SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

Vol6 No4
December 2022

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 6(4): 1-7 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

THE USE OF A SPECIALIZED COMPUTER GAME IN PRACTICAL CLASSES IN THE SPECIALITY CYBERSECURITY

Igor M. Kozubtsov, Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
Oleksii V. Silko, Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
Lesia M. Kozubtsova, Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine

ABSTRACT. The relevance of the research topic is due to the need for lecturers to find ways and technologies to maintain a high level of motivation and attention of students and cadets of the cybersecurity speciality in practical classes. Traditional methods and means, as practice shows, are not limitless. The main aspects of the work. The paper examines the existing best practices of the use of games by researchers in the educational process. Based on the positive results, it is proposed to develop specialized computer programs to increase the educational interest of students and cadets of the cybersecurity speciality in practical classes. Scientific novelty. The concept of building a training complex for training cybersecurity specialists based on a computer game is proposed for the first time.

KEYWORDS: *class, practical training, specialist, cybersecurity, computer game.*

INTRODUCTION:

With the advent of computer engineering, the motivation for traditional teaching methods began to fade paradoxically rapidly among students and cadets. Given the degree of declining interest among young people in technical (engineering) specialities and artificial demand for economic specialists, in modern market conditions, the problem of finding new approaches to the motivation of students and cadets has arisen.

To help solve this problem, gaming methods of adult education have come to the fore. Excessive use of a phone or tablet during training does not create a sense of compulsion in a person, but unfortunately, it covertly leads to gambling addiction – a disease of the XXI century.

However, this is not entirely true, since addiction increasingly arises from the game, game program, online games with which it connects the user [1]. There is nothing special about smartphones themselves that would cause addiction, but the real driving force of our attachment to these devices arises from the hypersocial environment in which a person lives in the modern world [2].

ANALYSIS OF RESEARCH AND PUBLICATIONS

An analysis of current research has shown that this issue has attracted the attention of quite a large number of scientists. Among the many publications, in relation to our subject of research, the following works are of great importance.

In work [3], an innovative idea of gamification of the higher education system through the introduction of computer games is proposed. In this paper, the hypothesis is laid that as a result of the introduction of game pedagogical technology for teaching electrical engineering disciplines by the method of virtual computer game, due to the interest shown by young people in computer games, a positive effect will be achieved in motivation and learning outcomes. The preliminary results served as the basis for the further development of the method of playing using a virtual computer during the independent training of cadets on training facilities [4].

It has been established that the use of gaming technologies in education (gamification) attracts the attention of a significant number of researchers.

"Gamification is an educational technology that is rapidly developing, having a huge potential to positively influence the effectiveness of the educational process" [5, p. 135]. According to V.Y. Buhaieva, gamification can be considered as a way of forming active professional behavior of future IT industry specialists.

Continuing to develop the idea of the prospects of gamification of higher education, it is interesting to note the opinion of researchers that:

"gamification is the concept of applying game mechanics and game design methods in a non–game context to attract and motivate people" [6, p. 25];

gamification reveals the possibility to consider the formal and informal space of the learner [7];

gamification allows you to build learning based on game methods and thus strategically improve learning and education [8].

In a separate group, it is possible to combine studies in which scientists consider gamification as a certain pedagogical technology: teaching [9]; innovative [10]; professionally-oriented learning [11].

A separate group of studies consists of the results of scientists, in which reflections on gamification are presented, namely:

on the advantages and disadvantages of gamification in online higher education [12];

as a warning to the modern and popular gamification process, the results revealed numerous risks in media practice [13].

Considering the abovementioned, we agree with the author that gamification is a trend of modern higher education [14] with many advantages and prospects, and at the same time excessive cybernetization of education makes it more vulnerable to cyber threats [15].

Problem statement and its connection with important scientific tasks. The result of the research analysis [3-15] showed that in modern pedagogy, the lecturer's problem of increasing the interest and motivation of students and cadets in cybersecurity by improvised means for the effective organization of the educational process remains relevant and unresolved. Taking into account the above, the authors have chosen this relevant area of research.

PURPOSE OF THE ARTICLE

To substantiate the concept of a training complex for training cybersecurity specialists based on a computer game.

To achieve the goal , the following tasks are set:

1. Analyze the current state of research and publications.

2. To develop a conceptual idea of using a computer game in the practice of training specialists in the field of cybersecurity.

MAIN RESULT OF THE RESEARCH

Until now, competitive (game) tasks are most used in the study of the processes of armed struggle.

With the advent of cyberspace, according to the authors [16], a new space for fighting has appeared – cybernetic.

In work [17], the researcher proposed the idea of considering the conflict of interaction of objects in cyberspace as a kind of model. Taking into account the classification of game theory problems [18, p. 221] and the strategy of a possible educational game in cyberspace [19], we can present this model in the form of the following Figure 1.

The main principle of gamification is to ensure the receipt of constant feedback from the user, providing the possibility of dynamic correction of his behavior [14].

The main aspects of gamification according to the researcher [14] are:

dynamics – the use of scenarios that require the user's attention and reaction;

mechanics – using scripted elements such as virtual rewards, statuses;

aesthetics – creating a general gaming experience that promotes the emotional involvement of the user;

social interaction is a wide range of techniques that ensure user interaction.

Gamification of the educational process, according to the author of the study [14] affects three areas of student behavior, namely:

– *cognitive* (the game contains a system of rules for players; provides solutions to specific problems adapted to the skill level of the player; the growth of difficulties contributes to the acquisition of appropriate skills by players; the content and organization of the game provide an opportunity for students to go different routes that allow players to choose their intermediate goals within the overall task);

– *emotional* (participation in the game allows players to experience different emotions from joy, pride in their achievements to disappointment. This is due to the fact that in order to acquire new knowledge, the player has to fail at some stage of the game. During the game, students' attitude to

mistakes changes (they have the right to make mistakes), they do not get a bad grade for an incorrect answer);

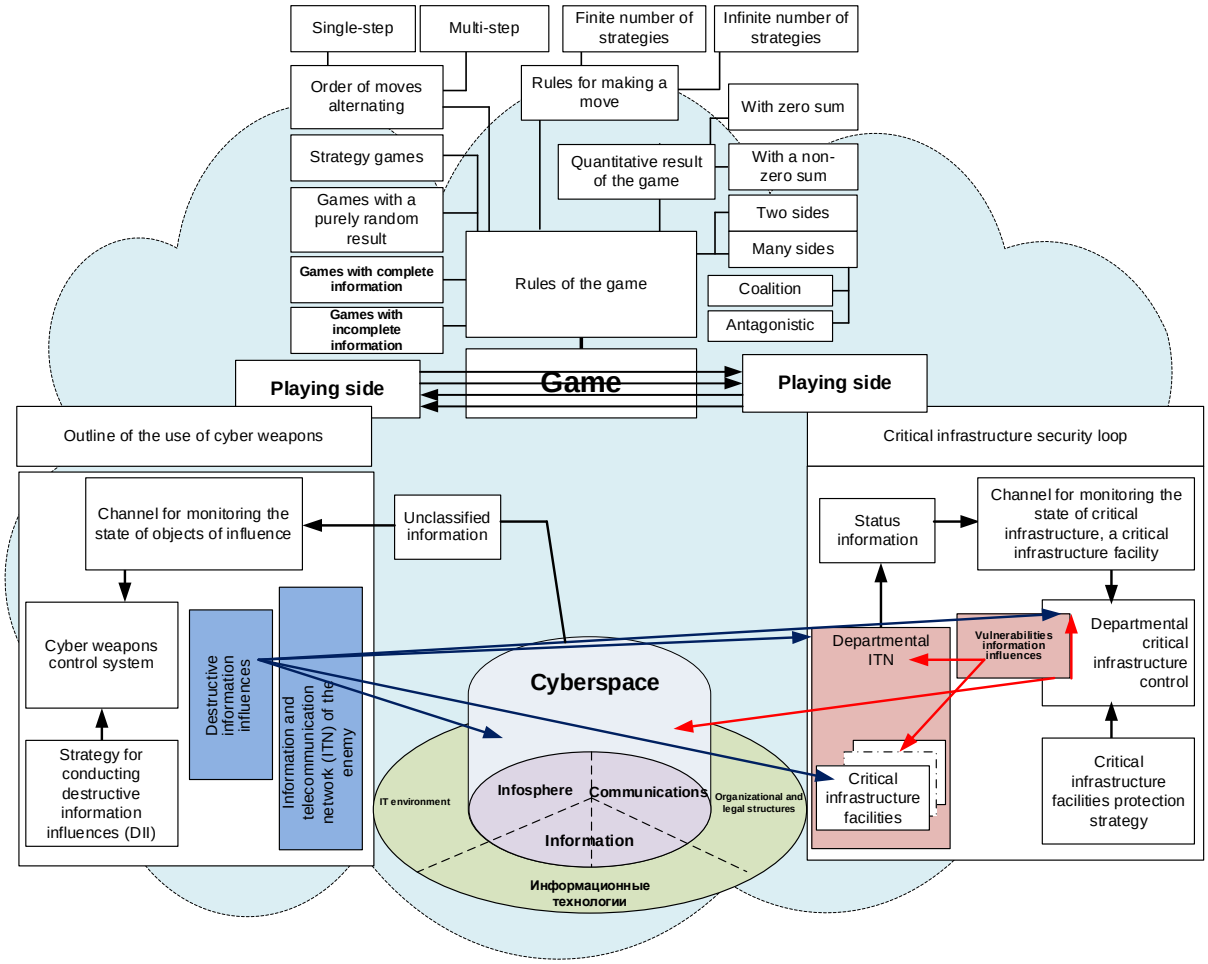


Figure 1 – A model of confrontation in cyberspace
taking into account the classification of game theory

– *social* (content of the game and its organization allow players to perform new roles and make decisions. Playing alone or in a team and performing various roles, players in the safe space of the game have the opportunity to form a willingness to work in team, dialog speech).

The game of cybersecurity, like any game, has certain rules that oblige all participants of the game to adhere to certain sequences, analysis and the choice of response algorithms, depending on the conditions of the tactical situation deployed on the virtual battlefield.

The value of the game cannot be exhausted and evaluated by entertainment and reactive capabilities [20]. The phenomenon of the game lies in the fact that, being entertainment, recreation, it is able to develop into study, into creativity, into a model of the type of human relations and manifestations in work.

In this study, it is proposed to consider the game from the point of view of the teaching method. Then the method of pedagogical play will be widely used in the development of military art, which means it will contribute to students and cadets in acquiring professional skills.

Unlike games in general [20], a controlled pedagogical game has an essential feature – a clearly formed learning goal and corresponding pedagogical results that can be justified, explicitly highlighted and characterized by an educational and cognitive orientation.

Taking into account the abovementioned, an educational model of the computer game "practical implementation of confrontation in cyberspace according to the rules of the ontology of

cybersecurity" is proposed, the functional model of which is presented in Fig. 2. On this model, it is possible to study (model) the influence of incoming processes in cyberspace.

By analogy to the work [20], we suggest that game software developers join the creation of a training game strategy for cybersecurity similar to the one used in computer games. Its emulation, like a computer game, is rationally used during practical training in the training of cybersecurity specialists.

The purpose of using the software product is for students and cadets to acquire primary practical skills in manual configuration of systems and components of a cybersecurity system. In addition, the game software product will be useful, for example, when configuring routers, firewall, etc. on a conditional educational information system (see Fig. 3).

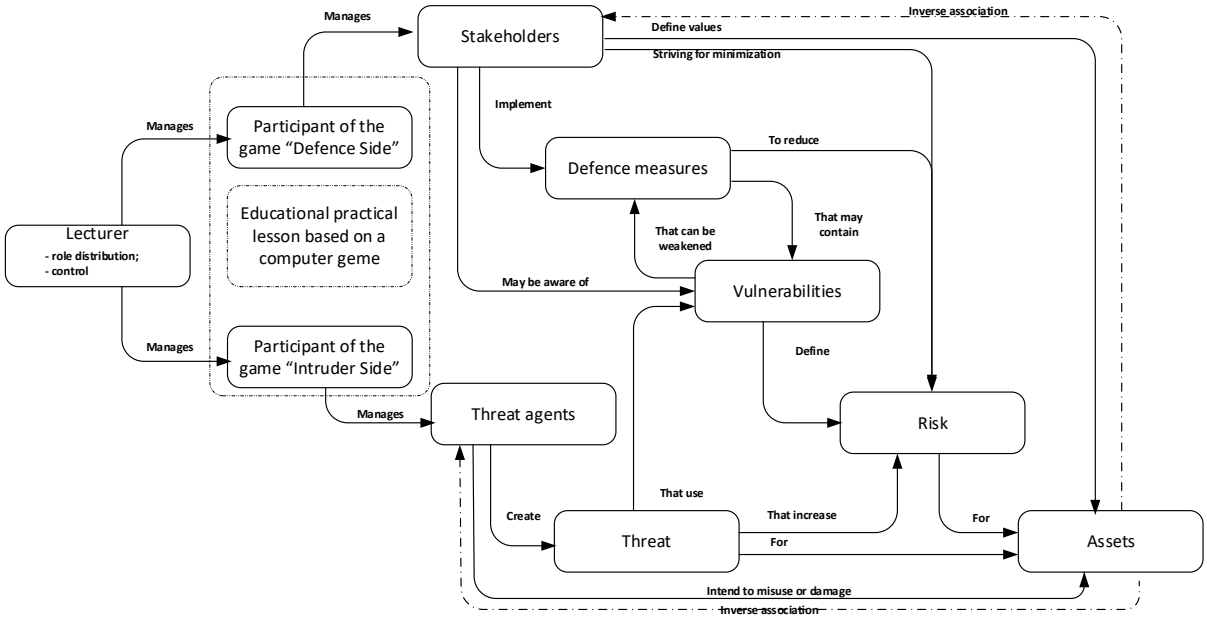


Figure 2 – Functional model practical implementation of confrontation in cyberspace according to the rules of the cybersecurity ontology

With the help of the game emulator, practical training of specialists in the field of cybersecurity can be carried out during training sessions:

arrangement of the workplace by a specialist;

on the speed of assembly / disassembly (block repair) of a computer, laptop;

simulate the settings of the access point to the components of the information and communication network (Fig. 3);

remote configuration of routers, firewall, etc.;

development of fast programming skills;

working out the algorithm for the commander's decision-making.

It is necessary to point out the main advantage when training specialists in the field of cybersecurity, which is that it is possible to preserve expensive equipment from damage as much as possible in case of erroneous actions of students.

Own modeling helps a cybersecurity specialist to clearly understand the sequence of elementary actions, study the construction of the network, understand the meaning of cyberspace protection in accordance with his sector of responsibility, develop a creative idea of searching for new contextual algorithms for implementing cybersecurity.

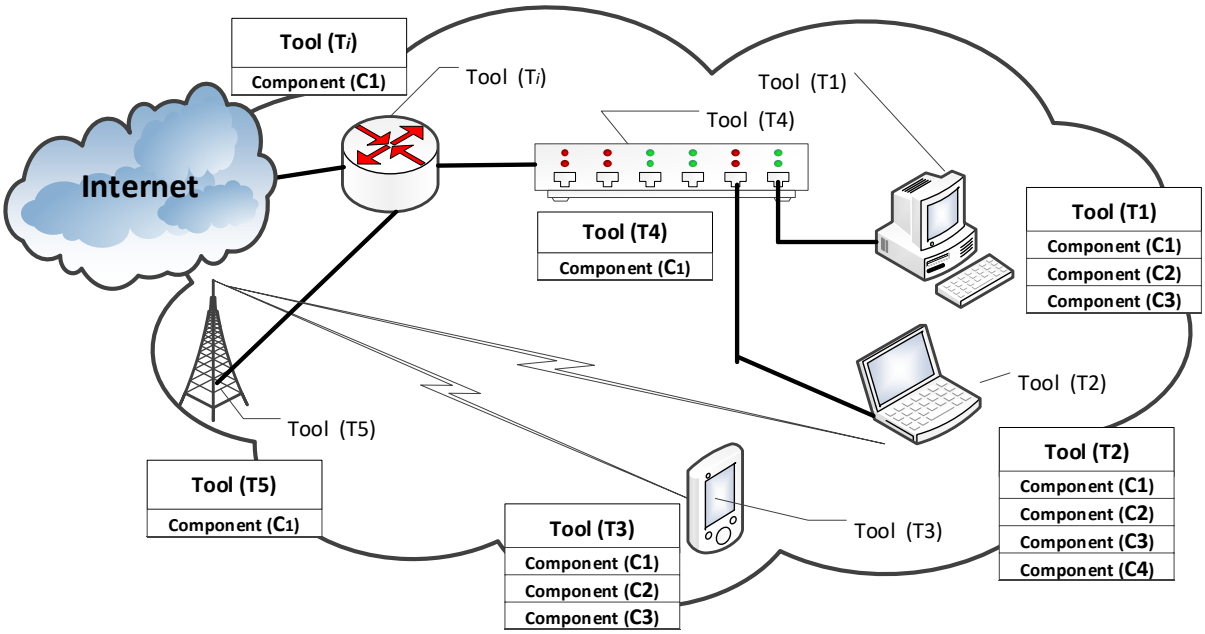


Figure 3 – A fragment of a conditional educational information system

The participant of the game "Intruder Side" under the guise of "Threat Agents" create educational cybernetic destructive informational effects if necessary to attack an enemy resource. At the same time, the participant of the "Defense Side" game, acting as a future specialist in the field of cybersecurity, should form a quasi-professional solution in the game that would neutralize the cybernetic destructive information impacts created by threat agents.

The result of the game will be the preservation of the integrity of the assets by the participants of the game "Defense Side".

So, the implementation of a computer game with a certain form of classes takes place in the following main areas[20]:

the didactic goal is set by students and cadets in the form of a game task;

educational activity is subject to the rules of the game;

the educational material is used as its means;

an element of sports competition is introduced into the educational activities of students and cadets, which turns the didactic task into a game;

the successful completion of a didactic task is associated with the game result.

Then the trainee, while learning during a computer game, does not suspect that he is learning something. In an ordinary higher school, it is not difficult to indicate the source of knowledge. There is no source of knowledge in a computer game that is easily learned by students and cadets. The learning process develops in the language of actions as a result of active contacts with each other. Such game training (by analogy with work [20] will be unobtrusive for cadets.

Discussion of preliminary results.

Estimates of the effectiveness of using computer games in the military sphere on the example of the use of virtual reality and 3d technologies given in work[21], confirm the high effectiveness of computer games in the educational process.

With the help of building training of cybersecurity specialists using a computer game, it is possible to increase the level of motivation, which is confirmed by the results achieved in similar areas, for example, motivation in esports players [22], which is confirmed by the gaming motives considered in the work [20].

It should be borne in mind that computer games increasingly carry a modern danger, which lies in the mass emotional, psychological perception of the game [23]. The paper [24] established the

influence of computer games as a new cultural factor on the formation of personality. With excessive enthusiasm for them, such a perception can lead a person to an aggressive manifestation [25] and when similar symptoms of computer addiction are detected [26].

It should be stated that virtual space is a new type of cultural space, which is characterized by freedom of creativity, illusory, dynamism, the ability to accelerate or turn time [27] and there is no way without it. As is known, there is no going back.

CONCLUSIONS

Gamification in higher school makes it possible to create such an information and learning environment that promotes independent, active striving of students and cadets to acquire knowledge, professional skills and abilities, such as critical thinking, decision-making, teamwork, being ready to cooperate; helps to reveal abilities and motivates self-education. Taking into account the presence of positive experience in the use of computer technologies in the training of people of different ages, it seems appropriate to use elements of the game in the training of specialists in the field of cybersecurity. At the same time, it is necessary to be careful about the use of gamification. It is clear that the spirit of struggle encourages students and cadets to do tasks faster and better, but if one of the participants gets a result that is much worse than that of the leaders, then with certain attitudes, this person may lose courage and decide that there is no point in learning, anti-motivation ensues. Game software developers are invited to develop specialized computer programs to increase the educational interest of students and cadets of the cybersecurity specialty in practical classes. Based on the above, it can be predicted that the use of computer games in the training of specialists in the field of cybersecurity at the initial level, whose purpose is to develop an interest in technology, improve communication skills that can be transferred to simulators of real means. The skills acquired during classes will be useful in future professional activities.

SCIENTIFIC NOVELTY

The concept of building a training complex for training cybersecurity specialists based on a computer game is proposed for the first time.

PROSPECTS FOR FURTHER SCIENTIFIC RESEARCH

The theoretical results obtained in the process of scientific research form the basis for further research in substantiating the technical task for the development of computer software from the game in cyberspace.

REFERENCE

1. Smartphone Addiction. URL: https://www.helpguide.org/articles/addictions/smartphone-addiction.htm#quiz.

2. Smartphone Addiction. URL: https://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time.

3. Kozubtsov I.M. Teaching electrical engineering disciplines by virtual computer game method // Electrical technologies, electric drive and electrical equipment of enterprises: collection of scientific papers of the II All-Russian Scientific and Technical Conference. Vol. 2. Ufa: USNTU Publishing House, 2009. Pp. 107–110.

4. Kozubtsov I.M.The concept of independent training of Ground Forces cadets on training equipment by playing on a virtual computer // Prospects for the development of weapons and military equipment of the Ground Forces. Collection of abstracts of the second All-Ukrainian Scientific and Technical Conference (Lviv, April 28-29, 2009). 2009. Pp. 77.

5. Buhaieva V.Y. Gamification as a way to form active professional behavior of future IT industry specialists // Pedagogy and psychology. 2018. №56. Pp. 129–135.

6. Tseas K., Katsioulas N. and Kalandaridis T. Gamification in higher education. M.S. thesis, Dept. Electrical and Computer Engineering, University of Thessaly. Volos, Greece. 2014.

7. Tkachenko O. Gamification of education: formal and informal space. Actual issues of Humanities. 2015. Issue 11. Pp. 303–309.

8. Kapp K. The gamification of learning and instruction game-based methods and strategies for training and education. San Francisco, USA: Pfeiffer, 2012.

9. Noskov Y.A. Learning technologies and gamification in academic activities // Yaroslav Pedagogical Bulletin. 2018. No. 6. Pp. 138–142.

10. Petrenko S.V. Gamification as an innovative educational technology // Innovation in education. 2018. VOL. 2. No. 7. Pp. 177–185.

11. Rybka N.M., Graization and experience of using computer games in teaching philosophy in technical institutions of higher education// Information technologies and training tools. 2018. VOL. 67, NO. 5. Pp. 213–225.

12. Kaufmann D.A. Reflection: Benefits of gamification in online higher education // Journal of Instructional Research. 2018. Vol. 7. Pp. 125–132.

13. Fiedotova N.A. Opportunities and risks of gamification in media practice // Sign: problematic field of media education. 2018. No. 4 (30). Pp. 54–59.

14. Volkova N.P. Gamification as one of the trends of modern higher education // Modern higher education: problems and prospects: VI All-Ukrainian Scientific and Practical Conference of students, postgraduates and scientists: abstracts of reports (Dnipro, 22.03.2018). 2018. Pp. 33–35.

15. Khlaponin Y.I., Kozubtsov I.M., Kozubtsova L.M. The problem of cybersecurity in educational information systems and information technologies // XIII Scientific and Practical Conference "Priority areas for the development of telecommunications systems and special-purpose networks. Use of units, complexes, communications, automation and cybersecurity in the Joint Forces Operation" (Kyiv, December 3, 2020). 2020. Pp. 279–280.

