability, management, consultants familiar with the unique needs of technology startups, technology marketing and assessment consultants, and PR firms), technical services offering precision machining, prototyping, testing, and so on, finance providers, such as venture capital firms or investment banks.

The digital technologies

According to EC (European Commission) With specific regard to digital startups, "the biggest transformation in business the world has seen in over a century" [24], they are radically changing the way people live, work, communicate, and play. Their pervasive diffusion is also causing significant repercussions on the dynamics of companies in European countries: 2.6 new digital job for each job destroyed is expected, manufacturing can achieve growth from 15 to 20% by 2030 if digitalized, revenue coming from digital technologies will growth of 2% for year, big data technology and services are expected to grow worldwide to USD 16.9 billion in 2015 at a compound annual growth rate of 40%, while companies using that data become 5–6% more productive.

Consequently, by proceeding with digital technologies adoption and implementation, an almost infinite number of economic opportunities for existing or new ventures is emerging, waiting to be grasped. Even more by considering that the boundaries of digital technologies in the three interrelated components of digital artifacts, platforms, and infrastructures are still unexplored, and every innovation such as cloud computing, data analytics, online communities, social media, 3D printing, and digital maker spaces contains indefinite applications.

In this way, the traditional funding gaps for new businesses, particularly in technology sectors, normally looking for small amounts of finance, can also be easily filled.

An ecosystem guarantees the passage of the traditional business environment to one no longer linked to individual or company factors but to a network of specialized partners with a wide availability of knowledge and open innovations.

Not by chance, some authors 24 put cities as the key organizing unit for innovation, entrepreneurship, and economic growth and argue about how digital startups and scale ups may take in place in cities and, sometime, require them as preferential ecosystem that help lever their development [25].

The different cybersecurity trends and threats for Startups

Establishing trust as a startup can be a long and demanding process. Cybercriminals target startup businesses because security measures may not be fully in place yet. Customer trust is critical in a time of widespread cybercrime and data privacy attacks. Startup owners now face the challenge of building consumer confidence as they build their business.

Cyberthreats and privacy issues can seriously affect enterprise. Recent studies show that 87% of consumers will do business elsewhere if a company is untrustworthy.

Recommendations for cyber security

1. Get the latest Cybersecurity Software - Hackers are devising more ingenious ways to break into systems and infect it with malware or steal data. Get the best and latest cybersecurity software you can get.

There is a lot of reliable security software recommended by experts that have a vast network enabling them to discover the latest malware attacks and develop bug fixes and security patches right away for their users.

2. Use a Robust Internet Security Suite and Firewall - With such a program, you can prevent accidental downloading of malicious software, and better detect and stop attacks like MITM (Man in the Middle), phishing, Trojan malware, and the like.[1]

3. Install SSL (Secure Sockets Layer) Certificate - It is a standard security protocol to install an SSL or Secure Sockets Layer. Trust brings in higher web traffic, and higher web traffic drives sales. 85% per cent of online customers say they refuse to purchase from a website with no SSL certificate. Site URLs that start with HTTPS can encrypt standard HTTP requests for a more secure shopping experience.

4. Set Up a Secured Cloud Storage -Cloud-based storage and back-up solutions add another layer of security to your business.

5. Create a Culture of Cybersecurity in Your Team- It is about building a culture of security protocols in your team.

6. Use Strong, Complicated Passwords - Every member needs to have their own network account. Require this from your customers as well.

7. Require your online vendors to prioritise security.

Conclusion

A flourishing entrepreneurship research stream believes that a chance to reach the above objectives lies in the ability to implement specific business environments called ecosystems. These are targeted on selective measure supporting the emerging of ventures with innovative business models but also their development and growth .

Moreover, the ecosystem needs to involve, since the beginning, many stakeholders/actors (at least an interested large corporation, policy makers, local bankers, and venture capitalists, people acting on the local culture, local universities, etc.) [26].

Nevertheless, both domains and actors are characterized by proximity and include hundreds of variables interacting in highly complex and idiosyncratic ways.

