# SPCSJ

# SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL6 No2
JUNE 2022

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 1-5 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

# A TALE OF BETRAYAL: MALICIOUS BROWSER EXTENSIONS IN THE CONTEXT OF CYBER SECURITY AND PRIVACY

**Giulia Melotti Garibaldi, Cyber Security Consultant Master's degree in Law, University of Milano-Bicocca, Italy**

**ABSTRACT:** Browser extensions are popular additions to web browsers meant to enhance the online user experience by providing customizable options to meet the individual needs of users. In the wide variety of extensions available on the market, spanning from ad blockers to password managers, some of these software modules have proven to be a double-edged sword. As a matter of fact, in the past few years we have witnessed an alarming increase of malicious extensions available for download, targeting unaware victims relying on their apparent functional nature while hiding a world of illicit data thefts and sharing practices to the consumers' detriment. In order to examine whether the trade-off of privacy for functionality might still be an ongoing issue, this article follows two different approaches where theory and practice go hand in hand. The first one consists of a technical state-of-the-art analysis of different browser extensions available for download on the Chrome Web Store, while the second comprises a study of the questionable risks posed by those technologies from a privacy perspective. With regards to the latter, the author acknowledges the worldwide reach of browser extensions, while understanding the existence of a vast regulatory landscape around the globe. For the purpose of this paper, the analysis solely focuses on the European privacy framework, consisting of the General Data Protection Regulation (hereafter referred to as the GDPR) and the Directive on Privacy and Electronic Communications (the ePrivacy Directive). The conclusion drawn is that, despite all the efforts to counteract malicious browser extensions, some of them are still perpetrating harm and breaching privacy principles in a way which might not seem evident to users.

**KEYWORDS:** *cyber; security; browser extensions; protection; privacy.*

## INTRODUCTION

A browser extension is a small module added to web browsers with the purpose of giving additional functionality to users in relation to many subjects, including, but not limited to, third party websites, native applications, browser appearance and browser security. Browser extensions can ask for permissions to gain access to specific browser data and control of the browser, while having the ability to send and receive information from arbitrary external servers. In some cases, all browser data, including login credentials, financial and health information, can be accessed and collected by the browser extension, and network requests can be intercepted, modified, or blocked.

In the circumstance that an extension has been granted the ability to interact with requests, it is possible for a malicious browser extension to deceive users for the purpose of phishing by forcing a redirect to a malicious site or attempting to get the user to download and execute malware [25]. Their documented success in tricking users should come as no surprise [26]: browser extensions interface with a broad audience which seems to be anything but wary. According to a survey conducted in 2021, users are confident that developers for both default browsers and browser extensions reliably ensure the safety of user data [27]. Moreover, while a large portion of those trusty users does not read browser extensions' privacy policies [11], others do not take further steps to ensure their privacy and security once those extensions are installed [27].

## TECHNICAL METHODOLOGY

The overall purpose of testing was to determine if any browser extensions on the most popular internet browser per market share in Europe, i.e., Chrome [28], violated the European privacy legal framework. The sample examined consisted of twenty randomly selected browser extensions sourced from the Chrome Web Store in May 2022 [5], with all extensions tested on a device running Windows 10 (20H2) operating system using Google Chrome version 101.0.4951.54 . The browser extensions were analysed

manually and then automatically with the assistance of the online tool CRXcavator [7]. The extensions were tested with the aim of enumerating permissions, external communication with remote servers and defined privacy policy in the light of the GDPR [10] and the ePrivacy Directive [9].

## RESULTS

It was observed that twenty percent of the browser extensions tested were in breach of the GDPR, as they did not have a defined privacy policy and externally shared collected information from the user without fulfilling the information obligations [18,19]. Moreover, they also had excessive control of the user's browser via permissions to access the chrome.webRequest API [4], allowing for traffic interception, blocking and modification.

It was also noticed that another twenty percent of browser extensions tested did have a defined privacy policy, but was insufficient to meet the requirements under European law due to, for instance, inappropriate legal basis [15], illegitimate re-use of data for secondary processes despite their incompatibility with the pre-defined utilization and retaining data beyond the originally stated purpose and for an indefinite time [14]. Also for the scenario in question, the browser extensions were externally sharing collected information from the users without informing them, while having excessive control of the browser via permissions to access the chrome.webRequest API.

Lastly, the remaining sixty percent of tested browser extensions met the requirements of the EU privacy legal framework, including compliant privacy policies referring to, *inter alia*, the collected data, the purpose of collection and correct legal basis, third party data sharing, security measures, individual rights and cross-border transfers outside of the EU/EEA, with specific reference to safeguards for third countries not providing adequate protection [18,19].