16. Antonovych P. About the essence and content of cyberwar// Military thought. 2011. No. 7. Pp. 39–46.

17. Semko V.V. Cybernetic space object interaction conflict model// Problems of informatization and management. 2012. Volume 2 No. 38. Pp. 88–92.

18. Chuiev Y.V. Research of operations in military science. Moscow: Voenizdat, 1970. 256 p.

19. Kozubtsov I.M., Kozubtsova L.M. Strategy of game in cybernetic space // Files of the International Scientific and Technical Conference "Modern information and telecommunications technologies" (Kyiv, November 17-20, 2015). 2015. Volume III Development of Information Technologies. Pp.52–54.

20. Kukshyn V. Game technologies in the classroom. Osvita.ua. (2008) URL: https://osvita.ua/school/method/technol/759.

21. Horodetskyi S.S., Beliakov V.A. Prospects of using virtual reality and 3d technologies for military-applied purposes // Electronic scientific journal "Homo Cyberus". 2018. №2(5). URL: http://journal.homocyberus.ru/perspektivy_ispolzovaniya_virtualnoj_realn.

22. Korchemnaia N.V. Research of students' motives for esports // Electronic scientific journal "Homo Cyberus". 2018. №2(5). URL: http://journal.homocyberus.ru/Korchemnaya_NV_2_2018.

23. Chaika H.V. Computer games as modern fairy tales // Practical psychology and social work. 2009. No. 4. Pp. 65-67.

24. Chaika H.V. Influence of computer games as a new factor of culture on the formation of personality // Contemporary topics of psychology. 2006. Vol. 3. Issue 3. Pp. 218–296.

25. Chaika H.V. Aggressive manifestations of computer players // Problems of general and pedagogical psychology: collection of scientific works of the G.S. Kostiuk Institute of psychology of NAPS of Ukraine. K.: Gnosis, 2008. Vol. 8. Part 3. Pp. 481–489

26. Chaika H.V. Symptoms of computer addiction // Practical psychology and social work. 2009. No. 10. Pp. 52–55.

27. Sicart M. Reality has always been augmented: Play and the promises of Pokémon GO // Mobile Media and Communication. 2017. Vol. 5. № 1. Pp. 30–33.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(4): 8-11 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

CRYPTOGRAPHY USE IN EVERYDAY LIFE

Niko salukvadze - mtsignobart uxucesi
Lizi Gogitidze - 51 public school
Giorigi Adamia - 52 public school

ABSTRACT: Cryptography plays a very important role in our everyday lives. Cryptography is used to transfer funds and data safety. It encrypts what we send so it can't be seen by anyone, other than the person we send it to or changed by a middleman. And thanks to the advances in cryptography, today we can send whatever want, without worrying about hackers getting this information. This article discusses how our information is encrypted and how secure this encryption method is.

KEYWORDS: *cryptography, cyber information, encrypted*

Introduction

In today's article, we talk about cryptography use in everyday life. Many people haven't heard anything about this word so they don't know how often cryptography is used in the 21st century. We can't take our phones as an example, because we store our most personal information on them they are very protected.

What is cryptography? what are the Different encryption methods? What is hashing? What is crypto analysis? How is cryptography used in everyday life?

The word cryptography comes from the greek word Kryptos, meaning hidden. Crypt means hidden, and the suffix -graphy stands for writing. It also is the science of hiding information. Cryptography is closely connected to mathematics and computer science. In everyday life, we see the use of cryptography in credit cards, transfers, passwords, and more. cryptography today is a normal profession that has sub-professions. Such as cryptoanalysis.

Cryptography and computer science are closely connected still both professions are quite demanded, both are very popular, and highly paid jobs but cryptography is more underrated.

Encryption methods and what they're used in

There are two different types of encryptions, symmetric and asymmetric. both have their advantages and disadvantages. Symmetric encryption works by giving the sender and the receiver a Secret Key this key is used to turn plaintext into ciphertext then this ciphertext is sent and the person that receives it uses the same key to decipher it back into plain text. This method's advantages are that symmetric encryption is fast and efficient when it comes to large files. Symmetric encryption is commonly used in Payment applications, such as card transactions where PII needs to be protected to prevent identity theft or fraudulent charges. Validations to confirm that the sender of a message is who he claims to be. Random number generation or hashing. The disadvantage to symmetric encryption is keeping the key secret. If a hacker gets this key all of the information that u send will be available to him. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.[1,2]

Asymmetric encryption uses a mathematically related pair of keys for encryption and decryption: a public key and a private key. If the public key is used for encryption, then the related private key is used for

decryption. if the private key is used for encryption, then the related public key is used for decryption. Although asymmetric encryption is much safer than symmetric it has many disadvantages such as: being slower, if the private key is lost u can't decrypt anything sent to you, public keys aren't authenticated, so no one can ensure a public key belongs to a specific person. Asymmetric encryption is used in key exchange, email security, web security, and other encryption systems that require key exchange over the public network such as SSL/TLS, SSH, and HTTPS

Hashing

Hashing is the process of transforming a given key or a string of characters into another value. this usually is represented by a shorter, value or key that represents and makes it easier to find the original string. A hash function generates new values using a mathematical hashing algorithm, known as a hash value or simply a hash. A good hash always uses a one-way hashing algorithm to prevent the hash from being turned into the original key. A hashing algorithm is a mathematical function that garbles data and makes it unreadable. Hashing is commonly used for Data indexing and retrieval, digital signatures, Encryption, and others.

the main difference between hashing and two other forms of data encryption is that once data is encrypted, it cannot be decrypted. This ensures that even if a hacker gets his hands on a hash, it will be useless since he cannot decrypt the contents of the message. Message Digest 5 and Secure Hashing Algorithm are two widely used hashing algorithms.

Hashing also has its disadvantage, for example, Hash is inefficient when there are many collisions it doesn't allow null values and hash collisions are practically not avoided for a large set of possible keys[5]

How SSL/HTTPS works

HTTPS(Hypertext Transfer Protocol Secure) secures communication and data between a user's web browser and a website. it appears in your URL when the website is secured by an SSL certificate.SSL(Secure Sockets Layer) is a bit of code on your web server that provides security for online communications.HTTPS uses an encryption protocol to encrypt communications. this protocol is called TLS(transport layer).HTTPS uses an asymmetric public key infrastructure to secure communications [3,4] .

Cryptoanalysis

Cryptoanalysis is the process of studying cryptographic systems to look for weaknesses or leaks of information. cryptoanalysis explores the weaknesses of the underlying mathematics of cryptographic systems but it includes looking for weaknesses in implementation, such as side-channel attacks or weak entropy inputs [5]. Side-channel attacks (SCAs) aim at extracting secrets from a chip or a system, through the measurement and analysis of physical parameters. Examples of these parameters are supply current, execution time, and electromagnetic emission. These attacks pose a serious threat to modules that integrate cryptographic systems, side-channel analysis techniques have proven successful in breaking encryptions and extracting the secret keys [6].

Money transfers

A lot of banks use ATMs because they are convenient and safe for taking money out of your bank account. And because their so widely used, the process of taking money out or putting it in needs to be encrypted. This encryption is known as Hardware Security Module Encryption(HSM). It protects our PIN confidentiality and other personal information, which exists on our credit or debit cards [7]. This system also ensures that cyber-criminals can't reach our PINs while the transaction is still active or when you use the ATM.

Conclusion

All in all, cryptography is a powerful tool today used for protecting our private information from hackers. We use it in our daily activities every time we send messages to transfer funds or transfer data, by using asymmetric or symmetric encryption our data is turned into cyphertext that cyber-criminals can't decipher without a special key. The most commonly used symmetric algorithm is AES-128 which is nearly impossible to decipher without a key. Even though modern encryption methods are really useful and convenient if not set up properly cyber criminals can decipher the information we send. And if the person loses their secret key somehow deciphering texts sent to them will be impossible to decipher.

Acknowledgement: This work was supported by Shota Rustaveli National Science Foundation of Georgia [SPG-22-218]

REFERENCE

1..Akkar, ML., Giraud, C. (2001). An Implementation of DES and AES, Secure against Some Attacks. In: Koç, Ç.K., Naccache, D., Paar, C. (eds) Cryptographic Hardware and Embedded Systems — CHES 2001. CHES 2001. Lecture Notes in Computer Science, vol 2162. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44709-1_26

2.Bogdanov, A., Khovratovich, D., Rechberger, C. (2011). Biclique Cryptanalysis of the Full AES. In: Lee, D.H., Wang, X. (eds) Advances in Cryptology – ASIACRYPT 2011. ASIACRYPT 2011. Lecture Notes in Computer Science, vol 7073. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25385-0_19

3. Increasing Usability of TLS Certificate Generation Process Using Secure Design; G. Iashvili, M. Iavich, A. Gagnidze, S. Gnatyuk; IVUS-2020; http://ceur-ws.org/Vol-2698/; 2020.

4.Canvel, B., Hiltgen, A., Vaudenay, S., Vuagnoux, M. (2003). Password Interception in an SSL/TLS Channel. In: Boneh, D. (eds) Advances in Cryptology - CRYPTO 2003. CRYPTO 2003. Lecture Notes in Computer Science, vol 2729. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-45146-4_34

5. Brier, É.,Joye, M. (2002). Weierstraß Elliptic Curves and Side-Channel Attacks. In: Naccache, D., Paillier, P. (eds) Public Key Cryptography. PKC 2002. Lecture Notes in Computer Science, vol 2274.

Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45664-3_24

6. Goyal, V., O'Neill, A., Rao, V. (2011). Correlated-Input Secure Hash Functions. In: Ishai, Y. (eds) Theory of Cryptography. TCC 2011. Lecture Notes in Computer Science, vol 6597. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-19571-6_12

7. Gagnidze, M. Iavich, G. Iashvili, Some Aspects of Post-Quantum Cryptosystems, Abstract book, EURO-ASIA FORUM IN POLITICS ECONOMICS AND BUSINESS – 2016, JULY 21-22, 2016, BELGRADE, SERBIA.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(4): 12-19 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

DIGITAL TECHNOLOGIES AND THEIR CYBER SECURITY IN LIGHT OF RECENT CHANGES IN ELECTORAL LAW

ციფრული ტექნოლოგიები და მათი კიბერუსაფრთხოება საარჩევნო კანონმდებლობაში შეტანილი ბოლო ცვლილებების ფონზე

Andro Gotsiridze – professor Business & Technology University of Georgia, Cybersecurity Consultant, Founder of CYSEC - Cyber Security Educational Research Center, Director of Cyber Security Bureau of Ministry of Defence of Georgia in 2014 -2017

ანდრო გოცირიძე, საქართველოს ბიზნესისა და ტექნოლოგიების უნივერსიტეტის პროფესორი, კიბერუსაფრთხოების კონსულტანტი. კიბერუსაფრთხოების საგანმანათლებლო კვლევითი ცენტრის CYSEC დამფუძნებელი, თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს დირექტორი 2014-2017 წლებში.

ABSTRACT:The democratic approach considers that all elections are expected to be free, open and fair, and based on secret ballot; Digital Solutions, IC Technologies are integral parts of the modern electoral process. Their usage increases confidence, the degree of freedom and impartiality of elections, but from a cybersecurity perspective, any process involving the use of electronic devices or digitized data contains risks. Technology cannot be introduced at the cost of compromising mentioned requirements.

Depending on the motives of the attacker, cyber threats can lead to a decrease in confidence in the democratic process. Due to the growing trend of using cyber and information operations to interfere in elections, the cybersecurity of electoral processes is definitely one of the most important tasks of the state. The article gives a short overview of the cyber threats to election and discusses some cybersecurity aspects of integration of digital solutions into elections processes.

KEYWORDS: *cybersecurity, digital solution*

აბსტრაქტი: დემოკრატიული საზოგადოება მოელის, რომ ნებისმიერი არჩევნები იქნება თავისუფალი, ღია, სამართლიანი და უზრუნველყოფს მოქალაქის არჩევანის ფარულობას.ციფრული ტექნოლოგიები, კომპიუტერული სისტემები და პროგრამული უზრუნველყოფა საარჩევნო პროცესის თითოეული კომპონენტის შემადგენელი ნაწილია. მათი გამოყენება არჩევნების სანდოობას, თავისუფლების ხარისხსა და მიუკერძოებლობას ზრდის, თუმცა, კიბერუსაფრთხოების პერსპექტივიდან, ნებისმიერი პროცესი, რომელიც მოიცავს ელექტრონული მოწყობილობის ან გაციფრულებული მონაცემების გამოყენებას, გარკვეულწილად, რისკის შემცველია. ცხადია, ტექნოლოგიების დანერგვა არ უნდა მოხდეს ზემოჩამოთვლილი მოთხოვნების ხარჯზე.თავდამსხმელის მოტივიდან გამომდინარე, კიბერსაფრთხეებმა შესაძლოა შეზღუდოს არჩევნების თავისუფლება, განაპირობოს

დემოკრატიული პროცესისადმი ნდობის შემცირება.ბუნებრივია, კიბერდანაშაულის ზრდის ტენდენციის პირობებში, საარჩევნო პროცესების კიბერუსაფრთხოება თანამედროვე სახელმწიფოსათვის ერთ ერთი უმნიშვნელოვანესი ამოცანაა. სტატიაში განვიხილავთ არჩევნებში გამოყენებული ციფრული ტექნოლოგიების გამოყენებისას წარმოქმნილ კიბერსაფრთხეებს და კიბერუსაფრთხოების ზოგიერთ ასპექტს.

საკვანძო სიტყვები: *ციფრული ტექნოლოგიები, კიბერუსაფრთხოება, თანამედროვე ტექნოლოგოები*

ციფრული ტექნოლოგიები, კომპიუტერული სისტემები და პროგრამული უზრუნველყოფა საარჩევნო პროცესის თითოეული კომპონენტის შემადგენელი ნაწილია. მათი გამოყენება არჩევნების სანდოობას, თავისუფლების ხარისხსა და მიუკერძოებლობას ზრდის, თუმცა, კიბერუსაფრთხოების პერსპექტივიდან, ნებისმიერი პროცესი, რომელიც მოიცავს ელექტრონული მოწყობილობის ან გაციფრულებული მონაცემების გამოყენებას, გარკვეულწილად, რისკის შემცველია.

ბუნებრივია, კიბერდანაშაულის ზრდის ტენდენციის პირობებში, საარჩევნო პროცესების კიბერუსაფრთხოება თანამედროვე სახელმწიფოსათვის ერთ ერთი უმნიშვნელოვანესი ამოცანაა.

ზოგადად, კიბერთავდასხმის ტექნიკური თუ ადამიანური ვექტორი მოიცავს თავად საინფორმაციო ტექნოლოგიური სისტემებს, ასევე მათი შექმნისა და მართვის პროცესებს. ნებისმიერ სფეროსა თუ ინდუსტრაში სისტემის ან პროგრამული უზრუნველყოფის ტექნიკური სიუსტის კვალდაკვალ, ხშირად, კიბერშეტევების განსახორციელებლად ადამაინური ფაქტორი გამოიყენება. ბუნებრივია, ეს ტენდენცია ვრცელდება საარჩევნო სისტემების კიბერუსაფრთხოებაზეც. თავდამსხმელის მოტივიდან გამომდინარე, კიბერსაფრთხეებმა შესაძლოა შეზღუდოს არჩევნების თავისუფლება, განაპირობოს დემოკრატიული პროცესისადმი ნდობის შემცირება.

როგორც აღინიშნა, თანამედროვე არჩევნების თითქმის ყველა კომპონენტიამა თუ იმ ფორმით დაკავშირებულია ციფრულ ტექნოლოგიებთან და პროცესებთან. საარჩევნო რეესტრებს წარმოება, ამომრჩეველთა, პარტიებისა და კანდიდატების რეგისტრაცია, პარტიებისა და კანდიდატების რეგისტრაცია, დამკვირვებელთა, საარჩევნო ადმინისტრაციის და ამომრჩეველთა ცნობიერების ამაღლების ღონისძიებები, კენჭისყრა, ხმების დათვლა და შედეგების მართვა, ინფორმაციის მიმოცვლა და ანალიზი, საჩივრებისა და დავების მართვის სისტემები და სხვა მნიშვნელოვანი პროცესები ძალიან ხშირადკომპიუტერული ტექნოლოგიების საშუალებით ხდება. ეს ტენდენცია მეტწილად საარჩევნო პროცესების

გაუმჯობესებას, არჩევნების სამართლიანობის და სანდოობის ამაღლებას იწვევს, თუმცა მზარდი კიბერრისკების პირობებში, მოუმზადებელი ნორმატიული ბაზის, კიბერრისკების მართვის არასრულყოფილი სისტემისა და არასკმარისი ცნობიერების პირობებში, სახელმწიფოსათვის უმნიშვნელოვანესი პროცესი- არჩევნები, არცთუ იშვიათად, მოწყვლადი ხდება ხოლმე.

საარჩევნო სისტემების გაციფრულება, რაც ერთის მხრივ, სათანადო ნორმატიული ბაზის შექმნას, პროცესების გამართვას, მეორეს მხრივ კი არჩევნების კიბერუსაფრთხოების უზრუნველყოფას გულისხმობს, საქართველოშიც არაერთხელ დამდგარა დღის წესრიგში.

მიმდინარე წელს საქართველოს კანონმდებლობაში შეტანილი ცვლილებები ცესკო -ს მომდევნო მუნიციპალურ არჩევნებზე ამომრჩეველთა ელექტრონული რეგისტრაციის, ელექტრონული კენჭისყრის, ხმათა ელექტრონული დათვლისა და არჩევნების შედეგების შემაჯამებელი ოქმის ელექტრონულად შედგენის უფლებამოსილებას ანიჭებს.ამასთან, ელექტრონული რეგისტრაცია ყველა საარჩევნო უბანზე უნდა იყოს დანერგილი, ხოლო ქაღალდის ბიულეტენების ელექტრონული დათვლის სისტემა კი, საჭიროებისამებრ, სოციოლოგიურად ვალიდური შედეგებისათვის საჭირო რაოდენობის უბნებში. რაც შეეხება ელექტრონულ კენჭისყრის სახეს, ის არ არის განსაზღვრული.

ამჟამად საქართველოში არსებობს გარკვეული მონაცემთა ბაზები, როგორიცაა ამომრჩეველთა ერთიანი სია, დამკვირვებელთა რეესტრი, პრესის, მედიისადა პარტიების რეგისტრაცია, ასევე, საქართველოს საარჩევნო კოდექსის მიხედვით, შესაძლებელია, საარჩევნო სუბიექტების, დამკვირვებლების, მედიის მიერ ელექტრონული საშუალებებით განაცხადების წარდგენას.

ზოგადად, სხვადასხვა ეტაპზე, ციფრული ტექნოლოგიები სხვადასხვა სახით გამოიყენება და მათ მიმართ არსებული კიბერსაფრთხეებიც, ისევე, როგორც მათი პრევენციის ან მიტიგაციის გზაც სხვადასხვა.

ქვემოთ განვიხილავთ არჩევნებში გამოყენებული ციფრული ტექნოლოგიების გამოყენებისას წარმოქმნილ კიბერსაფრთხეებს და კიბერუსაფრთხოების ზოგიერთ ასპექტს.

როგორც უკვე აღინიშნა, საქართველოში რამდენიმე ელექტრონული რეესტრი არსებობს და ინერგება ტექნოლოგიები საარჩევნო პროცესის სამართავად. ინტეგრირებული სისტემები და სერვისები, რომლებიც გაციფრულებული საარჩევნო მონაცემების სამართავად გამოიყენება **არჩევნების მართვის სისტემის** სახელითაა ცნობილი და იგი რამდენიმე სერვისს მოიცავს. სისტემის ზოგიერთი შემადგენელი ადგილობრივ დონეზეა ბაზირებული თუმცა კავშირი და ინფორმაციის მიმოცვლა აქვს ცენტრალურ ბაზასთან. არჩევნების მართვის სისტემის

შემადგენელი ნაწილია, ასევე სხვადასხვა მონაცემთა ბაზა, აპლიკაციები და სხვა პროგრამები, რომელთა მიმართ არსებული კიბერრისკები მთლიანი სისტემისთვისაც საფრთხის შემცველია.

საარჩევნო პროცესებში მოწყვლადი კომპონენტებია ამომრჩევლის ონლაინ-რეგისტრაცია, ხმის მიცემის ელექტრონული პროცესი, შედეგების შეჯამება და გამოცხადება, კომუნიკაცია, საარჩევნო კამპანიის წარმოების ელექტრონული საშუალებები და სხვა უამრავი პროცესი, რომელთა ოპტიმალური მართვა სწორედ ციფრული ტექნოლოგიების გამოყენებით მიიღწევა . თუმცა, ამგვარ მრავალფეროვან პროცესებს სათანადო კიბერრისკებიც ახლავს თან, რომელთა არასრული ჩამონათვალი შესაძლოა შემდეგნაირად წამოვიდგინოთ:

- **არაავტორიზებული წვდომა:** ინტერნეტთან კავშირის მქონე მონაცემთა ბაზები მოწყვლადია. თავდამსხმელს, წვდომის მოპოვების შემდგომ, შეუძლია დაამატოს, შეცვალოს, ამოშალოს ამომრჩეველი, გააყალბოს ხმა არჩევნების დღეს. იმ შემთხვევაშიც კი, თუ ამგვარი ქმედება მნიშვნელოვან გავლენას ვერ ახდენს არჩევნების შედეგზე, პროცესში ჩარევის აღქმა სერიოზულ საფრთხეს უქმნის არჩევნების სანდოობას
- **არასათანადო ტექნიკური მომსახურება ან ავტომატიზირებული განახლებების დაგვიანებული პროცესი** ხშირად განაპირობებს თავდამსხმელის მხრიდან მავნე პროგრამული უზრუნველყოფის იმპლანტაციას
- **ავტორიზებული პირის ანგარიშის კომპრომეტაცია.**თავდამსხმელმა შეიძლება მოახდინოს საარჩევნო ადმინისტრაციის წევრის ან სხვა ინსაიდერის ანგარიშის კომპრომეტაცია. არასათანადო კონტროლის პირობებში, მას საშუალება მიეცემა ამომრჩევლის შესახებ ჩანაწერები მისი შეხედულებისამებრ შეცვალოს. ლოგირებისა და მონიტორინგის სისტემის არარსებობის პირობებში ეს ხარვეზი აისახება არჩევნების შედეგზე.
- **დაკავშირებული სისტემების და მონაცემთა ბაზების კომპრომეტაცია.** როგორც აღინიშნა, არჩევნების მართვის სისტემასთან დაკავშირებულია სხვადასხვა აპლიკაცია, პროგრამა ან მონაცემთა ბაზა, რომელთაგან ზოგიერთი, შესაძლოა, არ იყოს სათანადოდ დაცული და მოხდეს მისი კომპრომეტაცია ან მონაცემების მანიპულაცია მათი გადაგზავნისას. გარკვეულ რისკს წარმოადგენს ასევე ის ფაქტორი, რომ ზოგჯერ

გარე ბაზებიდან მონაცემები პირდაპირ ხვდება არჩევნების მართვის სისტემებში, დამატებითი გადამოწმებისა და დადასტურების გარეშე. ასეთ შემთხვევაში შესაძლებელია ამომრჩევლის სტატუსის მანიპულირება მავნე აქტორის მხრიდან.