Beyond this theoretical-conceptual paper, aimed to connect the increasing sector of digital firms with a specific business environment, future surveys should focus their analyses at least on three directions. Firstly, a clear individuation of the needs and resources requested by digital firms and startups in the light of their own specificities; secondly, the detailed examination of the operative mechanisms of existing ecosystems precisely focused on digital technologies; and lastly, data management system and cybersecurity should be one of your company's top priorities.

[1] https://www.softvire.co.nz/kaspersky-total-security-2019-review/

REFERENCES:

1.MacInnis, D. J. 2011. A Framework for Conceptual Contributions in Marketing. *Journal of Marketing,* 75(4): 136–154. https://doi.org/10.1509/jmkg.75.4.136

2. Brown R, Mawson S, Mason C. Myth-busting and entrepreneurship policy: The case of high growth firms. Entrepreneurship & Regional Development. 2017;**29**(5-6).

3. EC (European Commission). Digital Entrepreneurship Scoreboard 2015. Brussels: Directorate-General for Internal Market, Industry,Entrepreneurship and SMEs; 2016.

4. Nambisan, S. 2016. Digital Entrepreneurship: Toward a Digital Technology Perspective of Entrepreneurship. *Entrepreneurship Theory and Practice,* (414): 1–27. https://doi.org/10.1111/etap.12254

5. Nambisan S. Digital entrepreneurship: Toward a digital technology perspective of entrepreneurship. Entrepreneurship Theory and Practice. 2017;41(6):1029-1055;

6.Bailetti, T. 2012. Technology Entrepreneurship: Overview, Definition, and Distinctive Aspects. *Technology Innovation Management Review,* 2(2): 5–12. http://timreview.ca/article/520

7.Davidsson, P. 2015. Entrepreneurial Opportunities and the Entrepreneurship Nexus: A Re-conceptualization. *Journal of Business Venturing,* 30(5): 674–695. https://doi.org/10.1016/j.jbusvent.2015.01.002

8.Brush, C. G., Manolova, T. S., & Edelman, L. F. 2008. Properties of Emerging Organizations: An Empirical Test. *Journal of Business Venturing,* 23(5): 547–566. https://doi.org/10.1016/j.jbusvent.2007.09.002

9.Hartmann, D. 2014. Turning Technology into Business Using University Patents. *Technology Innovation Management Review,* 4(12): 37–43. http://timreview.ca/article/856

10.Fauchart, E., & Gruber, M. 2011. Darwinians, Communitarians, and Missionaries: The Role of Founder Identity in Entrepreneurship. *Academy of Management Journal,* 54(5): 935–957. https://doi.org/10.5465/amj.2009.0211

11.Westerlund, M., Leminen, S., & Rajahonka, M. 2014. Designing Business Models for the Internet of Things. *Technology Innovation Management Review,* 4(7): 5–14. http://timreview.ca/article/807

12.Audretsch, D. B., Bonte, W., & Mahagaonkar, P. 2012. Financial Signaling By Innovative Nascent Ventures: The Relevance of Patents and Prototypes. *Research Policy,* 41(8): 1407–1421. https://doi.org/10.1016/j.respol.2012.02.003.

13 Autio E, Kenney M, Mustar P, Siegel D, Wright M. Entrepreneurial innovation: The importance of context. Research Policy. 2014;**43**(7):1097-1108.

14. Isenberg D. The Entrepreneurship Ecosystem Strategy as a New Paradigm for Economic Policy: Principles for Cultivating Entrepreneurship. Babson Park: Babson College; 2011.

15. Blank S. The Four Steps to the Epiphany: Successful Strategies for Products that Win. Pescadero (US) K & S Ranch; 2013.

16. ScaleIT. 2018. Available from: www. scaleit.biz/

17. EC (European Commission). Digital Transformation of European Industry and Enterprises. DG Internal Market, Industry, Entrepreneurship and SMEs; 2015

18. Brown R, Mason C. Inside the high-tech black box: A critique of technology entrepreneurship policy. Technovation. 2014;**3412**:773-784.