Concluding, sixty percent of the inspected browser extensions fulfill the requirements, while forty percent do not only neglect the considered data protection framework, but also collect personal identifiable data to an extent which cannot be assessed due to lack of information from the developers' side. Whether data is collected following the least intrusive approach or not is left to the imagination.

## DISCUSSION

The sample in analysis is not large enough to draw any firm conclusions from the research conducted, as this paper primarily exists with the aim of raising awareness and stimulating more research and debate on the topic. There is a possibility that, although the European privacy legal framework requirements are not met by certain extensions tested, their security and privacy posture could be greater than what immediately visible to the author conducting this research. All things considered, the presence of forty percent potential non-compliant browser extensions appears to be a significant number that cannot be ignored: according to this study, critical data safety pitfalls take place on a common basis, with extensions spying on users and stealing their information for unknown purposes without them being aware thereof. This unlawful and unrestraint access to data also seems capable of deceiving Chrome's revision processes [2]. Hence, the small test carried out in this paper could not only serve as a wake-up call for cybersecurity practices, but also for privacy compliance. In an intangible borderless yet impacting world such as the Internet, technologies like browser extensions might attempt to escape the application of provisions and principles to which they are indeed subject to, and the interconnection between cybersecurity and privacy could turn out to be the winning cocktail to duly grant the security and rights of data subjects. Instead of considering them separately, it is of pivotal importance that privacy becomes the beating heart of technology when designing and engineering valuable and efficient products.

Starting off with the GDPR, the latter finds its application regardless of where organizations are established in the world, as long as the processing of data for the offering of goods or services or to monitor individuals is carried out by European-based organizations or relates to individuals in the European Union [12]. Therefore, not only can browser extensions not shield themselves by invoking the place where they are established, but they cannot rely on the nature of the processed data either, as the GDPR leaves the door open to a wide definition of personal identifiable information [13]. Unless disaggregated and anonymized [23], kinds such dynamic IP addresses and logged HTTP requests, for instance, are sufficient elements to directly or indirectly identify an individual, leading to the creation of an extensive user profile entailing patterns where even highly sensitive information could be exposed [6, 24]. The processing of personal data is not, however, forbidden per se under the GDPR, as long as it is happening in a lawful, fair and transparent manner [14]. The cost for respecting those principles is less hefty than what might be expected: for forty percent of the extensions analysed, having a compliant privacy policy to disclose data practices upfront could be the right starting point.

While notices' format might have different nuances, their content should invariably correspond to the requirements as outlined in the GDPR. Google Chrome also provides guidelines to help developers in drafting notices to be published on the extension download page [3]. Privacy policies should unequivocally document the collected data and the ways in which such personal information is intended to be used by the controller according to the business objectives, including its disclosure to third-parties [18,19]. The processing of data needs to be justified with a legal basis [15]: where the GDPR provides for six different bases to choose from, picking the right one for a lawful data processing appears to be a sweet spot for many developers, either because they fail to demonstrate that the processing of personal data is indispensable to achieve the stated purposes (i.e., such collection of data is not justified, and therefore violating the privacy-by-default principle) [21], or because they choose to rely on the wrong one. The Chrome guidelines set a strict requirement to request consent when browser extensions simultaneously meet two conditions: they collect personal or sensitive data, and the processing of such data is not "closely related" to its functionality [3]. At the very same time, some browser extensions rely on legitimate interest even when collecting those types of data, justifying the latter by assessing their own business interests against those relating to their consumers and declaring the former as overriding. The prevailing confusion on the topic is however no wonder when no clear rules and *consensus* regarding browser extensions have been defined. While the GDPR requests consent when the processing of behavioural data or preferences might reveal individual sensitive attributes [17] or when data is inferred as the result of probabilistic assumption and constructed profiles can be used for automated decision-making [20], the ePrivacy Directive would require it in the event of access to or storing information on the user's terminal [8]. As a matter of fact, by looking at the current regulatory framework and ongoing legal debate, it is undisputed that consent is the required legal basis for similar technologies to cookies such as device fingerprinting [1]. Even though no clear-cut reference to browser extensions has been made, in this author's opinion browser extensions with access to powerful APIs such as the chrome.webRequest API are able to fingerprint devices by several sources such as user behaviour and analysis of overall network traffic, where such actions are executed covertly without the acknowledgment of the end user. The technical method of device fingerprinting by browser extensions would likely not fall under the exemptions defined in Article 5(3) ePrivacy Directive, and therefore users' consent cannot be avoided.

All things considered, compliance is more than a mere piece of paper. Notices might collect consent by users actively agreeing to a clear and unmistakeable request on the product's front-end interface through consent dialogs, disclose international data transfer, refer to the use of accurate data and grant data access rights [16, 18, 19], and that might still not be enough. In fact, browser extensions should effectively observe what they promise to their consumers, implementing data sharing practices which do not only live up to legal standards, but also to users' expectations. Even when authorized, the collection of large datasets for analytics personalization and profiling by an extension to increase productivity, for instance, can hardly be justified in the users' eyes.