- **ვებგვერდის გაყალბება:** თავდამსხმელი შესაძლოა ახდენდეს პოზიციონირებას, როგორც ოფიციალური საიტი, სინამდვილეში კი ცდილობდეს ამომრჩეველთა პერსონალური ინფორმაციის მოპარვას მიმსგავსებული გვერდის მეშვეობით
- DDoS შეტევა, რომლის მეშვეობითაც, თავდამსხმელი, აფერხებს რა სერვისის ხელმისაწვდომობას, ცდილობს შეზღუდოს ამომრჩევლის რეგისტრაციის შესაძლებლობა. საბოლოო ჯამში მსგავსმა ზემოქმედებამ შესაძლოა გამოიწვიოს არცევნებში მონაწილეობის დაბალი პროცენტი
- **არასათანადოდ დაცული ვებგვერდი**შესაძლოა გახდეს ამომრჩევლების მონაცემთა ბაზაში შეღწევის ვექტორი, რასაც თან სდევს ამომრჩეველთა შესახებ ჩანაწერის გაყალბება
- **ხმის მიცემის ელექტრონული მოწყობილობა** შესაძლოა კომპრომეტირებულ იქნას ფიზიკური ჩარევის, (მაგ. USB ან სხვა სახის მედიამატარებელი) ან გარე კავშირის (მაგ. უსადენო ინტერნეტი) გზით, რამაც, შესაძლოა შეცვალოს ინფორმაცია ხმის მიცემის შესახებ
- ოფიციალურ პირთა **ელფოსტის ანგარიშის კომპრომეტაცია**ფიშინგის ან სოციალური ინჟინერიის სხვა ტექნიკით, შესაძლოა გამოყენებულ იქნას თავდამსხმელის მიერ ყალბი ინფორმაციის გასავრცელებლად, არაკეთილსინდისიერი განკარგულების გასაცემად. კომპრომეტირებული ანგარიში ასევე გამოიყენება მავნე პროგრამული უზრუნველყოფის ქსელში გასავრცელებლად
- საარჩევნო ადმინისტრაციის **ვებგვერდის მანიპულაცია** - ხშირია Defacement ტიპის შეტევის განხორციელება ამომრჩევლის დაბნევის, დაშინების, შეცდომაში შეყვანის მიზნით. ასევე, შესაძლებელია ონლაინ ხმის მიცემის საიტის ლოკაციის შეცვლა, ამომრჩეველთა წვდომის გართულების მიზნით.
- **სოციალური ქსელის რისკებიდან** ყურადსაღებია ყალბი ანგარიშები ან ოფიციალური გვერდების კომპრომეტაცია. ეს ტექნიკა შესაძლებელია გამოყენებულ იქნას

სოციალური ქსელით შეცდომაში შემყვანი ინფრომაციის, არასწორი ლოკაციების, გაყალბებული შედეგების გასავრცელებლად.

ზოგადად, თუკი არჩევნების თანმდევ კიბერშეტევებს გავაანალიზებთ, ცხადი ხდება კანონზომიერება, რომ თავდამსხმელები კიბერშეტევების იაფ მეთოდებს ანიჭებენ უპირატესობას. ასე მაგალითად, დაბალტექნოლოგიური და ეკონომიკურად ეფექტური DDoS და Defacement სჭარბობს დახვეწილ APT შეტევებს. ეს უკანასკნელი ტიპი შეტევისა მეტად იშვიათად გამოიყენება და ისიც, მხოლოდ მაღალგანვიტარებული კიბერპოტენციალის მქონე სახელმწიფოთა საარჩევნო სისტემების წინააღმდეგ.

კიბერსაფრთხეებისაგან თავდასაცავად მნიშვნელოვანია ღონისძიებათა კომპლექსის გატარება:

- **ძლიერი პასვორდისა და მრავალფაქტორიანი ავთენტიფიკაციის პოლიტიკის** გატარება ნებისმიერი ავტორიზებული მომხმარებლისათვის. განსაკუთრებული ყურადღება უნდა დაეთმოს ადმინისტრირების უფლების მქონე მომხმარებლის ანგარიშების უსაფრთხოებას.
- **შეღწევადობის ტესტის, პროგრამის კოდის აუდიტის ჩატარება,** მიუხედავად იმისა, გამოყენებული პროგრამული უზრუნველყოფები ადმინისტრაციის მიერაა შექმნილი თუ ვენდორების მოწოდებულია. აუდიტისა და ტესტის შედეგები კარგ წარმოდგენას იძლევა სისტემის სისუსტეებზე. ასევე, მნიშვნელოვანია ფიშინგის და სოციალური ინჟინერიის სხვადასხვა სახეობების მიმართ ორგანიზაციის მდგრადობის ტესტები და რეგულარული სავარჯიშოები.
- პროგრამული უზრუნველყოფის **განახლებების პროცესის წარმოება ავტომატურ რეჟიმში** ყველა მოწყობილობასა თუ სისტემაზე, რომელიც კავშირშია არჩევნების მართვის სისტემასთან.
- მონაცემთა ბაზის სერვერების **ინტერნეტით ხელმისაწვდომობის** შეზღუდვა
- გარე სისტემებიდან შემოსული **მონაცემების ვალიდაციის მექანიზმის** გამართვა
- **მიმდინარე პროცესების ლოგირება და დაშვებების სწორი მენეჯმენტი.** როგორც წესი, უნდა ინახებოდეს მონაცემტა ბაზებში განხორციელებული ნებისმიერი ცვლილების სესახებ ჩანაწერი და უნდა ხდებოდეს მათი ანალიზი, ასევე,

ანომალიური აქტივობების კვლევა. წასული თანამშრომლების ან სხვა ინსაიდერების (მაგ. ვენდორის, კონტრაქტორის) სისტემასთან წვდომა ავტომატურად უნდა იზღუდებოდეს მისი საჭიროების გაქრობის მომენტიდან.

- საარჩევნო ადმინისტრაციის, ასევე არჩევნებში მონაწილე პირთა**ცნობიერების ამაღლება,**გასაკუთრებით, სოციალური მედიის რისკების თემატიკაზე. სოციალური მედიის როგორც ოფიციალური, ასევე პირადი ანგარიშები აუცილებელია დაცულ იქნეს ორმაგი ავტენტიფიკაციით. ძლიერი პასვორდის პოლიტიკასთან ერთად, ეს საუკეთესო ნაბიჯია ანგარიშის კომპრომეტაციის თავიდან ასაცილებლად.

ამრიგად, სახელმწიფოთა მიერ მხარდაჭერილი კიბერშეტევები ხშირად მიმართულია უნდობლობის გაღვივების, საზოგადოების პოლარიზაციისკენ და მიზნად ისახავს დემოკრატიული პროცესების შეფერხებასა და მოშლას. ნებისმიერი სისტემით ჩატარებული არჩევნები უნდა იყოს ღია, სამართლიანი, თავისუფალი და ემყარებოდეს ხმის მიცემის ფარულობას. ციფრული ტექნოლოგიების დანერგვა არ უნდა ახდენდეს რომელიმე ამ მახასიათებლის კომპრომეტაციას. ციფრული გადაწყვეტები ან საარჩევნო ტექნოლოგიები თავისთავად არ შეიცავენ უფრო მეტ ან ნაკლებ საფრთხეს, მაგრამ მათი დანერგვისას აუცილებელია გარკვეული სიფრთხილის დაცვა ციფრული პროცესების მოქმედ კანონმდებლობასთან შესაბამისობაში მოსაყვანად. ხშირად, კიბერუსაფრთხოების შესაბამისი მოთხოვნების დაცვით ციფრული ტექნოლოგიების დანერგვა ხელსუწყობს არჩევნების პროცესისადმი წაყენებული მოთხოვნების შესრულებას და მათ მაღალ ლეგიტიმაციას.

სტატიაში შევეცადეთ ფოკუსირება მოგვეხდინა კიბერშეტევებთან და ქსელის უსაფრთხოებასთან დაკავშირებულ საფრთხეებზე და მათთან გამკლავების გზებზე. საარჩევნო პროცესებში ჩარევაში მნიშვნელოვან როლს თამაშობს დეზინფორმაცია, სოციალური მედია და საინფორმაციო ოპერაციები, რომელთა გავლენა არჩევნების ძირითად მახასიათებლებსა და მის ლეგიტიმურობაზე ცალკე განხილვის თემაა და ამდენად, ეს მიმართულება წინამდებარე ნაშრომში ვერ მოხვდა.

ბიბლიოგრაფია

1. Sebastian Bay, Guna Šnore, Protecting Elections: a strategic communications approach. NATO Strategic Communications Centre of Excellence, 2019
2. Defence Intelligence Agency. Russia Military Power - Building a Military to Support Great Power Aspirations. Report, 2017. ხელმისაწვდომია www.dia.mil/Military-Power-Publications

3. Laura Galante, Shaun Eee. Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents. Atlantic Councis Issue Brief. September, 2018
4. Intelligence Community Assesment. Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. ICA 2017-01D, 6 January 2017
5. ა.გოცირიძე. კიბერსაფრთხეები და მათთან ბრძოლის სტრატეგიული მიმართულებები საქართველოს პერსპექტივიდან. თ.ხიდაშელი "ჰიბრიდული ომების ანატომია"-ში. გვ. 365-395. გამომცემლობა პალიტრა L.
6. Defending Digital Democracy Project**.** Belfer Center for Science and International Affairs**.** Harvard Kennedy School**.** The State and Local Election Cybersecurity Playbook. 2018.
7. Office of the Director of National Intelligence, Cyber Threat Intelligence Integration Center. Cyber Threats to Elections – a Lexicon. 2018

Scientific and Practical Cyber Security Journal (SPCSJ) 6(4): 20-28 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

MODERN THREATS IN CRYPTOCURRENCY

თანამედროვე საფრთხეები კრიპტოვალუტაში

Ketevan Maghradze, 141 Public school
ქეთევან მაღრაძე, 141-ე საჯარო სკოლა
Nutsa Kartlelishvili, 186 Public school
ნუცა ქართლელიშვილი, 186-ე საჯარო სკოლა
Natia Tarielashvili, 45 Public school
ნათია ტარიელაშვილი, 45-ე საჯარო სკოლა

ABSTRACT: The paper describes meaning of cryptography, its role in cryptocurrency, cryptocurrency, threats, and the biggest collapse of crypto history – Terra Ecosystem downfall. The authors of the papers offer explanation and analysis of the most popular topic of the 21st century.

KEYWORDS:*Cryptography, key of the cryptography, cryptocurrency, threats of the cryptocurrency, stablecoin, tokens, Luna, Terra, fall of the currency.*

აბსტრაქტი: ნაშრომში აღწერილია კრიპტოგრაფიის მნიშვნელობა, მისი როლი კრიპტოვალუტაში, კრიპტოვალუტა, საფრთხეები და კრიპტო ისტორიაში ყველაზე დიდი კოლაფსი- Terra ეკოსისტემის დაცემა. ნაშრომის ავტორები გვთავაზობენ21-ე საუკუნის ყველაზე აქტუალური თემების განმარტებასა და ანალიზს.

საკვანძო სიტყვები: *კრიპტოგრაფია, კრიპტოგრაფიის გასაღები, კრიპტოვალუტა, კრიპტოვალუტის საფრთხეები, სტეიბლქოინი, ლუნა, ტერა, ვალუტა დაცემა, თოქენები.*

შესავალი

ცივილიზაციის განვითარებასთან ერთად განვითარდა ტექნოლოგიები. დღეს ის ჩვენი ყოველდღიურობის განუყრელი ნაწილია. მრავალი დადებითის გარდა, მას უარყოფითი მხარეებიც აქვს. ერთ-ერთია ინფორმაციული დაუცველობა. ზუსტად ვერასდროს განვსაზღვრავთ, როდის ვიქნებით ჰაკერის და თავდასხმის მსხვერპლი ან როდის მიითვისებენ ჩვენს პერსონალურ ინფორმაციას. სწორედ ასეთი საფრთხეებისგან გვიცავს კრიპტოგრაფია, რომელიც შიფრავს სენსიტიურ მონაცემებს და მხოლოდ განკუთვნილი პირისთვის ხდის მას ხელმისაწვდომს. ის საუკუნებიაა არსებობს, მაგრამ ტექნოლოგიებში ბოლო რამდენიმე ათწლეულია რაც იყენებენ. სწორედ მასზე დაყრდნობით შეიქმნა კრიპტოვალუტა და მასთან ერთად განვითარდა წლების განმალობაში.

კრიპტოგრაფია

კრიპტოგრაფია არის ინფორმაციისა და კომუნიკაციების უზრუნველყოფის ტექნიკა კოდების გამოყენებით, რათა მხოლოდ იმ პირმა შეძლოს მისი გაგება და დამუშავება, ვისთვისაც არის განკუთვნილი ინფორმაცია[1]. ამგვარად თავიდან აიცილებს ინფორმაციაზე უნებართვო წვდომას. კრიპტოგრაფიაში ტექნოლოგიები, რომლებიც გამოიყენება ინფორმაციის დასაცავად, მიღებულია მათემატიკური ცნებებიდან და წესებზე დაფუძნებული გამოთვლების ნაკრებიდან, რომელიც ცნობილია როგორც ალგორითმები. ეს ალგორითმები გამოიყენება კრიპტოგრაფიული გასაღების გენერირებისთვის, ციფრული ხელმოწერისთვის, ვერიფიკაციისთვის, მონაცემთა კონფიდენციალურობის დასაცავად, ინტერნეტში ვებ გვერდების დათვალიერებისთვის და კონფიდენციალური ტრანზაქციების დასაცავად, როგორიცაა საკრედიტო ბარათი და სადებეტო ბარათი[2].

კრიპტოგრაფიის მახასიათებლები შემდეგია:

- **კონფიდენციალურობა:** ინფორმაციაზე წვდომა შეუძლია მხოლოდ იმ პირს, ვისთვისაც ის განკუთვნილია და მის გარდა სხვას არავის მიუწვდება ხელი ამ ინფორმაციაზე.
- **მთლიანობა:** ინფორმაციის შენახვაში ან გადასვლისას ვერ მოხერხდება გამგზავნსა და მიმღებს შორის რაიმე დამატებითი ინფორმაციის აღმოჩენის გარეშე.
- **არაუარყოფა:** ინფორმაციის შემქმნელს/გამგზავნს არ შეუძლია უარყოს მისი განზრახვა გაგზავნოს ინფორმაცია მოგვიანებით ეტაპზე.
- **ავთენტიფიკაცია:** გამგზავნისა და მიმღების ვინაობა დადასტურებულია. ასევე დადასტურებულია ინფორმაციის დანიშნულება/წარმოშობა.

ხშირად დაშიფვრის ყველაზე რთული კომპონენტი გასაღების მართვაა, რომელიც მოიცავს სიმეტრიული და ასიმეტრიული დაშიფვრის გასაღებების გენერირებას, გამოყენებას, დაარქივებას და წაშლას.

ძირითადად გამოიყენება სამი ტიპის გასაღები:

- **სიმეტრიული გასაღების კრიპტოგრაფია:** ეს არის დაშიფვრის სისტემა, სადაც შეტყობინების გამგზავნი და მიმღები იყენებენ ერთ საერთო გასაღებს შეტყობინებების დაშიფვრისა და გაშიფვრის მიზნით. სიმეტრიული საკვანძო სისტემები უფრო სწრაფი და მარტივია, მაგრამ პრობლემა ის არის, რომ გამგზავნმა და მიმღებმა როგორმე უნდა გაცვალონ გასაღები უსაფრთხოდ. ყველაზე პოპულარული სიმეტრიული გასაღების კრიპტოგრაფიული სისტემაა მონაცემთა დაშიფვრის სისტემა (AES).
- **ჰეშის ფუნქციები:** ამ ალგორითმში არ არის გამოყენებული რაიმე გასაღები. ფიქსირებული სიგრძის ჰეშის მნიშვნელობა გამოითვლება ჩვეულებრივი ტექსტის მიხედვით, რაც შეუძლებელს ხდის უბრალო ტექსტის შინაარსის აღდგენას. ბევრი ოპერაციული სისტემა იყენებს ჰეშის ფუნქციებს დასაშიფრად.

- **ასიმეტრიული გასაღების კრიპტოგრაფია:** ამ სისტემის მიხედვით წყვილი გასაღებები გამოიყენება ინფორმაციის დაშიფვრისა და გაშიფვრის მიზნით. საჯარო გასაღები გამოიყენება დაშიფვრისთვის, ხოლო პირადი გასაღები გამოიყენება გაშიფვრისთვის. საჯარო გასაღები და პირადი გასაღები განსხვავებულია. მაშინაც კი, თუ საჯარო გასაღები ყველასთვის ცნობილია, მიმღებს შეუძლია მხოლოდ მისი გაშიფვრა, რადგან მხოლოდ მან იცის პირადი გასაღები[3].

კრიპტოვალუტა

კრიპტოვალუტა არის ციფრული გადახდის სისტემა, რომელიც არ არის დამოკიდებული საბანკო სისტემაზე. ეს არის სისტემა, რომელსაც შეუძლია ნებისმიერ მომხმარებელს ნებისმიერ ადგილას მისცეს გადახდების გაგზავნის და მიღების საშუალება. იმის მაგივრად, რომ რეალურ სამყაროში მოხდეს ფიზიკური ფულის გადატანა და გაცვლა, კრიპტოვალუტის გადახდები არსებობს მხოლოდ ციფრული ჩანაწერების სახით ონლაინ მონაცემთა ბაზაში, რომელიც აღწერს კონკრეტულ ტრანზაქციებს. როდესაც თქვენ გადარიცხავთ კრიპტოვალუტის თანხებს, ტრანზაქციები აღირიცხება საჯარო მონაცემთა ბაზაში. კრიპტოვალუტა ინახება ციფრულ საფულეებში[4].

პირველი კრიპტოვალუტა იყო ბიტკოინი, რომელიც დაარსდა 2009 წელს და ის დღემდე ერთერთი ყველაზე ცნობილი კრიპტოვალუტაა.

კრიპტოვალუტები მუშაობს განაწილებულ საჯარო მონაცემთა ბაზაზე, რომელსაც ეწოდება ბლოკჩეინი, ყველა ტრანზაქციის ჩანაწერი, რომელიც ინახება ვალუტის მფლობელების მიერ.

კრიპტოვალუტის ერთეულები იქმნება პროცესის მეშვეობით, რომელსაც მაინინგს უწოდებენ, რაც გულისხმობს კომპიუტერის ენერგიის გამოყენებას რთული მათემატიკური ამოცანების ამოსახსნელად, რომლებიც წარმოქმნიან მონეტებს. მომხმარებლებს ასევე შეუძლიათ შეიძინონ ვალუტები სხვადასხვა გზით, შემდეგ შეინახონ და დახარჯონ ისინი კრიპტოგრაფიული საფულეების გამოყენებით.

მიუხედავად იმისა, რომ ბიტკოინი 2009 წლიდან არსებობს, კრიპტოვალუტები და ბლოკჩეინის ტექნოლოგიის აპლიკაციები კვლავ ჩნდება ფინანსური თვალსაზრისით და მომავალში მეტი გამოყენებაა მოსალოდნელი. ტრანზაქციები და სხვა ფინანსური აქტივები, საბოლოოდ შეიძლება მოხდეს ტექნოლოგიის გამოყენებით[6].

ყველაზე ცნობილი კრიპტოვალუტებია:

- **Bitcoin:** 2009 წელს დაარსებული ბიტკოინი იყო პირველი კრიპტოვალუტა და დღემდე ყველაზე ხშირად გამოყენებადია. ვალუტა შეიქმნა სატოში ნაკამოტოს მიერ - ფართოდ მიჩნეულია ფსევდონიმად ცალკეული პიროვნების ან ადამიანთა ჯგუფისთვის, რომელთა ზუსტი ვინაობა უცნობია.

- **Ethereum:** 2015 წელს შემუშავებული Ethereum არის ბლოკჩეინის პლატფორმა საკუთარი კრიპტოვალუტით, სახელწოდებით Ether (ETH) ან Ethereum. ეს არის ყველაზე პოპულარული კრიპტოვალუტა ბიტკოინის შემდეგ.
- **Litecoin:** ეს ვალუტა ყველაზე მეტად ჰგავს ბიტკოინს, მაგრამ უფრო სწრაფად განვითარდა ახალი ინოვაციების შესაქმნელად, მათ შორის მას litecoin-ს აქვს უფრო სწრაფი გადახდები და პროცესები მეტი ტრანზაქციის დასაშვებად.

არაბიტკოინის კრიპტოვალუტებს ერთობლივად უწოდებენ "ალტკოინებს", რათა განასხვავონ ისინი ორიგინალისგან.

კრიპტოვალუტები, როგორც წესი, შენდება ბლოკჩეინის ტექნოლოგიის გამოყენებით. ბლოკჩეინი აღწერს, თუ როგორ ხდება ტრანზაქციების ჩაწერა „ბლოკებად“ და დროის შტამპით. ეს საკმაოდ რთული, ტექნიკური პროცესია, მაგრამ შედეგი არის კრიპტოვალუტის ტრანზაქციების ციფრული ბაზა, რომლის ხელყოფა რთულია ჰაკერებისთვის.

გარდა ამისა, ტრანზაქციები მოითხოვს ორფაქტორიანი ავთენტიფიკაციის პროცესს. მაგალითად, შეიძლება მოგეთხოვოთ მომხმარებლის სახელი და პაროლი შეიყვანოთ ტრანზაქციის დასაწყებად. ამის შემდეგ, შეიძლება დაგჭირდეთ თქვენს პირად მობილურ ტელეფონში ტექსტის საშუალებით გაგზავნილი ავთენტიფიკაციის კოდის შეყვანა.

მიუხედავად იმისა, რომ ფასიანი ქაღალდები არსებობს, ეს არ ნიშნავს, რომ კრიპტოვალუტები არ არის გატეხილი. რამდენიმე დიდი კიბერთავდასხმა ძვირად დაუჯდა კრიპტოვალუტის დამწყებ ბიზნესს. ჰაკერებმა Coincheck-ზე 534 მილიონი დოლარი და BitGrail-ზე 195 მილიონი დოლარი შეადგინეს, რაც მათ 2018 წლის კრიპტოვალუტის ორ უდიდეს კიბერთავდასხმად აქციეს[4].

Stablecoins

Stablecoins არის კრიპტოვალუტები, რომელთა ღირებულება მიბმულია სხვა ვალუტის ღირებულებასთან. არსებობს სამი ტიპის stablecoin, მათი ღირებულების სტაბილიზაციის მექანიზმზე დაყრდნობით.

მიუხედავად იმისა, რომ ბიტკოინი რჩება ყველაზე პოპულარულ კრიპტოვალუტად, ის განიცდის მაღალ ცვალებადობას მის ფასში ან გაცვლით კურსში. მაგალითად, ბიტკოინის ფასი 2020 წლის მარტში $5,000-დან გაიზარდა 2021 წლის აპრილში $63,000-მდე და დაეცა თითქმის 50% მომდევნო ორი თვის განმავლობაში.