19. Mason C, Brown R. Creating good public policy to support high growth firms. Small Business Economics. 2013;**40**:211-225.
20. Lerner J. The future of public efforts to boost entrepreneurship and venture capital. Small Business Economics. 2010;**35**:255-264.
21. Bosma NS, Sternberg R. Entrepreneurship as an urban event? Empirical evidence from European cities. Regional Studies. 2014;**48**(6):1016-1033.
22. Isenberg DJ. How to start an entrepreneurial revolution. Harvard Business Review. 2010;**88**(6):41-49
23. Isenberg D. Worthless, Impossible and Stupid: How Contrarian Entrepreneurs Create and Capture Extraordinary Value. Cambridge: Harvard Business Review Press; 2013
24. Mason C. Public policy support for the informal venture capital market: A critical review. International Journal of Small Business. 2009;**27**:536-556
25. Lusch RF, Nambisan S. Service innovation: A service-dominant logic perspective. MIS Quarterly. 2015;**39**(1):155-175.
26. Isenberg DJ. How to start an entrepreneurial revolution. Harvard Business Review. 2010; **88**(6):41-49.

Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 74-78 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

MODELS AND METHODS OF WIRELESS DECENTRALIZED NETWORKS FOR ENERGY MONITORING OF CRITICAL INFRASTRUCTURE FACILITIES

Yuliia Kovaleva, 1-4 Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine
Tetiana Babenko, 1-4 Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine
Vira Ignisca 1-4 Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine

ABSTRACT: In this article, we describe the many models describing the dependence of power consumption on the operating modes of 802.15.4 / ZigBee devices at the MAC and NWK levels of the specification, it is not so much of practical interest to develop a realistic analytical model for predicting the lifetime of a system in IEEE 802.15.4 networks, taking into account the possible external impact on network, how much is the implementation of a new approach to building a reliable, fault-tolerant self-regulating autonomous decentralized network P2P architecture.

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

INTRODUCTION

Technological advances in microelectronics have enabled the mass production of miniature transceivers with extremely low power consumption that can be networked and communicated with each other using wireless communication channels. Autonomous networks of such devices are called wireless monitoring networks (WMN), which, in particular, emphasizes their main purpose - the collection of data from sensors (meters) for further analysis and transmission of control commands.

The change in the flows of active and reactive power caused by distributed generation has important technical and economic consequences for the distribution network, which makes it obvious the inconsistency of centralized approaches to the architecture of automated energy monitoring systems and actualizes the need to model processes in decentralized systems. A new approach to energy management in field equipment that takes into account the stochasticity of variables and adapts predictive models to compensate for data latency, signal latency, and disturbances in real time, allows you to create autonomous decentralized systems with a predictable lifespan and an acceptable level of service quality.

PROBLEM DEFINITION

Smart Metering is currently being implemented in the traditional energy system with an advanced communications network to collect meter readings to update the energy billing process. The implementation of these communication infrastructures and the associated Smart Grid applications is driving the rapid increase in data transmission in information networks. This, in turn, creates new problems: connection failures, delays in information transfer, data errors, etc., which are becoming more and more critical.

Extending network lifespan is a common goal of wireless research, as a network node is usually limited by the capacity of the power supply, which determines its lifetime. In works [1, 2], the concept of the energy value of a node was introduced, defined as the ratio of the total consumed energy to the initial energy of the battery. The value of a node is the higher, the less is the ratio of the energy expended by the

node when operating in the network to its initial energy. According to this model, the total energy consumption includes the energy spent on sending and receiving packets, sleep and sensing modes.