კრიპტოვალუტები, როგორიცაა ბიტკოინი და ეთერიუმი, გვთავაზობენ უამრავ სარგებელს, ერთ-ერთი ყველაზე მნიშვნელოვანი ფაქტორია, რომ ისინი არ მოითხოვენ ნდობას შუამავალი ინსტიტუტისგან გადახდების გაგზავნისთვის. მაგრამ ერთი მთავარი ნაკლი არის ის, რომ კრიპტოვალუტების ფასები არაპროგნოზირებადია და აქვს ტენდენცია მერყეობისკენ.

ეს ართულებს მათ გამოყენებას ყოველდღიურად ადამიანებისთვის. ზოგადად, ხალხი მოელის, რომ შეძლებს გაიგოს, რამდენი იქნება მათი ფული ერთი კვირის შემდეგ, როგორც მათი უსაფრთხოებისთვის, ასევე საარსებო წყაროსთვის.

კრიპტოვალუტის არაპროგნოზირებადობა ეწინააღმდეგება ზოგადად ფულის სტაბილურ ფასებს, როგორიცაა აშშ დოლარი ან სხვა. დოლარის მსგავსი ვალუტების ღირებულებები თანდათან იცვლება დროთა განმავლობაში, მაგრამ ყოველდღიური ცვლილებები ხშირად უფრო მკვეთრია კრიპტოვალუტებისთვის, რომლებიც რეგულარულად იზრდება და ეცემა[7].

კრიპტოვალუტის საფრთხეები

მიუხედავად იმისა, რომ კრიპტოვალუტის მომავალი მომხიბლავია, დიდი ფულის ინვესტიციისთვის მაინც სახიფათო ადგილად რჩება. სხვა ტრადიციულ ვალუტებთან შედარებით კრიპტოვალუტის ფასი ძალიან სენსიტიური და მერყევია.

ამის რამდენიმე მიზეზი არსებობს, პირველი - სულ რაღაც ათეული მარკეტია, რომელიც ბიტკოინს გადახდის საშუალებად აღიქვამს.

მეორე - რეგულაციების ნაკლებობაა, კრიპტოვალუტის მთავარი იდეა დეცენტრალიზებაა, ამიტომ არ არსებობს სამთავრებო ორგანიზაცია, რომელიც მას აკონტორლებს.

რადგან კრიპტო სამყარო თანდათან უფრო მეტ ყურადღებას და პოპულარობას იძენს, ხშირია კიბერთავდასხმებიც. მართალია ბლოკჩეინი ძლიერი დაცვის სისტემაა, მაგრამ ეს იმას არ ნიშნავს, რომ ინვესტორების ექაუნთები უსაფრთხოდაა. მომხმარებლები ე.წ. "private kay" (კომპლექსურ პაროლს) იყენებენ ექაუნთებზე შესასვლელად, რომელიც, ხშირ შემთხვევაში, კომპიუტერში ინახება, რაც ჰაკერებისთვის ადვილად ხელმისაწვდომს ხდის. სამწუხაროდ ერთხელ მოპარული პაროლის დაბრუნება შეუძლებელია, პაროლის დაცვა მომხმარებლის პასუხისმგებლობაა [8].

საბოლოოდ თუ მაინც გადავწყვეტთ კრიპტოვალუტის ყიდვას, ასარჩევად 9000-ზე მეტი ვალუტა გვაქვს, თუმცა ყველა მათგანი სანდო ნამდვილად არ არის.

"OneCoin" ცნობილისახიფათო ისტორიაა კრიპტოვალუტის ისტორიაში, მისმა ლიდერებმა სამ წელიწადში მოახერხეს 4 მილიარდი დოლარის მოპარვა ინვესტორებისგან. წლების განმავლობაში მარკეტინგით და სხვადასხვა ხერხებით არწმუნებდნენ საზოგადოებას, რომ თავიანთ ვალუტას "დიდი მომავალი" ჰქონდა, სამწუხაროდ, ამ მომავალმა ინვესტორებს გვერდი აუარა[9].

ინვესტიციისთვის ყველაზე ოპტიმალური გადაწყვეტილება იმდენი ფულის გადაცვლაა, რამდენის დაკარგვაც კომფორტული და უმტკივნეულო იქნება.

კიდევ ერთი მნიშვნელოვანი მინუსი, რომელიც კრიპტოვალუტას ახასიათებს გარემოზე უარყოფითი ზემოქმედებაა. ბლოკჩეინში ახალი ბლოკების დასამატებლად და ტრანზაქციების დასადასტურებლად, რთული მათემატიკური თავსატეხების ამოხსნაა

საჭირო, რაც დიდი ენერგიის რესურს მოითხოვს. ენერგიის მოხმარება კრიპტოვალუტიტს ტიპზე და მაინინგის პროცესზე არის დამოკიდებული მაგრამ ზოგადად, კრიპტოვალუტა უფრო მეტ ენერგიას ხარჯავს ვიდრე სხვა ტრადიცული ფინანსური ორგანიზაციები. მაგალითისთვის, ბიტკოინი ყოველწლიურად ჯამური ენერგიის 0,55% იყენებს, რაც დაახლოებით ექვივალენტია მალაიზისა ან შვედეთის მიერ დახარჯული ელექტორენერგიის. უამრავი სტარტაპი ცდილობს ამ პრობლემის გადაჭრას, მაგრამ ჯერ კიდევ გარემოსდამცველების კრიტიკის საგნად რჩება კრიპტოვალუტა[10][11].

ტერას ეკოსისტემის ჩამოშლა

ყველაფერი 2018 წელსდაიწყო, Terraform labs წევრების, დოკვონისადადენიელშინისმიერ. მათიმთავარიმიზანიიყოშეემუშავებინათუნივერსალურიგადახდისსისტემა, რომელიცკრიპტოვალუტასმოსახერხებელსგახდიდაყოველდღიურცხოვრებაში. მათდაარსესბლოქჩეინისქსელი Terra, რომელიცაწარმოებდალუნათოქენებსდაშექმნესალგორითმულისტეიბლქოინი UST (Terra USD) Terra-სქსელებისთვის. ისტრადიციულისტეიბლქოინებისგანინოვაციურადგანსხვავდება, თუსხვებიგამყარებულიასტაბილურისარეზერვოასეტებით (როგორიცაადოლარი, ოქრო), UST ეყრდნობათოქენლუნას. Luna მკვიდრითოქენია, რომელსაცოთხისხვადასხვადანიშნულებააქვსტერასქსელში :

1. ტერასსტეიბლქოინისფეგის (Peg - სტაბილურიფასი) შენარჩუნება;
2. გადასახადიტრანზაქციებისგანხორციელება;
3. პლატფორმისმართვაშიმონაწილეობისმიღებაარჩევითადადამატებით;
4. ფსონისდადება, ტერასფსონისდელეგირებულიმტკიცებულების (DPoS) საბუთზექსელისგადარიცხვისშეფასებისათვის.[12]

2019 წელსლუნასჩაშვებისსაწყისიფასიიყო $1.31, მაგრამპირველი 18 თვისგანმავლობაშიდაღმავლობისტრაექტორიაზეაღმოჩნდა. მისიფასისზრდამხოლოდ 2021 წლისთებერვალშიდაიწყო, პირველადმიაღწია $6.44 დარვათვისშემდეგ, 30 სექტემბერს, Columbus-5 Mainnet-ისგანახლებისშემდეგ, მიაღწიაყველადროისნიშნულს - $49.45. ასეთმაპროგრესმაშესაძლებლობამისცაგამდიდრებულიყვნენისეთიინვესტორები, რომელთაცბევრიფულიარჰქონდათ. ასეგაიზარდამისიღირებულება 135%-ითორთვეზენაკლებდროში, 2022 წლისაპრილისპიკამდე. ასევეშესაძლებელიიყო UST-სგანთავსება Anchor-ისპლატფორმაზე, რომელიცუზრუნველყოფდა 20%-იანწლიურიშემოსავალს. ასეთმამაჩვენებლებმაანალიტიკოსებიდააეჭვადააბსურდული, არამდგრადიუწოდეს. [13]

TerraUSD (UST) ტერაალგორითმულისტეიბლქოინია, რომელიცმყარდებაარარეზერვშიშენახულიაქტივებით, არამედმეორეკრიპტოვალუტით - ლუნათოქენებით, დაეყრდნობაალგორითმებს, რომლებითაცინარჩუნებს 1$-ისფეგს (1UST=1USD)[14], რაცშემდგომმასსტეიბლქოინადაკვალიფიკაციებს. 2022 წლის 7 მაისსკისწორედესწონასწორობადაირღვადა 1UST გახდა $0.985. მიუხედავადიმისა, რომესდიდისაფრთხეარუნდაყოფილიყო, 12 მაისსისევგანმეორდავარდნადაახლაუკვე $0,10 გახდამისიფასი[15]. ესყველაფერიპირდაპირპროპორციულადაისახალუნაზედა $120-დანჩამოვიდა $0,02-მდე - 99%-იანივარდნამისიღირებულებისა. Binance (ონლაინბირჟა, სადაცმომხმარებლებსშეუძიათკრიპტოვალუტითვაჭრობა) სიიდანაგდებსლუნასდააჩერებს UST-სთრეიდინგს, ინვესტორებივეღარაკვირდებიანმიმდინარემოვლენებს. ვარდნისერთ-ერთწინაპირობად 2 მილიარდიდოლარისღირებულების UST-სგამოტანაგახდა Anchor Protocol-დან, რისგამოცასობითმილიონისტებლქოინისწრაფადიქნალიკვიდირებული. ჯერკიდევდავობენთურამგამოიწვიაეს, ინტერესებისგაზრდისსაპასუხოდთუესიყომავნეთავდასხმატერასბლოქჩეინზე. ასევეარსებობდამოსაზრებები, რომერთ-ერთიდამფუძნებელი, დოკვონი, თვეებისგანმავლობაში, არალეგალურადანაღდებდა $2.7 მილიარდს, რამაცხელიშეუწყოტერასნგრევას. მოგვიანებითმანესინფორმაციაუარყო.

ასეთიკატასტროფისგამოსასწორებლად, 28 მაისს, ახალისისტემაჩაუშვეს - Luna 2.0. ხოლოძველ, ორიგინალ, მკვიდრთოქენს, LUNA Classic (LUNC) გადაარქვეს[16]. ისინიერთადიარსებებენ, იმისმაგივრადრომძველილუნა (ახლაუკვე LUNA Classic-ადწოდებული) სრულიადჩაანაცვლონ. მათშორისერთიუდიდესიგანსხვავებაა - ახალილუნაარშეიცავსალგორითმულსტეიბლქოინს. მისმომავალსვერავინიწინასწარმეტყველებს, ასევესაეჭვოათუროგორგაიზრდებამისიფასი, ანთუგაიზრდებასაერთოდ. Terraform lab-ისდამფუძნებელისთვისსაკმაოდრთულიიქნებაინვესტორებისნდობისმოპოვება.

საბოლოოდ, ტერასდაცემაინვესტორებს $40 მილიარდზემეტიდაუჯდა. ვარდნამარამხოლოდტერასკომპანია, არამედმთელიკრიპტოვალუტისბიზნესიდააზარალა $300 მილიარდისრაოდენობით. ამმოვლენას „შავიგედი“ უწოდეს (Black swan - მოვლენა, რომლისპროგნოზირებაშეუძლებელია, მაგრამაქვსკატასტროფულიშედეგი)[17,18]. ამანკიდევუფროუარყოფითადიმოქმედებაზარზე, რომელიციმდროსძალიანარასტაბილურიდართულადმართვადიიყო. სწორედამკოლაფსისშედეგადდადგაკრიპტოვალუტაკითხვისნიშნისქვეშ. ღირსთუარაინვესტირება? აქვსრაიმემომავალი? ისევგანმეორდებათუარარომელიმეკრიპტოსვარდნა? - ამკითხვებზეპასუხიარარსებობს, მაგრამაუცილებელიათავადგანვსაჯოთგვიღირსთუარაასეთბიზნესშიჩართვადაპასუხისმგებელივართთუარაშედეგებზე [19].

Acknowledgement: This work was supported by Shota Rustaveli National Science Foundation of Georgia [SPG-22-218]

ბიბლიოგრაფია

1. "A Brief History of Encryption (and Cryptography)." Thales Group, November 21, 2022. https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption
2. Richards, Kathleen. "What Is Cryptography? Definition from Searchsecurity." Security. TechTarget, September 27, 2021. - https://www.techtarget.com/searchsecurity/definition/cryptography?amp=1
3. "Home." Cryptography and its Types. Accessed December 24, 2022. - https://www.geeksforgeeks.org/cryptography-and-its-types/amp/
4. Seth, Shobhit. "Explaining the Crypto in Cryptocurrency." Investopedia. Investopedia, December 19, 2022. - https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/
5. "How Cryptography Is Used in Cryptocurrency." World Crypto Index. Accessed December 24, 2022. https://www.worldcryptoindex.com/how-cryptography-is-used-cryptocurrency/
6. "Cryptocurrency." Definition. Accessed December 24, 2022. - https://www.trendmicro.com/vinfo/us/security/definition/cryptocurrency
7. Hertig, Alyssa. "What Is a Stablecoin?" CoinDesk Latest Headlines RSS. CoinDesk, September 16, 2022. - https://www.coindesk.com/learn/what-is-a-stablecoin/
8. Robert Roohparvar, 2022 "the cybersecurity risks of Cruptocurrency" - https://www.infoguardsecurity.com/the-cybersecurity-risks-of-cryptocurrency/
9. Emma Newbery, 2021 "what we can learn from OneCoin crypto's biggest scam?" - https://www.fool.com/the-ascent/cryptocurrency/articles/what-we-can-learn-from-onecoin-cryptos-biggest-scam/
10. YL Computing, 2022 "რა არის მაინინგი და რატომ გამოყენება კრიპტოვალუტაში?" - https://pcclean.io/ka/what-is-mining-and-why-is-it-used-in-cryptocurrency/
11. Nic Carter, 2021 "How much energy does Bitcoin actually consume?" - https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume
12. Q.ai - Powering a Personal Wealth Movement. "What Really Happened to Luna Crypto?" Forbes. Forbes Magazine, October 12, 2022.- https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=65588f304ff1
13. "Terra (Luna) Crypto Price Prediction for 2022, 2025, and 2030." StormGain, September 30, 2022. - https://stormgain.com/blog/terra-luna-price-prediction
14. "უმსხვილესისტეიბლკოინიკოლაფსშია - კრიპტო-ინდუსტრია $40-მილიარდიანისკანდალისწინაშე." bm.ge. Accessed December 24, 2022. - https://bm.ge/ka/article/umsxvilesi-steiblkoini-kolafsshia---kripto-industria-40-miliardiani-skandalis-winashe/108567
15. Krisztian Sandor and Ekin Genç. "The Fall of Terra: A Timeline of the Meteoric Rise and Crash of UST and Luna." CoinDesk Latest Headlines RSS. CoinDesk, December 22, 2022. - https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/

16. Dawn Allcot, and GOBankingRates GOBankingRates is a publication for all things personal finance. “Terra 2.0 (Luna) Price Prediction.” Nasdaq. Accessed December 24, 2022. - https://www.nasdaq.com/articles/terra-2.0-luna-price-prediction
17. CoinMarketCap. “Black Swan Event: CoinMarketCap.” CoinMarketCap Alexandria. CoinMarketCap, August 21, 2021. - https://coinmarketcap.com/alexandria/glossary/black-swan-event
18. Gagnidze, M. Iavich, G. Iashvili, Some Aspects of Post-Quantum Cryptosystems, Abstract book, EURO-ASIA FORUM IN POLITICS ECONOMICS AND BUSINESS – 2016, JULY 21-22, 2016, BELGRADE, SERBIA.
19. Increasing Usability of TLS Certificate Generation Process Using Secure Design; G. Iashvili, M. Iavich, A. Gagnidze, S. Gnatyuk; IVUS-2020; http://ceur-ws.org/Vol-2698/; 2020.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(4): 29-33 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

MODERN THREATS OF CORPORATE NETWORKS

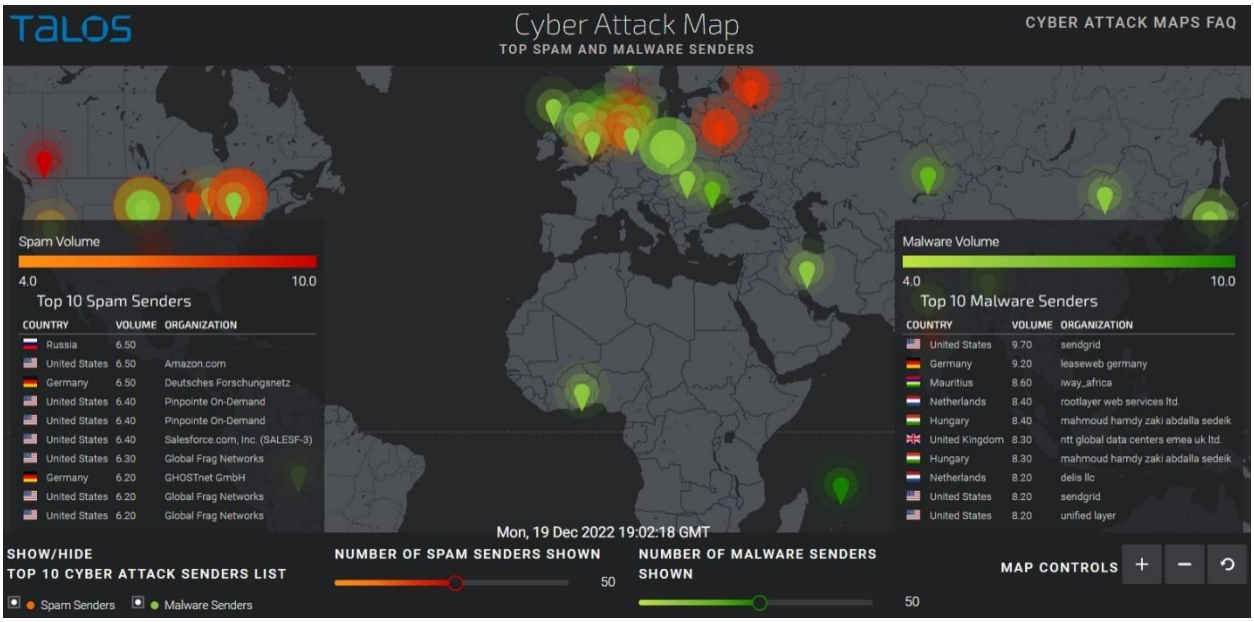
Giorgi Totladze, School Student
Nikoloz Erkomaishvili, School Student, N55 Public School
Nugzar Tomashvili, N166 Pubic Shool
Vano Mamporia, student, BTU
David Nioradze, N97 public school student

ABSTRACT:In our article, we reviewed modern threats in corporate computer networks and systems, will which cybercriminals have caused billions of dollars in damage to hundreds of medium-sized organizations and Giant Companies.we have discussed in detail the technologies through which various types of cyber-attacks were carried out around the world

KEYWORDS:*Dos Attack, Trojan, Malwares, Modern threats, Network security.*

Dos Attack

Denial of Service (DOS) attack is a type of attack that involves shutting down or delay a device or network. In other words, only one computer is used during attack and flooding servers with TCP and UDP packets. The goal of this attack is to overwhelm the target with traffic and making it inaccessible to users. The victims of this attack are such large companies as Google and GitHub on June 1, 2022, at 9:45 a.m., Google servers from 132 countries were receiving 10,000 requests per second. In exactly eight minutes, this rate increased tenfold, and this time 100,000 requests were made per second. Google's network security team immediately used the rule recommended by Cloud Armor and started blocking the traffic. In the two minutes the attack began to ramp up, growing from 100,000 Rps to a peak of 46 million Rps (request per second). Since Cloud Armor was already blocking the attack traffic, the attack continued as usual. Also, Google's work process was functioning normally. Over the next few minutes, the requests decreased significantly and finally at 10:54 am, the attacker probably determined that they did not manage to have the desired effect and slow down Google's work process, which would cause them the greatest financial loss. Also, an attack of such a scale needs huge financial support. There is a version that the attack stopped after 69 minutes because they did not get what they wantedand they could no longer see the point of continuing such an attack which requires gathering many DDOS bots and using them properly, as well as funding it all and organizing the biggest attack ever seen in the world in other words, the attackers saw that they could not achieve the result they wanted and stopped the attack and avoided spending more money. In addition to the fact that they wanted to cause financial damage by slowing down their service, they also researched how strong Google's servers are and how well they can withstand, an attack of like this and block traffic from different addresses and countries



Trojan Horseand Malwares

Trojan horse is a type of malware that can pretend to be a legitimate program whilst it attempts to cause damage. There are myriad types of trojan horses which daily infiltrate our personal computers, and corporate networks and employees might be endangered by them Rootkit Trojan: firstly aids other malicious programs by concealing their activity so they can deal Maximum harm to the victim Backdoor Trojan: can create backdoors at the corporate networks which in advance will give remote access to the hacker, having access to the network hacker can get any kind of private information it can phone numbers of employees information of debit and credit cards by knowing this information hacker can still money from employs.

Remote access tool(RAT) [1,2] : Remote access tool gives the user ability to interact with the victim's personal computer, laptop, mobile phone, or server. By giving access to a user to join the private network so the user and victim will be on the same network, viruses created with the Remote access tool can be evasive. Furthermore, the virus can cover itself instantly when it gets on the victim's gadget. If victim download or open this type of virus hackers can access their desktops, files, emails, social media accounts, and webcams too. Programs such as NJ rat, Orcus, and quasar. Belong to the family of Remote access tools (RAT)[1,2] Worm is a type of virus that can replicate itself and spread in the network If the worm bypasses security then without alarming the owner of the personal computer, network, server, etc. will install malevolent programs on the victim's workstation. This malevolent program could be any type of virus pretending a legitimate program. I love you worm I love you is a type of worm it was created in 2000 4. I love you is also known as the “love letter virus” and the “love bug worm”. It was spreading so quickly that many companies (Microsoft, Ford Motor company, as well as government organizations like the pentagon) had to completely shut down their services as they tried to mitigate virus damage. It is written in Guinness records as the most destructive virus. It was replicating himself and scanning for multi-media files and was replacing the theme His clones would lead to files being destroyed and more worms being produced. I love you worm reached 45 million users in just 10 days and eventually, it resulted in more than 15 billion worth of harm.

A Backdoor Trojan attack on a corporate network may galvanize employees to be intimidated and taken advantage of Using social engineering because this type of malware only can get into the network by downloading and opening it. gives remote access to the hacker, which in advance helps a hacker to get the credentials of the victim and can gain access to the corporate network by using the victim's (employee) computer and get private information about a company. Remote access tool(RAT) can be used like a back door trojan but it gives hackers more accurate information cause he or they can see the victim's desktop and get information about every little thing happening on the victim's (employee) computer and use this information to exploit company and hacker can camouflage themselves as a victim's persona towards others by having information about a victim.