However, the authors did not consider additional sources of energy costs, such as packet control in the GTS mode and retransmissions caused by network interference. The latter is decisive, since with heavy traffic, the retransmission of "unsuccessful" packets leads to significant additional energy consumption, leading to a reduction in the network lifetime. The model proposed in [3] eliminates this disadvantage, but does not offer an analytical method for calculating the probability of a failed transmission. In [4], a model for predicting communication delays in the GTS mode is proposed. There is a direct dependence of the lifetime of a wireless monitoring network on its security, so the issue of the system's resistance to external interference is crucial. Considering the many models describing the dependence of power consumption on the operating modes of 802.15.4 / ZigBee devices at the MAC and NWK levels of the specification, it is not so much of practical interest to develop a realistic analytical model for predicting the lifetime of a system in IEEE 802.15.4 networks, taking into account the possible external impact on network, how much is the implementation of a new approach to building a reliable, fault-tolerant self-regulating autonomous decentralized network P2P architecture.

The European Commission has created a Smart Grid Task Force (SGTF). SGTF defines smart grids as electrical grids that can effectively integrate the behavior and actions of all users connected to it - generators, consumers and potential customers - to provide a cost-effective, sustainable power system with low losses and high quality and security of supply and safety [5]. The Smart Grid Model (SGAM) architecture [6] was proposed by the European Standards Organization as a reference model for Smart Grids (Fig. 1).

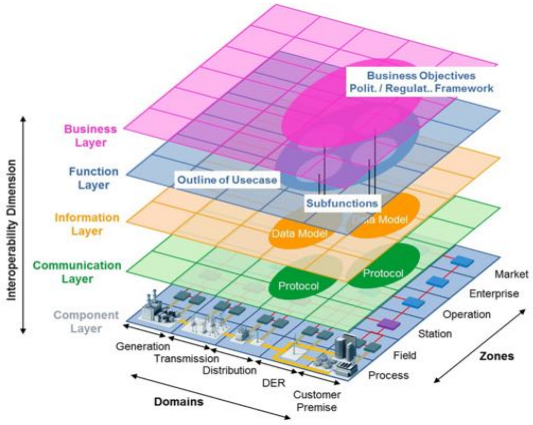


Figure 1. Reference architecture SGAM

The smart grid is transforming into an internet of energy, and blockchain technology can be a link between the smart grid and consumers, which will facilitate the active participation of end users in energy markets. The purpose of using blockchain technology in distributed control, management and verification of the implementation of demand control programs by intelligent energy monitoring grids is the need to ensure high reliability and decentralized operation by implementing instant transactions, protection against unauthorized access and demand regulation in real time. In this context, the smart grid represents peers coordinating their activities along the infrastructure chain in order to maintain decentralized demand and ensure stable network operation.

One of the main obstacles faced by smart metering today is data privacy and security, which in the case of blockchain is addressed using distributed block ledger functions. A distributed blockchain database is built and managed at the smart grid level. Each node is equipped with IoT-based meters that record controlled data in blocks within the blockchain. Thus, any node is a peer-to-peer distributed energy network node and can maintain a copy of the database that is automatically updated when new energy

consumption data is logged. The blockchain database consists of many blocks connected in a peer-to-peer chain and is held by the participants who decide to include data in the registry. The network is built by combining computers according to the principle of the same functions. That is, a computer receiving information is a server, and by transmitting information to the network it performs the function of a client. Networks of this kind operate on a peer-to-peer basis (originally peer-to-peer or P2P) and are called peer-to-peer or decentralized. Successful operation of WMN applications requires coordinated operation and management of a large number of distributed and loosely coupled field smart devices that identify and trust each other. Decentralization of the WMN infrastructure provides benefits, including a reduction in the amount of data transmitted to the Internet for processing and analysis, and improved security and confidentiality of information. Ensuring the validity of these operations means achieving a distributed consensus across the WMN field devices.

One of the biggest challenges in integrating blockchain into IoT is scalability. Due to the large number of devices and resource constraints, blockchain deployment in the IoT is particularly challenging. An optimal blockchain architecture must scale to many I / O devices (they become peers on the blockchain chain) and it must handle high transaction throughput.

Decentralization of the WMN infrastructure provides benefits, including a reduction in the amount of data transmitted to the Internet for processing and analysis, and improved security and confidentiality of information. Ensuring the validity of these operations means achieving a distributed consensus across the WMN field devices. Now three fundamentally different approaches to solving the problem of transferring and processing information by various platforms of existing solutions have been formed - the IBM Research solution based on Hyperledger Fabric technology [7], the IOTA consortium solution based on the Tangle protocol, which is based on DAG (Directed Acyclic Graph), and Qubic technology [8] and the advanced approach of the Radix project based on Tempo Ledger technology [9]. These approaches combine the ability to run on a wide variety of hardware, and a functional programming language allows for simpler analysis to prove code is correct and emphasizes parallelism, which means that different parts of a larger program can run concurrently to take advantage of multiple processors or even multiple processors. devices.

Proof-of-work (PoW) - The consensus mechanism is considered a highly energy-intensive technology. Given the importance of (PoW) - the consensus mechanism, IBM Research is developing a new method for implementing this mechanism using the computing power of devices of the Internet of Things
[10]

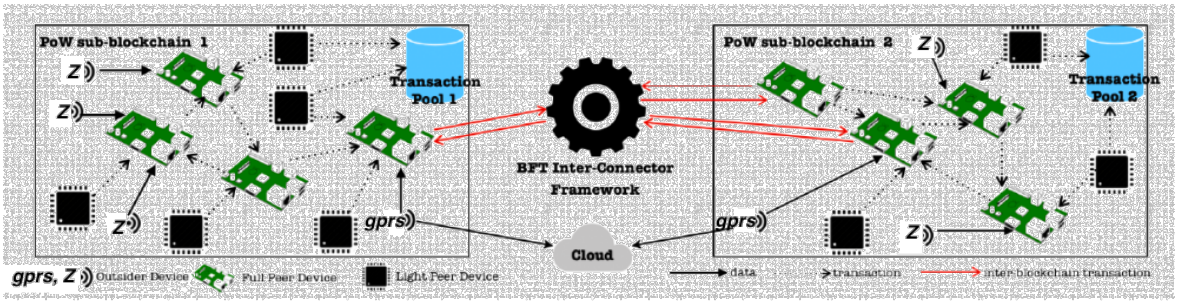


Figure 2. Hybrid WMN blockchain [8]

One of the biggest challenges in integrating blockchain into IoT is scalability. Due to the large number of devices and resource constraints, blockchain deployment in the IoT is particularly challenging. An optimal blockchain architecture must scale to many I / O devices (they become peers on the blockchain chain) and it must handle high transaction throughput. Hybrid-IoT, a platform developed by IBM Research, uses both PoW block diagrams and Bytantine Fault Tolerant (BFT) protocols to achieve

scalability. First, PoW block diagrams provide a distributed consensus among many IoT devices, peers on the blockchain in a clustered sub-blockchain. Hybrid-IoT uses the BFT inter-cluster interconnect framework to ensure mutual understanding between blockchains.

The chosen structure of virtualized I / O devices represented by Hybrid-IoT peers with different roles within a separate PoW blockchain proves the effectiveness of the PoW blockchain design, which also prevents security vulnerabilities.

IoT network devices have an extremely wide range of computing power and energy resources, and some of them cannot solve the complex problems provided by PoW. Dividing nodes into groups allows the algorithm to decide what proportion in each group should mine, depending on the amount of energy used by each node. In this model, only some of the nodes (nodes) implement full PoW. IBM found that when placing nodes in clusters of 250 units, only 7% of these sub-blockchains performed PoW, achieving the best results in terms of economy, scalability, and security.

IOTA, designed with scalability in mind, introduced the concept of a dedicated smart contract platform called Qubic, running on top of the core IOTA protocol. Individual Qubics are essentially quorum-based distributed computing tasks. Qubic uses the IOTA Tangle to package and distribute cubes from their owners to the oracles who will handle them. Technically, the Tangle method is an acyclic graph - it is a looping method where loops can be executed in parallel. Cubes can live on Tangle while dormant. When specific inputs become available or changed, they are "awakened" and processed, which can cause a cascade of other cubes to wake up as new results appear. This allows you to create a very dynamic programming environment that allows you to add new cubes at any time and bind them to any input. After the cube has been processed, the quorum reached, and the results sent to the Tangle, two things happen: 1) qubic goes to sleep again, waiting for the next input change, and 2) the cascade effect is triggered so that the dependent qubic unfolds and starts processing with new inputs. The technology assumes an economical mode of operation and is optimized for low power consumption and small amount of memory in field devices, which does not exclude large-scale calculations, especially those that can be parallelized and distributed over a large number of processors.