Defense against trojans and worms

Trojan defense program technologically takes on the classic defense [3-5]. Trojans trick users by letting in their personal computer most infections, this can be avoided by remaining cautious and using good security programs. Trojans look just like a game that has been downloaded for long time or an email that was sent from unknown source or from suspicious websites offering free content, it is better to download free programs from creator's site rather than unauthorized servers. Protection against common cyber threats and cybersecurity should on front line of defending yourself. A security solution must run fast, scan and alert you if Trojan virus is detected. There are many different types of Trojans, and each can do many different things. Once Trojan is inside, it can lay low and start collecting information. As well as start making back doors without getting detected, or it could just take over your computer. There are many ways to protect yourself:

• Having a fully patched computer behind a firewall

• Run diagnostic scans

• Automatically updating your operating system, ensuring the latest security updates

• Avoiding suspicious websites

• Being skeptical of unverified attachments and links in unfamiliar emails staying behind firewall

• Using strong password

The 21st century is the time that most people call the era of technology and the era of opportunity. Imagine in the 1950s if you told your friend who is in France, you would see him and talk to him from America. Your friends would laugh at you and consider you crazy, but today modern means of communication allow us to reduce the distance to a minimum and through virtual reality work together on different projects even from different continents of the earth. Cyberwar is one of the mandatory things when there is any conflict between countries [6]. By means of cyber war and the secret information obtained, the country can use all this to its advantage. Securing your company's digital data is incredibly important if you want to protect the sensitive data that might be contained on your network and computers, whether it be employee data, customer data, or company secrets. But no system is safe. A simple example of this is the well-known story of how a Russian hacker hacked the FBI with just one computer and symbolically left 1 dollar in all FBI bank accounts. Here I will also say thatthe program can help a person but not change the brain. Most people will understand what I want to say with all this later. Evgeniy Bogachev is a Russian hacker who has been indicted by the United States Department of Justice for his alleged role in several high-profile cyberattacks. He is believed to be the mastermind behind the Gameover Zeus botnet, which was used to steal sensitive information from computers around the world. In 2015, the U.S. government offered a $3 million reward for information leading to his arrest and prosecution. According to the public opinion Bogachev showed everyone that we can achieve a lot without support of servers and huge hardware. The main thing here is our brain and how we use it. The program can help a person but not change the brain. Perhaps you will have a question: How was the attack organized? While Bogachev knowingly acted in a role as an administrator, others involved in the scheme conspired to distribute spam and phishing emails, which contained links to compromised websites [7]. Victims who visited these websites were infected with the malware whichBogachev and others utilized to steal money from victim’s bank accounts.

Conclusions:

As we can see from our research, we investigated various well-known methods of compromising modern computer networks, as well as methods and technologies for protecting against such threats. The main thing is that we have received special skills to analyze different degrees of threats in modern computer networks and have learned the process of implementing these technologies in real everyday network service.

Acknowledgement: This work was supported by Shota Rustaveli National Science Foundation of Georgia [SPG-22-218]

BIBLIOGRAPHY

1. Johnson, N.T.; Waddell, P.G.; Clegg, W.; Probert, M.R. Remote Access Revolution: Chemical Crystallographers Enter a New Era at Diamond Light Source Beamline I19. *Crystals* 2017, *7*, 360. https://doi.org/10.3390/cryst7120360
2. D. Hou, Z. Miao, H. Xing and H. Wu, "V-RSIR: An Open Access Web-Based Image Annotation Tool for Remote Sensing Image Retrieval," in *IEEE Access*, vol. 7, pp. 83852-83862, 2019, doi: 10.1109/ACCESS.2019.2924933.
3. Z. Huang, Q. Wang, Y. Chen and X. Jiang, "A Survey on Machine Learning Against Hardware Trojan Attacks: Recent Advances and Challenges," in *IEEE Access*, vol. 8, pp. 10796-10826, 2020, doi: 10.1109/ACCESS.2020.2965016.
4. D. Yang, C. Gao and J. Huang, "Dynamic Game for Strategy Selection in Hardware Trojan Attack and Defense," in IEEE Access, vol. 8, pp. 213094-213103, 2020, doi: 10.1109/ACCESS.2020.3040395.

5. K. S. Subramani, N. Helal, A. Antonopoulos, A. Nosratinia and Y. Makris, "Amplitude-Modulating Analog/RF Hardware Trojans in Wireless Networks: Risks and Remedies," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3497-3510, 2020, doi: 10.1109/TIFS.2020.2990792.
6. Maksim Iavich, SergiyGnatyuk, Giorgi Iashvili, AndriyFesenko, ENSURING EUROPEAN CIVIL AVIATION CYBERSECURITY, Scientific and practical cyber security journal, 2019.
7. Maksim Iavich, SergiyGnatyuk, Giorgi Iashvili, AndriyFesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(4): 34-39 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

PYTHON USE IN GAMING

Nikoloz Tchitanava Student at the "Tbilisi's Archimede's School"
Luka Tchitanava, Student at the "Atitanti School"
Dachi Beridze, Student at the "Tbilisi N147 Public School"
Beqa Chxirodze, Student at the"N169 Public School"

ABSTRACT: In this article,we talk about Usage of Python programming language in gamedevelopment: advantages,disadvantages,engines working on python and comparison with the different programming languages used for game creation.
Our research shows that, python is the best choice for 2D games. It gives developers ability to create the game easily and quickly.
KEYWORDS: python, game, 2D games

Introduction:

We live in the most technologically advanced era. This helps different fields like game development.The video games industry is growing every single day. Because of corona virus, people spent lots of time at their homes. They had free time and no place to go, so majority of worlds population started spending more time on their gadgets. During this boom, not only the players, but also the people who wanted to learn game development doubled in numbers.In 2022, the number of gamers worldwide was estimated at three billion, down from the 3.2 billion global gamers during the height of COVID-19 in 2021. Despite this momentarily decline, global gaming audiences are projected to increase at a steady growth rate. Number of game developers raised by 37% in 2021,yet the games industry is experiencing a tremendous global skills shortage. Nor is it not getting easier to match the right talent with the right opportunity, especially given the additional challenges brought on by remote work and distributed teams. A change is desperately needed.So, for people who want to become game developers in the future, python based game engines might be the best first step.

First Video games

Scientist William Higginbotham is credited with developing the first video game in October 1958. It was a relatively simple tennis game that played similarly to the legendary video game Pong from the 1970s. He had a little analog computer that could show different curves on an oscilloscope, including the trajectory of a ball in motion. Higginbotham needed a few hours to develop the concept for a tennis game and a few days to put the fundamental components together. Higginbotham had no issue building the straightforward game display because he had experience designing displays for radar systems and other electrical equipment.

Drawings by Higginbotham were used to create plans. About two weeks were spent developing the device by technician Robert Dvorak. The first video game was ready for release after some debugging. Tennis for Two was the name of the game. Players could push a button to hit the ball in the direction of their opponent and spin a knob to change the ball's angle. Players couldn't miss the ball as long as they pressed the button in their court, but if they hit it at the wrong moment or tilted, the ball wouldn't cross the net. A ball would bounce like a tennis ball when it struck the ground. The players pressed a reset button to begin the following round once the ball left the court or went through the

net. Tennis for Two needed more modern video games' sophisticated graphics. A side image of a tennis court with only two lines—one for the net and one for the ground—was displayed on the cathode ray tube display. The ball was merely a dot that moved back and forth. Players have to keep track of their scores as well. Many resistors, capacitors, and relays were used in the game's circuitry, but transistors were also used for the quick switching required when the ball was in play. Unfortunately, they could not develop the engines that would have allowed other developers to produce their games at the time. They were forced to start from scratch each time as a result.[1]

Game engine description

A game engine is a software architecture primarily made for video games. It typically comes with essential libraries and assistance applications. Game engines are tools developers can use to create games for computers and other gaming platforms. The primary features that a game engine often offers include rendering engines ("renderers") for 2D or 3D graphics, physics engines or collision detection (and response), sound, scripting, animation, artificial intelligence, networking, streaming, memory management, threading, localization support, scene graph, and video support for cinematics. Implementers of game engines frequently save money on the game production process by reusing/adapting, in large part, the same game engine to produce other games or to help with game porting to numerous platforms. For instance, a game for the Atari 2600 had to be created from the ground up to best use the display hardware. Today, makers of games for older systems refer to this basic display routine as the kernel. Although there was more room for maneuvering other systems,[2] memory limitations frequently prevented the data-heavy designs that an engine requires. Very little could be reused between games, not even on more forgiving platforms. Most of the code had to be thrown out later anyway because following generations of games would employ entirely different game designs that took advantage of more excellent resources due to the rapid advancement of arcade hardware, which was the leading edge of the market at the time. Because of this, most game designs from the 1980s used a fixed set of rules, a limited amount of levels, and graphics data. Since the heyday of arcade games, it has become customary for video game developers to create their game engines for use with first-party software. The fluid side-scrolling engine created by Shigeru Miyamoto's team at Nintendo for the Nintendo Entertainment System was a prominent example of an in-house game engine on home consoles in the middle of the 1980s (NES). Super Mario Bros later used the technology they had created for the side-scrolling racing game Excite bike, which was released in 1984. (1985). As a result, Mario could easily transition from a stroll to a run rather than moving at a fixed speed, like in earlier platform games. Even though third-party game engines were uncommon until the emergence of 3D computer graphics in the 1990s, several 2D game creation systems were created for independent video game development in the 1980s. Pinball Construction Set (1983), ASCII's War Game Construction Kit (1983Th), under Force Construction (1984), Adventure Construction Set (1984), Garry Kitchen's Game Maker (1985), Wargame Construction Set (1986), Shoot-'Em-Up Construction Kit (1987), Arcade Game Construction Kit (1988), and most notably ASCII's RPG Maker engines from 1998 onwards are some of them. Another classic title still accessible is Click & Play (1994).

Around the middle of the 1990s, the phrase "game engine" came into use, particularly about 3D games like first-person shooters that used a first-person shooter engine. Unreal Engine was first released in 1998 by Tim Sweeney's company, Epic Games. Since Doom and Quake by Id Program were so well-liked, other developers decided to license the core software instead of starting from scratch and creating their graphics, characters, weapons, and levels referred to as "game content" or

"game assets." Teams could expand and specialize due to the separation of game-specific rules and data from fundamental ideas like collision detection and game entities. Later games, with the engine and content developed independently, used a similar strategy, including Epic Games' 1998 Unreal and id Software's Quake III Arena. A high-end commercial gaming engine license can cost anywhere between US$10,000 and millions. Then several appointments might exceed several dozen businesses, as seen with the Unreal Engine. Licensing technologies have proven to be a valuable supplemental revenue source for several game producers. At the very least, reusable engines expedite and simplify the process of creating game sequels, an essential benefit in the cutthroat video game market. Around 2000, there was intense competition between Epic and id, but since then, Unreal Engine from Epic has become far more well-liked than id Tech 4 and its successor, id Tech 5. One of the most complicated programs ever created, modern game engines frequently contain dozens of intricately tuned modules that interact to provide a tightly regulated user experience. Level design, rendering, scripting, and art have become distinct due to the ongoing development of gaming engines. For instance, an average game development team now typically has far more artists than actual programmers.[3][4][5]

Python based game engines

Game engines for Python most often take the form of Python libraries, which can be installed in a variety of ways. Most are available on PyPI and can be installed with pip. However, a few are available only on GitHub, GitLab, or other code sharing locations, and they may require other installation steps.

Pros and cons of python based game engines compared to others

Python is a general purpose programming language, and it’s used for a variety of tasks other than writing computer games. In contrast, there are many different stand-alone game engines that are tailored specifically to writing games. Some of these include:

The Unreal Engine

Unity

Godot

These stand-alone game engines differ from Python game engines in several key aspects:

Language support: Languages like C++, C#, and JavaScript are popular for games written in stand-alone game engines, as the engines themselves are often written in these languages. Very few stand-alone engines support Python.Proprietary scripting support: In addition, many stand-alone game engines maintain and support their own scripting languages, which may not resemble Python. For example, Unity uses C# natively, while Unreal works best with C++.

Platform support: Many modern stand-alone game engines can produce games for a variety of platforms, including mobile and dedicated game systems, with very little effort. In contrast, porting a Python game across various platforms, especially mobile platforms, can be a major undertaking.

Licensing options: Games written using a stand-alone game engine may have different licensing options and restrictions, based on the engine used.

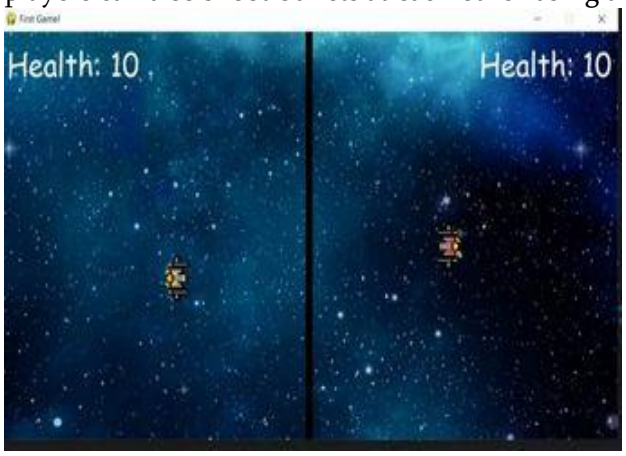
So why use Python to write games at all? In a word, Python. Using a stand-alone game engine often requires you to learn a new programming or scripting language. Python game engines leverage your existing knowledge of Python, reducing the learning curve and getting you moving forward quickly.There are many game engines available for the Python environment. The engines that you’ll learn about here all share the following criteria:They’re relatively popular engines, or they cover

aspects of gaming that aren't usually covered.They're currently maintained.They have good documentation available.[6][7]

Our project
For this research, we created the game.Here is the summary of it.

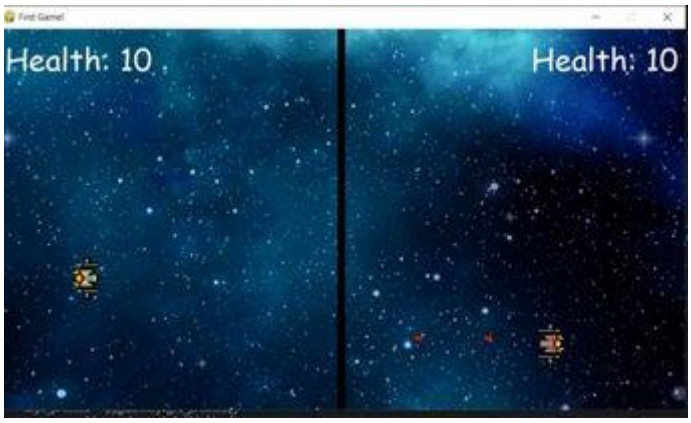
Gamedescription:

A game where two spaceships fight each other. The game has two players, one controlling a red spaceship and the other controlling a yellow spaceship. The players can move their spaceships around the screen using the WASD keys for the yellow player and the arrow keys for the red player. The players can also shoot bullets at each other using the control keys.



The game has a health bar for each player, and the player whose health reaches 0 first loses the game. The game also has a border that divides the screen in half and that the spaceships cannot pass through. The game displays the current health of each player on the screen, as well as the spaceships and any bullets that have been fired.

The game has a fixed frame rate of 60 frames per second and the spaceships and bullets move at a fixed velocity. The game has a maximum of 3 bullets that can be on the screen at any given time for each player. Also, it has an event system that can be triggered by the players getting hit by bullets, which causes the spaceship to flash and become invulnerable for a short period of time.



Conclusions:

main problem was downloading the pygame itself. Sometimes the operating system or code writing environment may give you hard time using the library. Code writing is simple, the syntaxes are easy to remember and it does not need much time to run. It takes around 5 hours to create the mini game, that you can enjoy later with your friends. It will also help you to understand the main principles of game creation, which you can also use in different engines. Unfortunately, python based game engines are suitable just for the 2D games such as platformers*. It is not for creating big projects like AAA* and AA* games. But, if you are new to game development(like us), python based game development is great, because it is much more easy than other engines such as “Unreal engine” or “Unity”.

Footnotes:

AAA games-The term "AAA Games" is a classification used within the video gaming industry to signify high-budget, high-profile games that are typically produced and distributed by large, well-known publishers. These games often rank as “blockbusters” due to their extreme popularity.

AA games-“AA” (although rarely used) means budgets around just several million.

Platformers-A platform game, commonly referred to as a “platformer,” is a style of video game where the player makes a character move through an environment with a series of action-based moves, like running, jumping, or swinging from ropes.

Acknowledgement: This work was supported by Shota Rustaveli National Science Foundation of Georgia [SPG-22-218]

REFERENCES

1. Alan Chodos, This Month in Physics History, APS News, 2008 (Volume 17, Number 9)
2. What is a Gaming of Game Engine, ARM Glossary https://www.arm.com/glossary/gaming-engines
3. What is a Game Engine?,Fullscale IO https://fullscale.io/blog/what-is-game-engine/

4. The Complete Game Engine Overview, Perforce https://www.perforce.com/resources/vcs/game-engine-overview
5. PyGame: A Primer on Game Programming in Python https://realpython.com/pygame-a-primer/
6. Jon Fincher, Top Python Game Engines https://realpython.com/top-python-game-engines/

Scientific and Practical Cyber Security Journal (SPCSJ) 6(4): 40-56 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

OSINT & AI

OSINT და ხელოვნური ინტელექტი

Alex Naskidashvili, School Student
ალექსი ნასყიდაშვილი, სკოლის მოსწავლე
Alexandre Mizandari, School Student
ალექსანდრე მიზანდარი, სკოლის მოსწავლე
Irakli Chxaidze, School Student
ირაკლი ჩხაიძე, სკოლიდ მოსწავლე
Vladimir Elizarovi, School Student
ვლადინირ ელიზაროვი, სკოლის მოსწავლე

ABSTRACT: In today's world where everyone leaves a cyber trail, it's hard to track things down.Therefore, this information can be used against this person, which in many cases has bad consequences. This work is about specific methods and programs that help us find and analyze specific information. Also worth noting is the importance of artificial intelligence (AI) in recent years. It already plays an important role in many other fields, for example in the medical field, therefore it has a great influence on OSINT today, which is manifested in the fact that many individual and different tools are created (IBM Watson, Maltego, KNIME).

KEYWORDS: *OSINT, Vulnerability, Information, Artificial Intelligence, Tools, Tools Usage*

ანოტაცია: დღევანდელ სამყაროში, სადაც ყოველი ადამიანი ტოვებს კიბერ კვალს, რთულია რამის დამავლა. აქედან გამომდინარე ეს ინფორმაცია შეიძლება იყოს გამოყენებული ამ ადამიანის მიმართ, რასაც ხშირ შემთხვევაში ცუდი შედეგები მოყვება.ამ ნამუშევარში საუბარია სწორედ კონკრეტული ხერხებზე და პროგრამებზე, რომლებიც გვეხმარებიან სპეციფიკური ინფორმაციის მოძიებაში და გაანალიზებაში.ასევე აღსანიშნავია ბოლო წლებში ხელოვნური ინტელექტის (AI) მნიშვნელობა. მას უკვე სხვა მრავალ სფეროში მნიშვნელოვანი როლი უჭირავს, მაგალითად სამედიცინო სფეროში, აქედან გამომდინარე მან დიდი გავლენით OSINT -ზე მოქმედებს დღესდღეობით, რაც გამოიხატება იმაში, რომ ბევრი ინდივიდუალური და განსხვავებული ინსტრუმენტი იქმნება (IBM Watson, Maltego, KNIME).

საკვანძო სიტყვები: *OSINT, სისუსტეები, ინფორმაცია, ხელოვნური ინტელექტი, ხელსაწყოები, ინსტრუმენტების მოხმარება*

რა არის OSINT ?

OSINT ანუ Open Source Intelligence – ნიშნავს ინფორმაციის მოგროვება / გამოძიება ღია წყაროების გამოყენებით. ეს არის ტექნიკისა და ინსტრუმენტების ერთობლიობა, რომელიც გამოიყენება საჯარო ინფორმაციის და მონაცემთა შეგროვებისთვის, გარკვეული მიზნებისა და სფეროების სასარგებლო და გამოყენებადი ცოდნის მისაღებად.

დღეს ინტერნეტი წარმოადგენს ინფორმაციის უდიდეს ნაკადს, რაც ერთდროულად არის როგორც სასარგებლო, ასევე, ზოგ შემთხვევაში, მავნებელიც კი.

ინტერნეტის დადებით მხარეს მონაცემთა მაქსიმალური ხელმისაწვდომობა წარმოადგენს, რაც ნიშნავს იმას, რომ ინფორმაციის გარკვეული ნაწილი ე.წ. ღია წვდომაშია, აქედან გამომდინარე ნებისმიერ მსურველს, პრაქტიკულად, ნებისმიერი ინფორმაციის მიღება შეუძლია.

უარყოფითი მხარე, ამ შემთხვევაში, ბოროტმოქმედის მიერ მიღებული ინფორმაციის გამოყენებაა. ინფორმაციის მავნე მიზნებით გამოყენების ერთ-ერთი ნათელი მაგალითია ფიშინგი, როდესაც მსხვერპლის ელ-ფოსტაზე სპეციალური მავნე კონტენტის შემცველი წერილი იგზავნება. კონტენტი შეიძლება იყოს სხვადასხვა სახის, დაწყებული უბრალო ტექსტით, დამთავრებული ვიდეო ან აუდიო ჩანაწერებით.

OSINT შეიძლება იყოს გამოყენებული ორი მიმართულებით:

პირველი მიმართულება ინტერნეტ სივრცეში გამოძიებაა, რომელიც საჭირო ინფორმაციის მოპოვებასა და სხვადასხვა პირს შორის სხვადასხვა კავშირის დადგენაში ეხმარება. OSINT - ის მეშვეობით, იზოგება სოლიდური თანხები, რადგან ამ ტიპის გამოძიების მეთოდების გამოყენებით, ორგანიზაციებს შორის თაღლითობის რისკი (ინტერესთა კონფლიქტის მაგალითები) საგრძნობლად მცირდება.

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).

რაში გამოიყენება OSINT ?

OSINT შექმნილ იქნა აშშ-ში 1940-იან წლებში, საერთაშორისო მაუწყებლობის მონიტორინგის სამსახურებთან ერთად. მისი თანამშრომლები ახორციელებდნენ უცხო ქვეყნების რადიო გადაცემების ჩაწერასა და ანალიზს, რის შემდეგაც მონაცემები ანგარიშების სახით გადაეცემოდა სამხედრო და სადაზვერვო უწყებებს. CIA-ს და პენტაგონის ზოგიერთი ოფიციალური პირის მიხედვით, აშშ-ს ხელმძღვანელობამ ინფორმაციის 80% ღია წყაროებიდან იღებს და მხოლოდ 20% ფარული წყაროებიდან.

დღესდღეისობით ღია წყაროების სადაზვერვო ინფორმაციას იყენებენ არა მხოლოდ სამთავრობო უსაფრთხოებისა და თავდაცვის უწყებები, არამედ კერძო კომპანიებიც.

OSINT მეთოდები, მიზნად ისახავს ზოგადი ინფორმაციის შეგროვებას მარტივად ხელმისაწვდომი წყაროებიდან და საშუალებას იძლევა მიიღოთ ობიექტის შესახებ ზოგადი ინფორმაცია. ინფორმაცია გროვდება მექანიკურად ან სპეციალური სერვისებისა და

ხელსაწყოების დახმარებით, რომლებიც ამარტივებს მონაცემთა შეგროვებას, სისტემატიზაციასა და ანალიზს.

OSINT-ის საშუალებით შესაძლებელია მარტივად იპოვოთ ხარვეზები და სისუსტეები საკუთარ უსაფრთხოების სისტემაში, მომხმარებელთა ინფორმაციის დაცვაში, ასევე შეგიძლიათ გაიგოთ სამიზნე აუდიტორიის ფსიქოლოგიური თავისებურებები და საჭიროებები.

IT ინდუსტრიასა და ინფორმაციის უსაფრთხოებაში OSINT ეხმარება კონკურენტების შესახებ ინფორმაციის შეგროვებას, ობიექტების უსაფრთხოების ანალიზს, უსაფრთხოების ხარვეზების, ინფორმაციის გაჟონვისა და შესაძლო საფრთხეების და მათი წყაროების აღმოჩენაში.

OSINT შესაძლებელია გამოყენებულ იქნას არა მხოლოდ ლეგიტიმური, არამედ უკანონო მიზნებისთვისაც. მაგალითად, თავდამსხმელს შეუძლია მოიპაროს მომხმარებლის პირადი მონაცემები და ინფორმაცია პირის ან ორგანიზაციის საქმიანობის შესახებ; მოიპოვოს კონფიდენციალური ინფორმაცია და გამოიყენოს იგი შანტაჟის, გამოძალვისთვის და სხვა.

AI -ს ამოყენება OSINT-ში

ხელოვნური ინტელექტი (AI) შეიძლება გამოყენებულ იქნას OSINT-თან ერთად ინფორმაციის შეგროვების პროცესის ავტომატიზაციისა და ეფექტურობის გასაუმჯობესებლად. მაგალითად, ხელოვნური ინტელექტის ალგორითმები შეიძლება ივარჯიშონ, რათა ამოიცნონ და ამოიღონ შესაბამისი ინფორმაცია დიდი მოცულობის ონლაინ მონაცემებიდან, როგორიცაა სოციალური მედიის პოსტები. ეს შეიძლება დაეხმაროს ორგანიზაციებს დაზოგონ დრო და რესურსები, რომლებიც სხვანაირად დაიხარჯებოდა ინფორმაციის ხელით მოპოვებაში.

ხელოვნური ინტელექტის გამოყენება ასევე შეიძლება OSINT-ის საშუალებით შეგროვებული ინფორმაციის გასაანალიზებლად და ინტერპრეტაციისთვის. მაგალითად, ხელოვნური ინტელექტის სისტემას შეუძლია განსაზღვროს შაბლონები ან კავშირები ერთი შეხედვით დაუკავშირებელ ინფორმაციას შორის, ან იწინასწარმეტყველოს მომავალი მოვლენები წარსული ტენდენციების საფუძველზე.

AI-ს გამოყენების ერთ-ერთი მთავარი უპირატესობა OSINT-თან ერთად არის დიდი რაოდენობით ინფორმაციის სწრაფად და ზუსტად დამუშავების შესაძლებლობა. ეს შეიძლება იყოს განსაკუთრებით გამოსადეგი სიტუაციებში, სადაც დრო მნიშვნელოვანია, როგორიცაა ეროვნული უსაფრთხოების პოტენციურ საფრთხეზე რეაგირება.

თუმცა, მნიშვნელოვანია აღინიშნოს, რომ AI-ზე დაფუძნებული OSINT არ არის შეზღუდვების გარეშე. ყველა ხელოვნური ინტელექტის სისტემის მსგავსად, ის მხოლოდ ისეთივე კარგია, როგორც მონაცემები, რომლებზედაც ვარჯიშობს და ექვემდებარება მიკერძოებას და შეცდომებს, თუ სასწავლო მონაცემები არ არის რეპრეზენტატიული ან ზუსტი. გარდა ამისა, AI-ზე დაფუძნებულ OSINT სისტემებს შეიძლება არ შეეძლოთ გარკვეული ტიპის

ინფორმაციაზე წვდომა, როგორიცაა ინფორმაცია, რომელიც დაცულია კონფიდენციალურობის კანონებით ან ხელმისაწვდომია მხოლოდ ფარული ან უკანონო საშუალებებით.

მთლიანობაში, ხელოვნური ინტელექტი შეიძლება იყოს ძლიერი ინსტრუმენტი OSINT-ის ეფექტურობის გასაუმჯობესებლად, მაგრამ მნიშვნელოვანია მისი პასუხისმგებლობით გამოყენება და ინფორმაციის სხვა წყაროებთან ერთად გამოყენების უზრუნველყოფა სრული და ზუსტი სურათის უზრუნველსაყოფად.

AI ტექნოლოგია აგრძელებს წინსვლას ასტრონომიული ტემპით, ასევე ხდება მისი აპლიკაციები OSINT -ითვის. ქვემოთ მოცემულია ჰიპოთეტური სცენარი, რომელიც ხაზს უსვამს AI -ს გამოყენებით OSINT გამოძიებაში.

პროცესის მაგალითი:

1. გამომძიებელი იღებს ხაზგასმული მონაცემების ნაწილებს ავტომატური AI ალგორითმიდან, ვთქვათ, ეს ალგორითმი აღმოაჩენს საკვანძო სიტყვებს ან ფრაზებს, რომლებიც მონიშნულია Twitter-ში ან chatroom-ის პოსტებში.

2. ისინი აღნიშნავენ სიმბოლოს არსებობას, რომელიც ეხება კონკრეტულ ექსტრემისტულ ჯგუფს.

3. Web Crawlers აგროვებს ინფორმაციას ათასობით წყაროდან, როგორიცაა სოციალური მედია, ინგლისური ან უცხოენოვანი მედია, ახალი ამბების ამონარიდები და ა.შ.

4. შეგროვებული ინფორმაცია იწარმოება წინასწარ განსაზღვრული AI ალგორითმების მეშვეობით, რომლებიც შექმნილია შაბლონების იდენტიფიცირებისთვის ან გეოგრაფიული/დროებითი პროფილის შესაქმნელად.

5. დაზვერვის ანგარიში შემდეგ ავტომატურად გენერირდება მომხმარებლის პრეფერენციების მიხედვით. მიუხედავად იმისა, რომ არცერთი ეს შემთხვევა არ შეიძლება რევოლუციურად გამოიყურებოდეს სადაზვერვო პროცესისთვის, ეფექტურობა, რომლითაც AI-ები მუშაობენ, მნიშვნელოვნად აუმჯობესებს პროცესს და ანალიტიკოსს საშუალებას აძლევს მეტი დრო დახარჯოს ანალიზზე. ამაში მდგომარეობს AI ტექნოლოგიის მთავარი სარგებელი OSINT ციკლში. AI-ს ყველა ამ აპლიკაციის OSINT-ში გადაკვეთამ და ტექნოლოგიის შემდგომმა განვითარებამ შეიძლება იდეალურად მიგვიყვანოს AI-მდე, რომელსაც შეუძლია სწრაფად ამოიცნოს შესაბამისი ინფორმაცია ყველა წყაროზე და მიაწოდოს ის საბოლოო მომხმარებელს, ან სხვა სიტყვებით რომ ვთქვათ, შექმნას „Siri“ უსაფრთხოების კლირენსი“

რა tools -ები არსებობს

1) OSINT Framework

ეს წარმოადგენს ყველაზე სრულყოფილ ღია კოდის მონაცემთა ბაზას, წყაროები დაჯგუფებულია კატეგორიების მიხედვით. შეიძლება გაიხსნას კონკრეტული კლასი, შემდგომში იყოს წვდომა ქვეკლასზე და მოძებნოს ინფორმაციის კონკრეტული წყარო.

OSINT Framework-ის დახმარებით შეგიძლიათ იპოვოთ ინფორმაცია ისეთი კრიტერიუმით, როგორიცაა ელფოსტა, ტელეფონის ნომერი, IP მისამართი, სოციალური ქსელები და მრავალი სხვა.

2) Metagoofil

ეს არის მეტაძიების სისტემა, რომელიც იყენებს სხვა საძიებო სისტემებს საჯაროდ ხელმისაწვდომი PDF, Word, Powerpoint და Excel ფაილების მოსაძებნად და მისაღებად. ეს შეგიძლიათ გამოიყენოთ ტექნიკური დოკუმენტაციის, კლიენტის მონაცემთა ბაზების, დირექტივების, კატალოგებისა და სხვა სასარგებლო ინფორმაციის გასაანალიზებლად.

3) Shodan

ეს არის საძიებო სისტემა, რომელიც შექმნილია IPv4 მისამართებით ინტერნეტთან დაკავშირებული მოწყობილობების მოსაძებნად, როგორიცაა მარშრუტიზატორები, ვიდეო სათვალთვალო კამერები, უსაფრთხოების სენსორები და ა.შ. მისი დახმარებით ნებისმიერ მსურველს შეუძლია იპოვოს დაუცველი ან ნაკლებად დაცული მოწყობილობა, დაამონიტორინგოს და მიიღოს საინტერესო ინფორმაცია. ეს სახელი მან მიიღო System Shock თამაშების ანტაგონისტის, შეშლილი ხელოვნური ინტელექტისგან.

4) SpiderFoot

კიდევ ერთი სასარგებლო სადაზვერვო ინსტრუმენტს წარმოადგენს SpiderFoot, რომელიც საშუალებას გაძლევთ შეაგროვოთ მაქსიმალური ინფორმაცია ნებისმიერი საიტის ან სერვერის შესახებ. SpiderFoot არის სადაზვერვო ინსტრუმენტი, რომელიც ავტომატურად ასკანირებს ასზე მეტ საჯარო მონაცემთა წყაროს, რათა შეაგროვოს ინტელექტუალური ინფორმაცია IP მისამართებზე, დომენის სახელებზე, ელფოსტის მისამართებზე და ა.შ.

5) OpenAI

OpenAI არის კვლევითი ორგანიზაცია, რომელიც ორიენტირებულია ხელოვნური ინტელექტის (AI) ტექნოლოგიების განვითარებაზე. იგი დაარსდა 2015 წელს მაღალი დონის ტექნიკური ლიდერების ჯგუფის მიერ, მათ შორის ილონ მასკი, სემ ალტმანი, გრეგ ბროკმანი, ილია სუცკევერი და ვოიცეჩ ზარემბა, მეგობრული AI-ის განვითარებისა და განვითარების მიზნით.

Google Dorking

დღეისთვის Google-ის საძიებო სისტემას თითქმის ყველა ვებ-საიტი აქვთ დასკანირებული და დაინდექსიერებული, რათა მომხმარებელმა შეძლოს სწორი ინფორმაციის სწრაფად მიღება. თუმცა ეს შეიძლება იყოს გამოყენებული სულ სხვა გზით. ამაში მათ ეხმარებას Google Dorking-ი

Google Dorking - ეს არის ინფორმაციის გაფართოებული ძიების ინსტრუმენტი, რომელიც Google საძიებო სისტემას იყენებს და ამავდროულად გამოიყენება ვებ-საიტის სისუსტეების აღმოჩენაში და კონფიგურაციული ინფორმაციის პოვნაში, მაგალითად ფაილების ან დამალული გვერდების. Dork queries ბევრი ადამიანი განიხილავს, როგორც "ჰაკირების ტექნიკად". მისი ბუნების გამო, დაუცველობა შეიძლება გამოყენებულ იქნას სხვადასხვა მიზნებისთვის და ძალიან ხშირად ცუდი მიზნებისთვის.

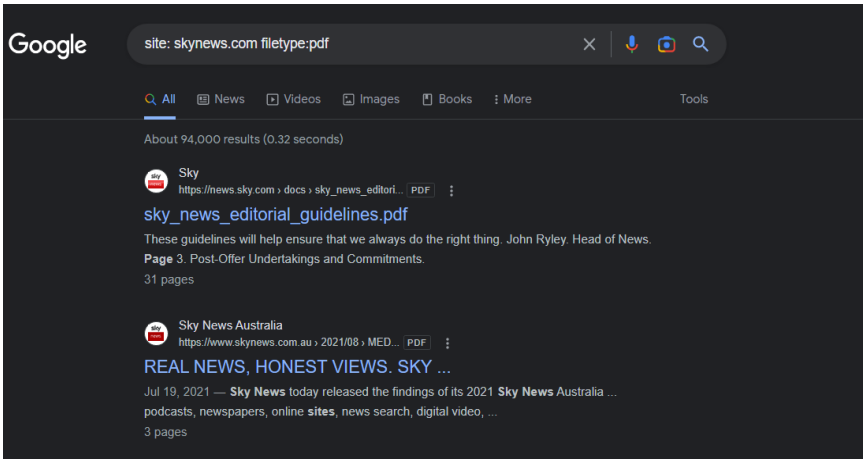
საჭირო ინფორმაციის მოსაძიებლად არსებობს Google-მა შექმნა სპეციალური მოთხოვნების ენა, რომელშიც სპეციფიური ნიშნები და ოპერატორები გვეხმარებიან. მაგალითად სპეციფიკური ნიშნები არიან:

- ვარსკვლავი [*] -რომელიც შეიძლება იყოს ჩანაცვლებული ნებისმიერი სხვა სიტყვით.
- ტილდი [~] - რომელიც ეძებს სიტყვის სინონიმებს
- მინუსი [-] - ანუ ძიებიდან რაღაცა სიტყვის წაშლა
- ბრჭყალები [“] - ვთქვათ, თუ გვინდოდა შევავიწროვოთ საძიებო მოთხოვნა, შეგვიძლია გამოვიყენოთ ციტატები. Google ამ ბრჭყალებს შორის არსებულ ყველაფერს ზუსტად განმარტავს და მხოლოდ მოწოდებული ფრაზის შედეგებს დააბრუნებს

ხოლო პოპულარული ოპერატორები:

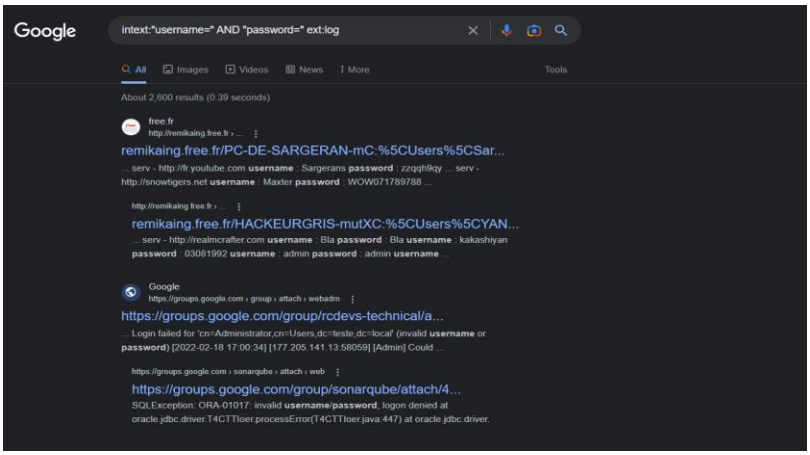
- filetype - რომელიც ფაილების ტიპებს მიხედვით ეძებს
- site - მხოლოდ კონკრეტული საიტი მოძებნოს
- inurl - მოვიძიოთ კონკრეტული სიტყვა, რომელიც URL შეიცავს
- intitle - მოვიძიობთ სიტყვა ან წინადადება ვებ-საიტის სათაურში.

ამიერად Google Dorking-ი ხდის უფრო კომფორტულ და სწრაფ მუშაობას მის საძიებლო სისტემასთან. მაგალითად skynews.com ვესაიტზე გვინდა მხოლოდ pdf ფაილები ამოგვიგდოს. ამისთვის ბრაუზერის search ხაზში ვწერთ ამას: site: skynews.com filetype:pdf . (სურ. 1)



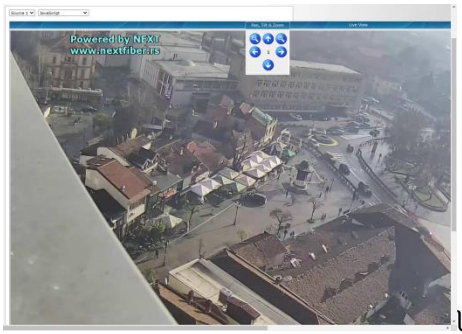
სურათი 1 skynews.com ვებ-საიზე აღმოჩენილი Pdf ფაილები

მაგრამ პარალელურად შეიძლება ეს გამოყენებული იქნას პაროლების ან კრიტიკული სისუსტეების მოსაძიებლად. მაგალითად სურ. 2 -ზე ასახულია მომხმარებლის სახელები და პაროლები.



სურათი 2 მოძებნილი სახელები და პაროლები

თუ გარკვეული უბნების მონიტორინგს გვესაჭიროება, Google Dorking დაგვეხმარება რეალურ დროში კამერების პოვნაში მნიშვნელოვანი IP შეზღუდვების გარეშე. Google Dorking-ი გვაძლევს წვდომას სხვადასხვა პირდაპირ ეთერში გლობალურად, მათ შორის სამხედროებისა და მთავრობის კამერებზე. ამისთვის ეს მოთხოვნილება უნდა გავაგზავნოთ: intitle: Webcamxp 5. (სურ.3)



სურათი 3 Google Dorking -ით მოძიებული კამერა

Shodan

Shodan არის საძიებო სისტემა ინტერნეტთან დაკავშირებული მოწყობილობებისთვის. იგი შეიქმნა 2009 წელს ჯონ მეთერლის მიერ და ხშირად მოიხსენიება როგორც "გუგლი ჰაკერებისთვის". პლატფორმა მომხმარებლებს საშუალებას აძლევს მოძებნონ ინტერნეტთან დაკავშირებული კონკრეტული ტიპის მოწყობილობები ან სერვერები, როგორიცაა ვებკამერები, მარშრუტიზატორები, სერვერები და სხვა.

Shodan-ის ერთ-ერთი უნიკალური მახასიათებელია მისი უნარი იპოვოს მოწყობილობები, რომლებიც არ არის გამიზნული საჯაროდ ხელმისაწვდომი. მაგალითად, შესაძლებელია სამრეწველო კონტროლის სისტემების პოვნა შოდანის ძიებით. ამან გამოიწვია

კიბერუსაფრთხოების ექსპერტების შეშფოთება, რადგან ამ ტიპის სისტემები ხშირად არ არის ისეთი უსაფრთხო, როგორც ტრადიციული კომპიუტერები და ემუქრებათ გატეხვის რისკი.

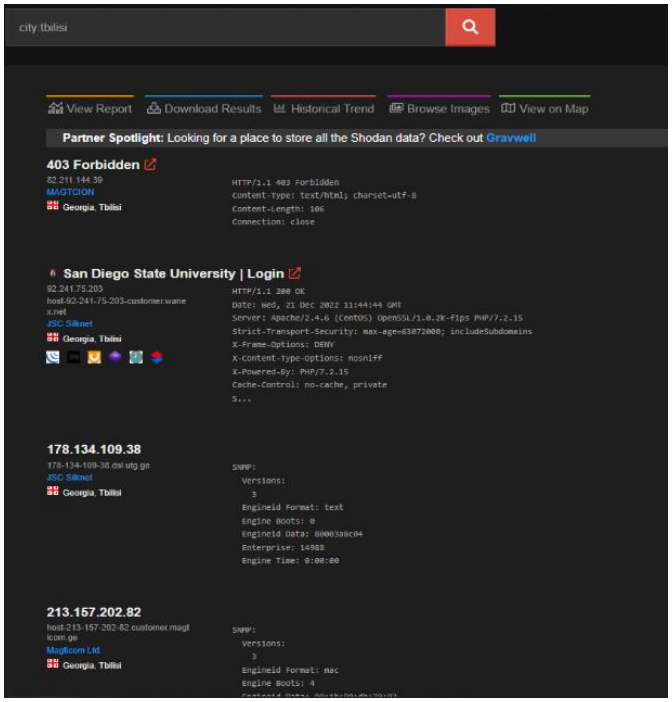
შოდანი არ გამოიყენება მხოლოდ ჰაკერების მიერ. მას ასევე იყენებენ უსაფრთხოების მკვლევარები, ქსელის ადმინისტრატორები და სხვები ინტერნეტთან დაკავშირებულ მოწყობილობებსა და სისტემებში დაუცველობის დასადგენად. კონკრეტული ტიპის მოწყობილობების ან სერვერების ძიებით, შესაძლებელია იდენტიფიცირება, ვისაც შეიძლება ჰქონდეს სუსტი პაროლები, მოძველებული პროგრამული უზრუნველყოფა ან სხვა დაუცველობა, რომელთა გამოყენება შესაძლებელია.

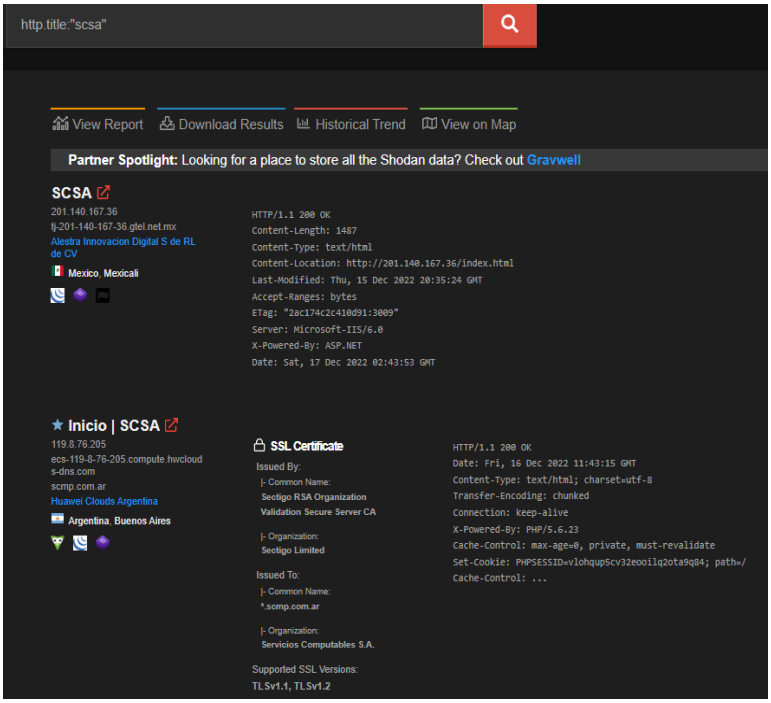
მიუხედავად იმისა, რომ Shodan არის სასარგებლო ინსტრუმენტი უსაფრთხოების პოტენციური რისკების იდენტიფიცირებისთვის, მნიშვნელოვანია აღინიშნოს, რომ ის არ არის ჰაკერული ინსტრუმენტი. ის უბრალოდ საშუალებას აძლევს მომხმარებლებს მოძებნონ და იპოვონ ინტერნეტთან დაკავშირებული მოწყობილობები და სერვერები. მომხმარებლის გადასაწყვეტია, როგორ გამოიყენოს ეს ინფორმაცია და შეატყობინოს თუ არა აღმოჩენილ დაუცველობას.

საბოლოოდ, Shodan არის საძიებო სისტემა ინტერნეტთან დაკავშირებული მოწყობილობებისთვის, რომელიც შეიძლება გამოყენებულ იქნას სხვადასხვა მიზნებისთვის, მათ შორის უსაფრთხოების პოტენციური დაუცველობის იდენტიფიცირებისთვის. მიუხედავად იმისა, რომ ეს არის სასარგებლო ინსტრუმენტი, მნიშვნელოვანია მისი გამოყენება პასუხისმგებლობით და დაიცვას ყველა მოქმედი კანონი და რეგულაცია მისი გამოყენებისას.