RADIX has proposed a peer-to-peer network of nodes with logical clocks to generate temporary evidence of the chronological order of events. Radix has achieved a solution to both problems in such a way that it does not need PoW (mining), it does not need PoS (proof of stake), and it does not need master nodes to confirm transactions. The system is secure by providing nodes with a historical record of the generated temporary evidence. RADIX DLT has linear scalability. This means that the more nodes added to the network, the more it will scale. Unlike current solutions, each node added increases the throughput of the Radix network. Radix will allow even resource-limited devices to participate as nodes on the network. The Radix node can be run on a device with a 16MB memory and a 100 MHz processor. This will make decentralization even more perfect.

Radix Tokens (RAD) uses decentralized leger technology (DLT) to record transactions. RadixDLT offers a system that improves, albeit different, blocking technology in terms of scalability. RadixDLT stores all transactions and orders in a protocol in a global distributed ledger called Tempo Ledger. This book consists of three main components: a network cluster of nodes, a global register database distributed across nodes, and an algorithm for generating a cryptographically secure record of temporarily ordered events.

CONCLUSION:

As blockchain technology develops, the most promising solution seems to be RadixDLT, since it is devoid of IOTA's drawbacks in terms of the cumbersome mechanism for implementing smart contracts and is not as demanding on hardware resources as IBM Hyperledger. In terms of hardware solutions, the most likely is the use of productive "light" nodes on low-power devices such as the Raspberry Pi, which are controlled by a Radix-based master node. This implementation does not imply the installation of the

central server of the system, and its synchronization is carried out by the master nodes, dispersed geographically. This increases the overall performance of the network, optimizes its power consumption and provides guaranteed resilience to various types of cyber attacks.

REFERENCE:

[1] Sofiane Ouni, Zayneb Trabelsi Ayoub/ Predicting communication delay and energy consumption for ieee 802.15.4/zigbee wireless sensor networks.- International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.1, January 2013. Pp. 141-152

[2] Eduardo Casilari, Jose M. Cano-García, Gonzalo Campos-Garrido/ Modeling of Current Consumption in 802.15.4/ZigBee Sensor Motes.- Sensors 2010, 10, 5443-5468; doi:10.3390/s100605443

[3] Bruno Bougard, Francky Catthoor, Denis C. Daly, Anantha Chandrakasan, Wim Dehaene/ Energy Efficiency of the IEEE 802.15.4 Standard in Dense Wireless Microsensor Networks: Modeling and Improvement Perspectives. - Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE'05)

[4] Jefferson Antonio Zeni Trevisan, Andre´ Augusto Mariano, Eduardo Parente Ribeiro/ Average Power Consumption Model For Wireless Sensor Networks.- Universidade Federal do Paraná. Av. Coronel Francisco Heráclito dos Santos, 210. Curitiba - PR - 81531-970 - Brazil. 1jtrevisan@ufpr.br. Доступ: www.inatel.br/.../82-averagepowerconsumptionmodelforwir...

[5] CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid Reference Architecture; 2012. [Online] Available at: http://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

[6] Smart Grid Task Force - EG1 Report, Interoperability, Standards, and Functionality Applied to Large Scale Smart Metering Deployments, October 2015.

[7] Gokhan Sagirlar, Barbara Carminati, Elena Ferrari, John D. Sheehan, Emanuele Ragnoli. Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-blockchains.- IEEE International Conference on Blockchain (Blockchain-2018), July 30 - August 03, 2018 Halifax, Canada https://arxiv.org/abs/1804.03903