Shodan ის მოხმარება:

თუ ჩვენ საძიებო ველში ჩავწერთ Country:ge Shodan ავტომატურად ამოგვიგდებს იმ Host -ებს რომლებიც საქართველოში არის, ხოლო თუ ჩავწერთ City:Tbilisi ამ შემთხვევაში ამოაგდებს ყველა დასკანერებულ Host რომელიც არის თბილისში (სურ. 1 ა,ბ):





სურათი 1 ა

თბილისში მოძებნილი მოწყობილობები არის

სურათი 1 ბ

ყველა ვებსაიტი რომლის სათაური SCSA

უკვე იცით როგორ მუშაობს Google Dork ის intitle Command -ი. შოდანზეც არსებობს მსგავსი Command სახელად http.title. თუ ჩვენ საძიებო ველში ჩავწერთ http.title:“scsa” -ს ამოაგდებს ყველა ვებსაიტს რისი სათაურიც არის SCSA. ასევე არის Port ქომანდი რითითაც შეგიძლიათ მიუთითოთ სასურველი პორტი. ამ შემთხვევაში შოდან გაჩვენებს ყველა ჰოსტს რომელსაც აქვს გახსნილი თქვენი მითითებული პორტი.

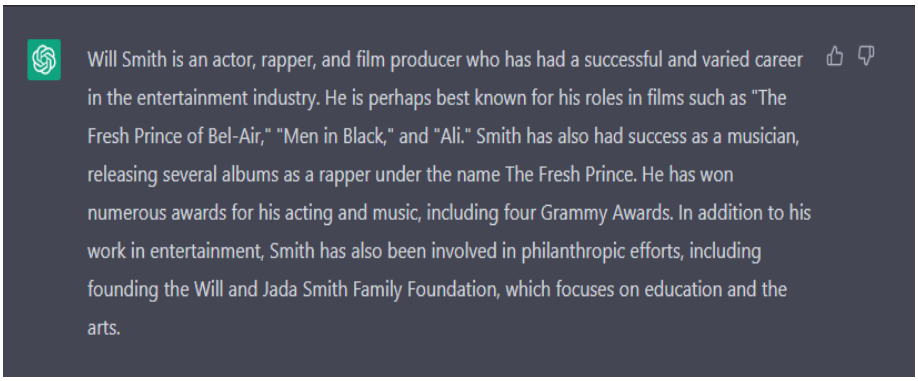
OpenAI

OpenAI ატარებს კვლევებს AI-თან დაკავშირებულ სხვადასხვა სფეროში, მათ შორის მანქანური სწავლა, კომპიუტერული ხედვა, ბუნებრივი ენის დამუშავება და რობოტიკა. ორგანიზაცია ცნობილია ღრმა სწავლებაზე მუშაობით, მანქანური სწავლების ტიპი, რომელიც გულისხმობს ხელოვნური ნერვული ქსელების მომზადებას მონაცემთა დიდ ნაკრებებზე.

OpenAI-ის ერთ-ერთი მნიშვნელოვანი მიღწევაა GPT-3-ის, ენის დამუშავების AI სისტემის განვითარება, რომელსაც შეუძლია ადამიანის მსგავსი ტექსტის გენერირება. სხვა მნიშვნელოვანი პროექტებია DALL-E, ხელოვნური ინტელექტის სისტემა, რომელსაც შეუძლია სურათების გენერირება ტექსტის აღწერილობიდან და AI სისტემების განვითარება თამაშებისთვის, როგორიცაა ჭადრაკი და Go.

OpenAI არის მომგებიანი ორგანიზაცია, მაგრამ მას აქვს ვალდებულება საჯაროობისა და გამჭვირვალობისადმი თავის კვლევაში და AI ტექნოლოგიების პასუხისმგებლობით განვითარებაზე. მან ასევე დაამყარა პარტნიორობა უამრავ სხვა ორგანიზაციასთან, მათ შორის Microsoft-თან და ელონ მასკის ფონდთან, თავისი კვლევის მიზნების გასაგრძელებლად.

მის ვებ-საიტზე გადასვლილას, მომხმარებელს შეუძლია ნებისმიერი მოთხოვნა გააგზავნოს, რის შემდეგ ხელოვნური ინტელექტი მას ღია წყაროებიდან აკრეფილ და გაანალიზებულ ინფორმაციას გადმოუგდებს. ეს შესაძლებლობა აძლევს ადამიანს წამებში მიიღოს ღირებული ინფორმაცია სხვა ადამიანებზე. მაგალითი შეგვიძლია განვიხილოთ რომელიმე ცნობილ ადამიანზე, მაგალითად Will Smith-ზე და მოთხოვნის გაგზავნის შემდეგ AI ამოგვიგდებს მოძიებულ ინფორმაციას ამ პიროვნებაზე. (სურ. 1)



სურათი 1 Will Smith-ზე მოძიებული ინფორმაცია

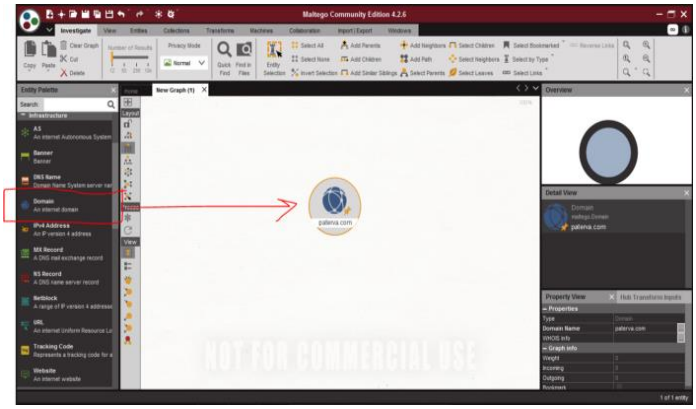
Maltego

Maltego არის პროგრამული უზრუნველყოფის ინსტრუმენტი, რომელიც გამოიყენება მონაცემთა მოპოვებისა და ინფორმაციის შეგროვებისთვის. იგი გამოიყენება სხვადასხვა წყაროდან მიღებული მონაცემების ანალიზისა და ვიზუალიზაციისთვის, რათა დადგინდეს ურთიერთობები და კავშირები სხვადასხვა ერთეულებს შორის. Maltego ხშირად გამოიყენება უსაფრთხოების პროფესიონალების, გამომძიებლებისა და ანალიტიკოსების მიერ, რათა მიიღონ ინფორმაცია ქსელების, ორგანიზაციებისა და ინდივიდების შესახებ.

პროგრამული უზრუნველყოფა მომხმარებლებს საშუალებას აძლევს შეასრულონ ისეთი ამოცანები, როგორიცაა ადამიანებს, ორგანიზაციებს, ვებ-საიტებსა და სხვა ერთეულებს შორის ურთიერთობების იდენტიფიცირება, აგრეთვე ფარული კავშირებისა და შაბლონების აღმოჩენა. მას ასევე აქვს ვიზუალიზაციის მრავალი ვარიანტი, მათ შორის გრაფიკები და რუკები, რაც მომხმარებლებს დაეხმარება მონაცემთა გაგებაში და ინტერპრეტაციაში.

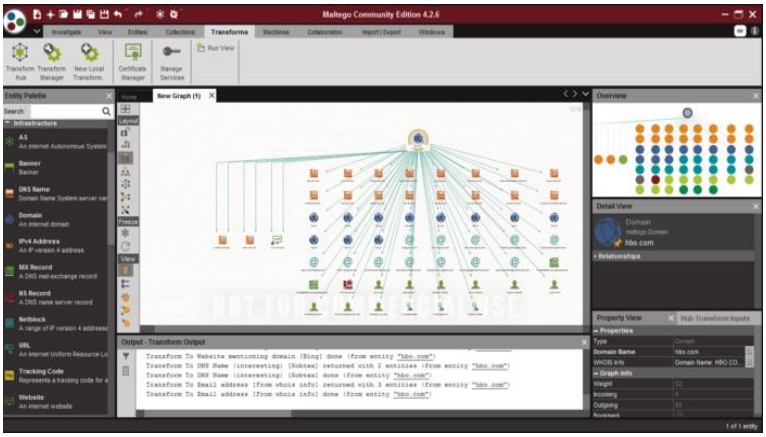
Maltego შეიძლება გამოყენებულ იქნას სხვადასხვა მიზნებისთვის, მათ შორის კიბერ უსაფრთხოებითვის ან თაღლითობის გამოვლენისთვის. ის ხელმისაწვდომია როგორც უფასო, ასევე ფასიანი ვერსიით, სადაც ფასიანი ვერსია გთავაზობთ დამატებით ფუნქციებსა და შესაძლებლობებს.

ვთქვათ ჩვენი მიზანია hbo.com ვებ-საიტზე მაქსიმალური ინფორმაციის გაგება. ამისთვის ჩვენ შევქმნით ახალ გრაფას და მანდ ჩავსვათ hto.com ვებ-საიტის ლინკს. (სურ. 1)



სურათი 1 hto.com ვებსაიტი Maltego -ში

მარჯვენა ღილაკის დაჭერისას გამოჩნდება მენიუ, სადაც All Transforms-ზე დაჭერისას Maltego ყველა შესაძლო ინფორმაციას გამოავლენს, მაგალითად ადამიანის სახელებს, DNS სერვერებს, ელ-ფოსტებს, დაკავშირებული საიტები და ა.შ. (სურ. 2)



სურათი 2 ყველა შესაძლო ნაპოვნი ინფორმაცია

საბოლოოდ, ამ უზარმაზარი ინფორმაციის ხელით მოძიებაში საკმაოდ დიდი დრო დასჭირდებოდა, სანამ Maltego-მ ეს წუთებში გააკეთა და გრაფიკულად გამოსახაც კიდეც.

Recommendation Systems

ხელოვნური ინტელექტი (AI) და მანქანათმცოდნეობა (ML) ჩვეულებრივი ხდება. ისინი გამოიყენება ამოცანების შესასრულებლად და კრიტიკული გადაწყვეტილებების მიღებაში დასახმარებლად ინდუსტრიების ფართო სპექტრში, მათ შორის ენერგეტიკის, სამედიცინო და ფინანსური სექტორებში.

სხვა გამოყენებებთან ერთად, AI და ML სიმძლავრის რეკომენდატორი სისტემები. ეს სისტემები რეკომენდაციას უწევს პროდუქტებს, კონტენტს ან მომსახურებას, რომელიც შეიძლება მოეწონოს მომხმარებლებს, იქნება ეს ისინი ონლაინ ყიდულობენ, ირჩევენ ფილმს ან სიმღერას სტრიმინგისთვის, თუ ათვალიერებენ ახალი ამბების სტატიებს.

კომპანიები იყენებენ სარეკომენდაციო სისტემებს, რადგან ისინი ეხმარებიან მყიდველის გამოცდილების პერსონალიზაციას, შემოსავლის გაზრდას და კლიენტების შეკავებისა და ბრენდის ლოიალობის გაუმჯობესებას.

სარეკომენდაციო სისტემების ტიპები

სარეკომენდაციო სისტემის სამი ძირითადი ტიპი არსებობს:

- Content-based filtering - იყენებს მსგავსებებს პროდუქტებში, სერვისებში ან კონტენტის ფუნქციებში, ასევე მომხმარებლის შესახებ დაგროვილ ინფორმაციას რეკომენდაციების გასაკეთებლად.

- Collaborative filtering - ეყრდნობა მსგავსი მომხმარებლების პრეფერენციებს კონკრეტული მომხმარებლისთვის რეკომენდაციების შეთავაზების მიზნით.
- Hybrid recommender systems - აერთიანებს ორ ან მეტ სარეკომენდაციო სტრატეგიას და იყენებს თითოეულის უპირატესობებს რეკომენდაციების გასაკეთებლად სხვადასხვა გზით.

რა არის content-based filtering და როგორ მუშაობს იგი?

კონტენტზე დაფუძნებული ფილტრაცია არის სარეკომენდაციო სისტემის ტიპი, რომელიც ცდილობს გამოიცნოს რა შეიძლება მოეწონოს მომხმარებელს ამ მომხმარებლის აქტივობიდან გამომდინარე.

კონტენტზე დაფუძნებული რეკომენდატორი მუშაობს იმ მონაცემებთან, რომლებსაც მომხმარებელი აწვდის, ცალსახად (რეიტინგი) ან იმპლიციურად (ბმულზე დაწკაპუნებით). ამ მონაცემებზე დაყრდნობით იქმნება მომხმარებლის პროფილი, რომელიც შემდეგ გამოიყენება მომხმარებლისთვის შეთავაზებების გასაკეთებლად. რაც უფრო მეტ ინფორმაციას აწვდის მომხმარებელი ან იღებს ზომებს ამ რეკომენდაციებზე, ძრავა უფრო და უფრო ზუსტი ხდება.

სარეკომენდაციო სისტემამ უნდა გადაწყვიტოს ინფორმაციის მიწოდების ორ მეთოდს შორის, როდესაც მომხმარებელს რეკომენდაციებს აძლევს:

- Exploitation - სისტემა ირჩევს მსგავს დოკუმენტებს, რომლებზეც მომხმარებელმა უკვე გამოთქვა უპირატესობა.
- Exploration - სისტემა ირჩევს დოკუმენტებს, სადაც მომხმარებლის პროფილი არ იძლევა მტკიცებულებებს მომხმარებლის რეაქციის პროგნოზირებისთვის.

ახლა გადავიდეთ content-based filtring -ის პროგრამირების Python ენაზე დაწერილ კოდზე. ამისთვის ასევე დაგვჭირდება ეს სამი ბიბლიოთეკა: Jupyter notebook; Python==3.5.7; scikit-learn.

1) მონაცემების ჩატვირთვა

TF*IDF ალგორითმი გამოიყენება ნებისმიერი დოკუმენტის საკვანძო სიტყვის ასაწონად და ამ საკვანძო სიტყვისთვის მნიშვნელობის მინიჭებისთვის დოკუმენტში მისი გამოჩენის რაოდენობის მიხედვით.

თითოეულ სიტყვას ან ტერმინს აქვს შესაბამისი TF და IDF ქულა. ტერმინის TF და IDF ქულების ნამრავლს ეწოდება ამ ტერმინის TF*IDF წონა. TF (Term Frequency) არის დოკუმენტში სიტყვის გამოჩენის რაოდენობა (სურ. 1).

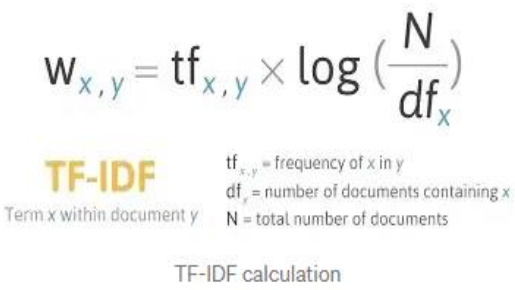
```
TF(t) = (Number of times term t appears in a document) / (Total
number of terms in the document).
```

სურათი 1 TF -ის აღწერა

სიტყვის IDF (Inverse Document Frequency) არის საზომი იმისა, თუ რამდენად მნიშვნელოვანია ეს ტერმინი მთელ კორპუსში (სურ. 2 ა,ბ).

```
IDF(t) = log_e(Total number of documents / Number of documents with
term t in it).
```

სურათი 2 ა IDF -ს აღწერა



TF-IDF calculation

სურათი 2 ბ TF*IDF ალგორითმი

Python-ში scikit-learn გაწვდით წინასწარ აშენებულ TF-IDF ვექტორიზატორს, რომელიც ითვლის TF-IDF ქულას თითოეული დოკუმენტის აღწერილობისთვის, სიტყვა-სიტყვით (სურ. 3).

```
tf = TfidfVectorizer(analyzer='word', ngram_range=(1, 3), min_df=0,
stop_words='english')
tfidf_matrix = tf.fit_transform(ds['description'])
```

სურათი 3 სიტყვების გამეორეს კოდი

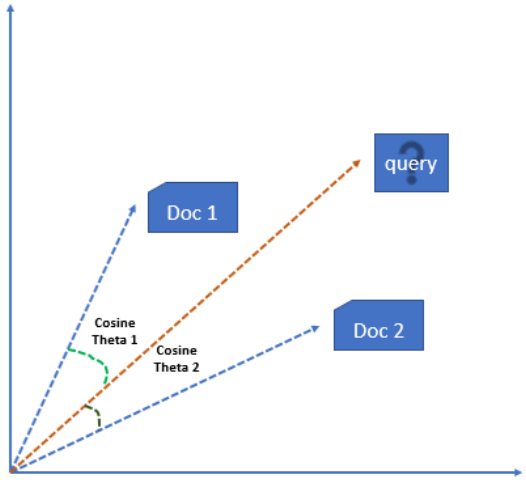
აქ, "tfidf_matrix" არის მატრიცა, რომელიც შეიცავს თითოეულ სიტყვას და მის TF-IDF ქულას თითოეულ დოკუმენტთან, ან ამ შემთხვევაში ერთეულთან მიმართებაში. ასევე, გაჩერებული სიტყვები უბრალოდ სიტყვებია, რომლებიც არ მატებენ მნიშვნელოვან მნიშვნელობას ჩვენს სისტემას, როგორიცაა "an", "is", "the" და, შესაბამისად, სისტემა იგნორირებულია.

2) ვექტორულ-სივრცითი მოდელი

ამ მოდელში თითოეული ელემენტი ინახება როგორც მისი ატრიბუტების ვექტორი (რომლებიც ასევე ვექტორებია) n-განზომილებიან სივრცეში და ვექტორებს შორის კუთხეები გამოითვლება ვექტორებს შორის მსგავსების დასადგენად.

მომხმარებლის მოწონებების/არმოწონების/ზომების გამოთვლის მეთოდი გამოითვლება მომხმარებლის პროფილის ვექტორსა (Ui) და დოკუმენტის ვექტორს შორის კუთხის კოსინუსის აღებით; ან ჩვენს შემთხვევაში, კუთხე დოკუმენტის ორ ვექტორს შორის.

კოსინუსის გამოყენების საბოლოო მიზეზი არის ის, რომ კოსინუსის მნიშვნელობა გაიზრდება, როდესაც ვექტორებს შორის კუთხე მცირდება, რაც უფრო მეტ მსგავსებას ნიშნავს (სურ. 4).



სურათი 4 კოსინუსის კუთხე

3) კოსინუსების მსგავსების გამოთვლა

```
cosine_similarities = linear_kernel(tfidf_matrix, tfidf_matrix)
results = {}
for idx, row in ds.iterrows():
   similar_indices = cosine_similarities[idx].argsort()[:-100:-1]
   similar_items = [(cosine_similarities[idx][i], ds['id'][i]) for i
in similar_indices]
   results[row['id']] = similar_items[1:]
```

სურათი 5 კოსინუსის მსგავსების გამოთვლის python კოდი

აქ ჩვენ გამოვთვალეთ თითოეული ელემენტის კოსინუსური მსგავსება მონაცემთა ნაკრების ყველა სხვა ელემენტთან, შემდეგ დავალაგეთ ისინი მათი მსგავსების მიხედვით "i" პუნქტთან და შევინახეთ მნიშვნელობები "results" (სურ. 5).

4) რეკომენდაციის გაცემა

ამ ნაწილში, ჩვენ საბოლოოდ ვნახავთ რეკომენდატორთა სისტემას მოქმედებაში.

```
def item(id):
  return ds.loc[ds['id'] == id]['description'].tolist()[0].split(' -
')[0]

# Just reads the results out of the dictionary.def

recommend(item_id, num):
    print("Recommending " + str(num) + " products similar to " +
item(item_id) + "...")
    print("-------")    recs = results[item_id][:num]
    for rec in recs:
       print("Recommended: " + item(rec[1]) + " (score:" +
str(rec[0]) + ")")
```

სურათი 6რეკომენდაციის გაცემის python კოდი

აქ ჩვენ უბრალოდ შევიყვანთ „item_id“-ს და რეკომენდაციების რაოდენობას, რომელიც ჩვენ გვინდა. ამიერიდან ფუნქცია აგროვებს ამ „item_id“-ის შესაბამის „შედეგებს[]“ და ვიღებთ რეკომენდაციებს ეკრანზე (სურ. 6).

5) რეზულტატი

აქ არის მიმოხილვა, თუ რა ხდება ზემოთ მოცემულ ფუნქციის გამოძახებისას (სურ. 7 ა,ბ).

```
recommend(item_id=11, num=5)
```

სურათი 7 ა საბოლოო ფუნქცია

```
Recommending 10 products similar to Relax fit organic ctn jeans-shor...
-------
Recommended: Relax fit organic ctn jeans-reg (score:0.8908101955877065)
Recommended: Relax fit organic ctn jeans-long (score:0.8866113828050025)
Recommended: Reg fit organic ctn jeans-short (score:0.507668259865595)
Recommended: Reg fit organic ctn jeans-long (score:0.48801052800273903)
Recommended: Reg fit organic ctn jeans-reg (score:0.48488884889129785)
Recommended: Custodian pants (score:0.1925730494862419)
Recommended: Shop pants (score:0.18030173682681883)
Recommended: Shop pants (score:0.1733375276479681)
Recommended: Custodian pants (score:0.1710311820622527)
Recommended: Inga shorts (score:0.17023045978100093)
```

სურათი 7 ბ ორგანული ბამბის ჯინს-შორტების მსგავსი რეკომენდაციები

კონტენტზე დაფუძნებულ ფილტრაციას აქვს როგორც დადებითი ისე უარყოფითი მხარეების. დადებითად შეიძლება ჩავთვალოთ, ის რომ ეს ფილტრაცია მომხმარებლის დამოუკიდებლად არსებობს. კონტენტზე დაფუძნებულ მეთოდს მხოლოდ ერთეულებისა და ერთი მომხმარებლის პროფილის ანალიზი სჭირდება რეკომენდაციისთვის, რაც პროცესს ნაკლებად რთულს ხდის და აქედან გამომდინარე უფრო ზუსტ და საიმედო შედეგებს იძლევა. ამავდროულად კონტენტზე დაფუძნებულ ტექნოლოგიას აქვს ნაკლოვანებებიც. ერთ-ერთი ითვლება შეზღუდული შინაარსის ანალიზი, ანუ თუ კონტენტი არ შეიცავს საკმარის ინფორმაციას ნივთზე, რეკომენდაცია დიდი ალბათობით არა ზუსტი იქნება. ასევე აღსანიშნავია, რომ კონტენტზე დაფუძნებული ფილტრაცია უზრუნველყოფს სიახლის შეზღუდულ ხარისხს, რადგან ის უნდა შეესაბამებოდეს მომხმარებლის პროფილის მახასიათებლებს ხელმისაწვდომ ელემენტებთან.

შედეგი: საბოლოოდ, კონტენტზე დაფუძნებული ფილტრაცია საკმაოდ გავრცელებული რეკომედაციის ტექნოლოგიაა, რომელიც მომხმარებელს აკონტროლებს და მისი შეყვანილი მონაცემებიდან გამომდინარე, მსგავს ინფორმაციას იძლევა. მაგრამ, როგორც ზემოთ აღნიშნულია, კონტენტზე დაფუძნებული ფილტრაცია არ არის პრაქტიკული, უფრო სწორად, არც ისე საიმედო, როდესაც ელემენტების რაოდენობა იზრდება მკაფიო და დიფერენცირებული აღწერების საჭიროებასთან ერთად. ამის გადასაწყვეტად, შესაძლებელია განახორციელდეს ერთობლივი ფილტრაციის ტექნიკა, რომელიც უკეთესი, ზუსტი და მასშტაბური აღმოჩნდება.

დასკვნა:მიუხედავად ტექნოლოგიური მიღწევებისა, OSINT-ის მრავალი პრაქტიკოსისთვის, crowdsourcing რჩება ყველაზე მძლავრ ინსტრუმენტად. ვინაიდან ორგანიზაციები, კერძო კომპანიები და დაინტერესებული პირები თავიანთ გამოკვლევებს საჯაროდ აწვდიან, ერთობლივი ეფექტი აძლიერებს OSINT-ის შემდგომ გამოკვლევებს, რომლებიც გააგრძელებენ ერთობლივ მუშაობას სწრაფად განვითარებად ტექნოლოგიასთან. AI ტექნოლოგია კვლავაც წარმოუდგენლად სასარგებლოა OSINT-ში მონაცემთა შეგროვებისთვის, დეზინფორმაციის გაფილტვრისთვის, შაბლონის იდენტიფიკაციისთვის და მთლიანი პროცესის გასამარტივებლად. მართლაც, ზოგიერთი ვარაუდობს, რომ ხელოვნური ინტელექტის ტექნოლოგია აუწყებს ახალ გარიჟრაჟს OSINT პრაქტიკოსებისთვის, სადაც სწორად შერჩეული ალგორითმი საბოლოო მომხმარებელს მიაწვდის ზუსტ ინფორმაციას, რომელსაც ისინი ეძებენ. მიუხედავად იმისა, რომ ძლიერი AI, რომელსაც შეუძლია შეცვალოს ადამიანის ანალიზი, რჩება ფანტაზიად, ხელოვნური ინტელექტის ტექნოლოგიაში ექსპონენციალურ წინსვლა ნიშნავს, რომ ასეთი ალგორითმები, რომლებსაც შეუძლიათ სწრაფად გაავრცელონ და ამოიცნონ დაზვერვის ძირითადი ნაწილები, სხვა არაფერია, თუ არა ოცნებები. აღსანიშნავია ასევე ზემოთ აღნიშნული ხერხები, საიდანაც გამომდინარე ნათლად ჩანს ადამიანის შესაძლებლობები თუ ის სწორად და ეფექტურად გამოიყენებს კონკრეტულ ინფორმაციულ წყაროებს.

ბიბლიოგრაფია

1. OSINT Framework ოფიციალური ვებ-საიტი https://osintframework.com
2. Metagoofil ხელსაწყოს Open Source კოდი https://www.kali.org/tools/metagoofil/
3. ოფიციალური Shodan -ის ვებ-საიტი https://www.shodan.io/
4. დამატებითი ინფორმაცია Shodan -ზე და საძიებლო ხელსაწყოს გამოყენებაზე: https://github.com/jakejarvis/awesome-shodan-queries; https://osintcurio.us/2021/05/13/searching-with-shodan
5. ხელოვნური ინტილექტის გამოყენება OSINT -ში https://chat.openai.com/chat
6. მეტი ინფორმაცია OpenAI ორგანიზაციაზე https://openai.com/about/
7. Matlego -ს დოკუმენტაციები https://docs.maltego.com/support/home
8. კელერი, ჯ. (2019) ხელოვნური ინტელექტის მანქანათმცოდნეობის ინდუსტრიის დღე. სამხედრო და კოსმოსური ელექტრონიკა. https://www.militaryaerospace.com/computers/article/14069043/artificial-intelligence-machine-learning-industry-day.
9. უილსონი, ჯ.რ. (2020) მკვლევარებმა მიზნად ისახეს ხელოვნური ინტელექტის შესახებ ბრძოლის ველის სენსორების კოორდინაციისთვის. Military & Aerospace Electronics https://www.militaryaerospace.com/communications/article/16710965/researchers-set-eir-sights-on-artificial-intelligence-to-coordinate-battlefield-sensors.
10. Van Puyvelde, D, Coulthart, S.& Hossain. M. (2017) Beyond the Buzzword: Big Data და National Security Decision-Making.

11. Upwork Team research on content-based filtring (2021) https://www.upwork.com/resources/what-is-content-based-filtering
12. Nikita Sharma - Recommender Systems with Python — Part I: Content-Based Filtering. (2019)

Scientific and Practical Cyber Security Journal (SPCSJ) 6(4): 57-63 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

USAGE OF COLLATZ CONJECTURE IN CRYPTOGRAPHY

Andria Kelekhsaevi, Cervantes Gymnasium-gess
Gega Shavdatuashvili, Cervantes Gymnasium-gess
Giorgi Meliqidze, 176 pubic school
Giorgi Mchedlidze, school Opiza

ABSTRACT: This article distinguishes Usage of Collatz Conjecture in cryptography. In particular, how we can hash information using the "3n+1" algorithm. We review a new method of irreversible hash and its usage in the modern world using,"3x+1" problem.

KEYWORDS: *Collatz Conjecture, Cryptography, Collatz problem, irreversible hash, Encryption*

Introduction:

Hashing is the process of transforming any given key or a string of characters into another value. This is usually represented by a shorter, fixed-length value or key that represents and makes it easier to find or employ the original string.

The most popular use for hashing is the implementation of hash tables. A hash table stores key and value pairs in a list that is accessible through its index. Because key and value pairs are unlimited, the hash function will map the keys to the table size. A hash value then becomes the index for a specific element. A hash function generates new values according to a mathematical hashing algorithm, known as a hash value or simply a hash. To prevent the conversion of hash back into the original key, a good hash always uses a one-way hashing algorithm.

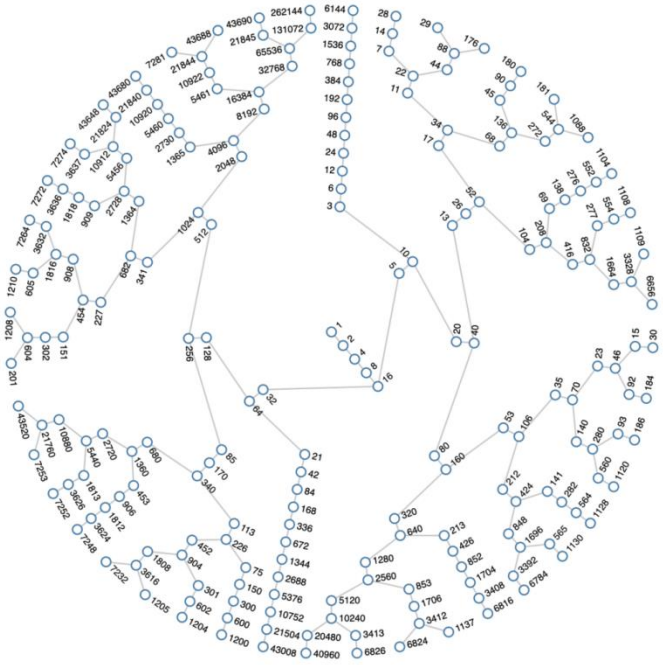
Hashing is relevant to -- but not limited to -- data indexing and retrieval, digital signatures, cybersecurity and cryptography.

Collatz Conjecture:

The Collatz conjecture is one of the most famous unsolved problems in mathematics. The conjecture asks whether repeating two simple arithmetic operations will eventually transform every positive integer into 1**.**

The Collatz conjecture states that the orbit of every number under f eventually reaches 1. And while no one has proved the conjecture, it has been verified for every number less than 268. So if you're looking for a counterexample, you can start at around 300 quintillion [1].

It's easy to verify that the Collatz conjecture is true for any particular number: Just compute the orbit until you arrive at 1.



The importance of Collatz Conjecture in cryptography

By implementing the Collatz conjecture in cryptography we create an irreversible hash. Unlike encryption, Cryptographic Hash Functions are one-way. Once encrypted, you can never decrypt them even if you have the exact hashing algorithm that was used for the encryption [2].

Our Encryption works in that way:

1) We divide the alphabet into 13 pairs and mark each letter with ones and zeros.
The default corresponding number of each letter is zero and it becomes one only when the letter appears in the word [3].

(For example we turn word "hello" in given binary table)

Pairs of letters:		Binary Values:	
a	***b***	*0*	*0*
c	***d***	*0*	*0*
e	***f***	***1***	*0*
g	***h***	*0*	***1***
i	***j***	*0*	*0*
k	***l***	*0*	***1***
m	***n***	*0*	*0*
o	***p***	***1***	*0*
q	***r***	*0*	*0*
s	***t***	*0*	*0*
u	***v***	*0*	*0*
w	***x***	*0*	*0*
y	***z***	*0*	*0*

2) *After the first step of encryption, we add a special number to every sum of ones that correspond to a letter that was used in a given word. We do not add a special number to pairs where one doesn't appear. Special numbers are the same every time and are generated by adding the index of each letter in the same pair [4]. You can view it here:*

Final Value:		
3	*0*	*3*
7	*0*	*7*
11	***+1***	***12***
15	**+1**	**16**
19	*0*	*19*
23	**+1 +1**	***25***
27	*0*	*27*
31	**+1**	***32***
35	*0*	*35*
39	*0*	*39*
43	*0*	*43*
47	*0*	*47*
51	*0*	*51*

3) *After this step of encryption, we are left with the following result:* ***00121602503200000***

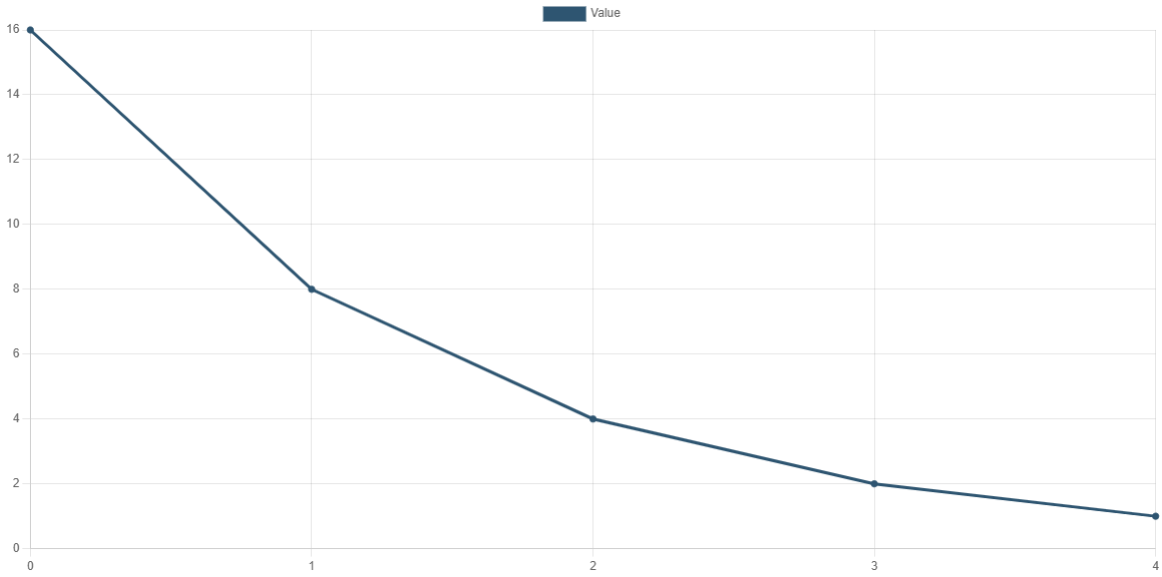
So on step 1 enc(k)("hello") = **00121602503200000**

After turning our string into a number hash we are going to use the 3x+1 problem to hash it even better and make it irreversible. The 3x+1 problem or so-called Collatz problem allows us to create a hash that will be impossible to decrypt because of its random pattern.

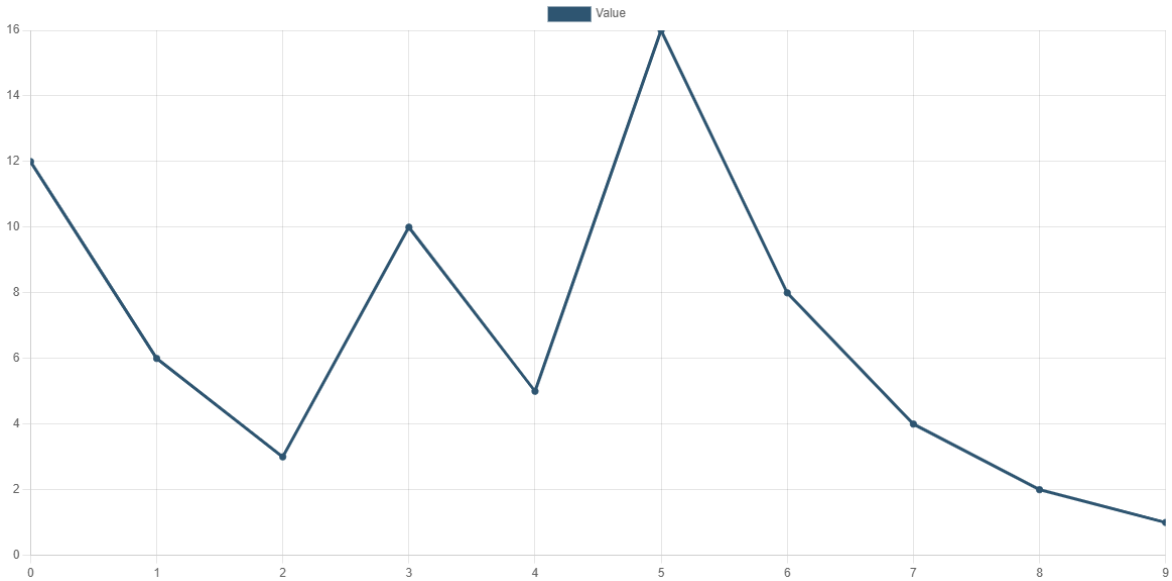
From the above hash, we ignore zeros and put every other number we got into a Collatz function. That means we will use the 3x+1 algorithm on 12,16,25 and 32. After finishing the algorithm we take the highest number in the Collatz tree and correspond it to the number that was used. If two different numbers

have the same highest number in the algorithm then we just choose 2-nd highest (except starting number) and so on [5,6].

Now, let's watch each step:

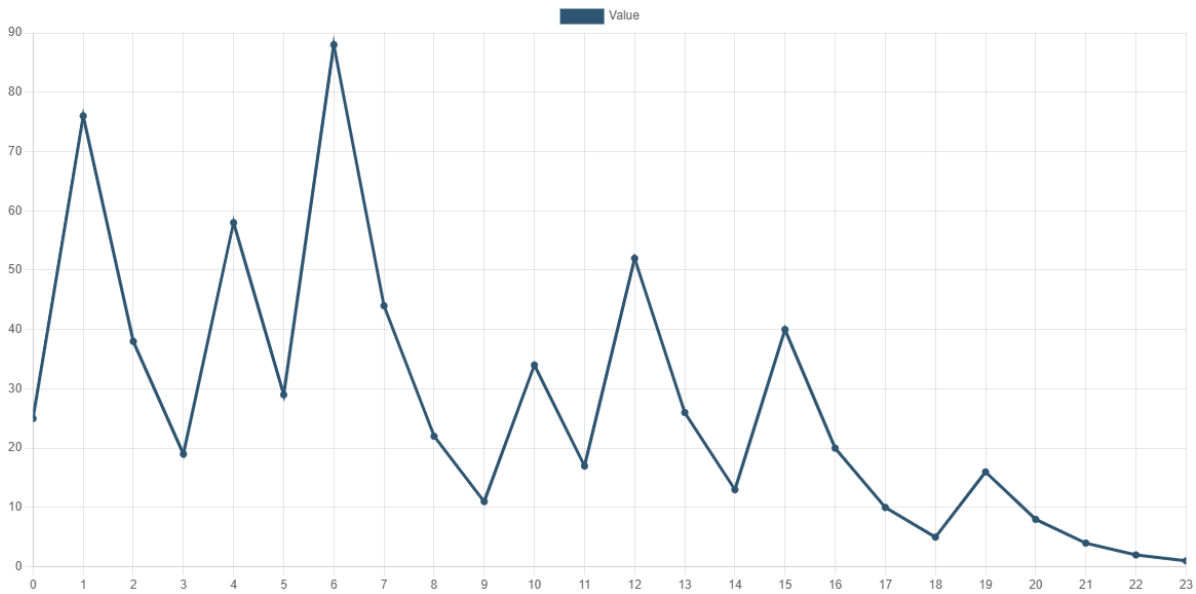


16 -->8 -->4 -->2 -->1
The highest number in this algorithm is 16 itself.
So enc(k)("h") = enc(k)(16) = 16

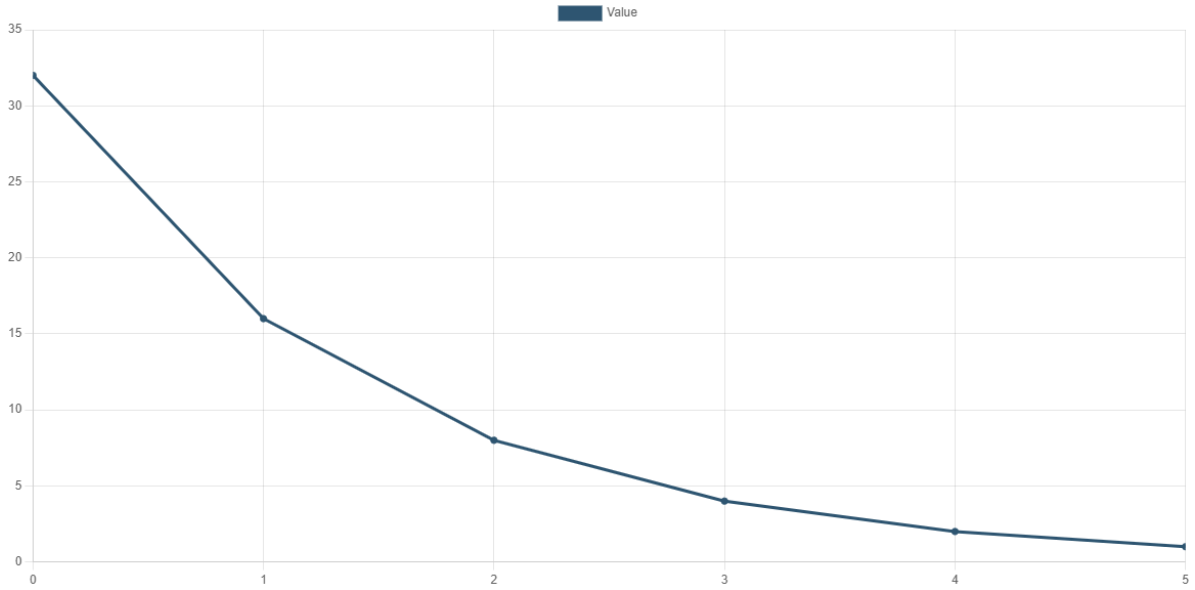


12 -->6 -->3 -->10 -->5 -->16 -->8 -->4 -->2 -->1

The highest number in this algorithm is also 16 so we choose the 2nd highest number (except starting number),which is 10.
soenc(k)("e") = enc(k)(12) = 10



25 -->76 -->38 -->19 -->58 -->29 -->88 -->44 -->22 -->11 -->34 -->17 -->52 -->26 -->13 -->40 -->20 -->10 -->5 -->16 -->8 -->4 -->2 -->1
The highest number in this algorithm is 88 so enc(k)("l") = enc(k)(25) = 88. Since "l" is used twice in hello, we put 88 twice in a final hash.



32 -->16 -->8 -->4 -->2 -->1
Highest number in this algorithm is 32 so enc(k)("o") = enc(k)(32) = 32.

After finishing our last step we are left with a hash that looks like this: **1610888832** so enc(k)("hello") = enc(k)(00121602503200000) = **1610888832**
After the whole hashing process word "hello" turned into a 1610888832. We would like to prove why it's impossible to decrypt a hash generated by our algorithm. Even if the attacker knows the method that was used they won't be able to decrypt the hash because of a simple reason. The Collatz problem. They won't be able to find the exact
number that was used as a starting point in our algorithm. Even If starting number might not change after the algorithm (like it happened with "h" when 16 was = 16) it is still impossible. Let's say the attacker knows that 88 was the highest number in our algorithm [7]. They put 88 in the Collatz conjecture algorithm and are left with the next problem:

88 -->44 -->22 -->11 -->34 -->17 -->52 -->26 -->13 -->40 -->20 -->10 -->5 -->16 -->8 -->4 -->2 -->1

The attacker might think that they will be able to find the number we used to hash but in reality, they have to do the
reverse path search [8]. To make it simple, we used the number 25 to get the number 88, and even if the attacker uses the back road:

reverse:
88 -->29 -->58 -->19 -->38 -->76 -->25
They will keep on going because of a simple reason. The attacker won't know where to stop. Our hashed number was
25 but the attacker will keep on searching for the starting number:
88 -->29 -->58 -->19 -->38 -->76 -->25 -->50 --> and so on.

Conclusion:

In the given article, we overviewed hashing and explained why and how Collatz Conjecture (3x+1 Problem) can be used in cryptography. We discussed an algorithm which sorts the English alphabet in 13 pairs and creates a binary table where each binary number corresponds to a specific letter. After the first stage of hashing our algorithm sums all the ones in the same row and adds a special number to each result. Final step is to put the result into a Collatz conjecture algorithm and pick the highest number in the path.

Over 80 years Collatz problem remains unsolved, so implementing it in cryptography gives a new, unique method of hashing which is irreversible and can’t be decrypted.

Acknowledgement: This work was supported by Shota Rustaveli National Science Foundation of Georgia [SPG-22-218]

BIBLIOGRAPHY

1. L. Colussi, “The convergence classes of Collatz function,” *Theoretical Computer Science*, vol. 412, no. 39, pp. 5409–5419, 2011.
2. P. C. Hew, “Working in binary protects the repetends of 1/3h: Comment on Colussi’s ’The convergence classes of Collatz function’,” *Theoretical Computer Science*, vol. 618, pp. 135–141, 2016.
3. R. K. Guy, “Don’t try to solve these problems,” *Computers and Mathematics with Applications*, vol. 90, no. 1, pp. 35–41, 1983.
4. G. T. Leavens and M. Vermeulen, “ search programs,” *Computers & Mathematics with Applications. An International Journal*, vol. 24, no. 11, pp. 79–99, 1992.
5. R. E. Crandall, “On the "3x+1" problem,” *Mathematics of Computation*, vol. 32, no. 144, pp. 1281–1292, 1978.
6. W. Ren, S. Li, R. Xiao, and W. Bi, “Collatz Conjecture for 2100000-1 is true - algorithms for verifying extremely large numbers,” in *Proceedings of the IEEE UIC 2018*, pp. 411–416, Guangzhou, China, October 2018.
7. I. Krasikov and J. C. Lagarias, “Bounds for the problem using difference inequalities,” *ActaArithmetica*, vol. 109, no. 3, pp. 237–258, 2003. View at: Publisher Site | Google Scholar | MathSciNet
8. Gagnidze, M. Iavich, G. Iashvili, Some Aspects of Post-Quantum Cryptosystems, Abstract book, EURO-ASIA FORUM IN POLITICS ECONOMICS AND BUSINESS – 2016, JULY 21-22, 2016, BELGRADE, SERBIA.