## CONCLUSION

While multiple browser extensions are still lagging behind in aligning their products to the European privacy requirements, these technologies could unleash much more potential than what they are currently doing by not being compliant. When adopting a consumer-centric view, transparently disclosing data practices to individuals, and refraining from intrusive tracking, profiling and data exfiltration, developers could demonstrate they are far away from merely serving their economic interests while caring for individual rights. Not only for the Data Protection Authorities, which have been particularly attentive and prone to fine for failure in fulfilment of information obligations and legal basis for the processing of data over the past years [22]: this change would also be an act of responsibility towards consumers, who would be capable of understanding to what extent browser extensions operate, while being empowered to make informed and autonomous choices regarding their own rights. If it is true that technology cannot be avoided, a conscious and ethical use of it could make the real difference.

**REFERENCES**


1. *Article 29 Working Party on Device Fingerprinting.* 2014. Article 29 Data Protection Working Party. "Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting". WP 224. https://www.dataprotection.ro/servlet/ViewDocument?id=1089

2. Chrome Developers. "Publish your extension". Accessed April 26, 2022. https://developer.chrome.com/docs/webstore/publish/

3. Chrome Developers. 2016, updated 2021. "Updated Privacy Policy & Secure Handling Requirements". Accessed April 28, 2022. https://developer.chrome.com/docs/webstore/user_data/

4. Chrome.webRequest API. Accessed April 27, 2022 https://developer.chrome.com/docs/extensions/reference/webRequest/

5. Chrome Web Store. Accessed May 3, 2022. https://chrome.google.com/webstore/category/extensions

6. *Court of Justice of the EU* (CJEU). 2016. Breyer, Case C-582/14, at para. 49 https://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=40417

7. *EU Directive on Privacy and Electronic Communications* (ePrivacy Directive). 2002. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

8. *EU General Data Protection Regulation* (GDPR). 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". OJ 2016 L 119/1. https://eur-lex.europa.eu/eli/reg/2016/679/oj

9. Eurostat. 2022. "How do EU citizens manage their personal data online?". Accessed May 3, 2022. https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20220127-1

10. Georgescu, Elena. 2021. "Have You Ever Installed a Malicious Chrome Extension?". Heimdal Security. Accessed April 25, 2022.

https://heimdalsecurity.com/blog/malicious-chrome-extension/

11. Jadali, Sam. 2019. "DataSpii: The catastrophic data leak via browser extensions". SecurityWithSam.com. Accessed April 27, 2022. https://securitywithsam.com/

12. Kariryaa, Ankit, Gianluca Savino, Carolin Stellmacher, Johannes Schöning. 2021. "Understanding Users' Knowledge about the Privacy and Security of Browser Extensions". *Proceedings of the Seventeenth Symposium on Usable Privacy and Security* (9-10 August 2021). Accessed April 26, 2022. https://www.researchgate.net/profile/Johannes-Schoening/publication/356892773_Understanding_Users%27_Knowledge_about_the_Privacy_and_Security_of_Browser_Extensions/links/61b1b4ec4d7ff64f05372925/Understanding-Users-Knowledge-about-the-Privacy-and-Security-of-Browser-Extensions.pdf?origin=publication_detail

13. Vailshery, Lionel Sujay. 2022. "Market share held by the leading internet browsers in Europe from 2009 to 2021". Statista. Accessed May 3, 2022. https://www.statista.com/statistics/269881/market-share-held-by-internet-browsers-in-europe/

Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 6-14 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

# CYBER SECURITY IN THE LOGISTICS INDUSTRY

**Ebrahim Aref Ahmed Al-Sobaihi, Mechanical Engineering Faculty, Institute of Technology, Hungarian University of Agriculture and Life Science, Gödöllő, Hungary**
**Prof. Dr. Dr. Patrick Siegfried, Department Logistik & Supply Chain Management, ISM International School of Management, Mörfelder Landstraße 55, 60598 Frankfurt/Main, Germany**

**ABSTRACT**: As of late, 'Digital protection' has arisen as a generally utilized term with expanded reception by experts and government officials the same. Be that as it may, similarly as with much in vogue language, there is by all accounts next to no comprehension of what the term involves. Albeit this is may not be an issue when the term is utilized in a casual setting, it might conceivably create impressive issues with regards to hierarchical technique, business destinations, or peaceful accords. In this work, we concentrate on the current writing to distinguish the principle definitions that accommodated the term 'Network safety by legitimate sources. We then, at that point, lead different lexical and semantic examination methods trying to all the more likely comprehend the extension and setting of these definitions, alongside their importance. At long last, given the investigation directed, we propose another further developed definition that we then, at that point, show to be a more agent definition utilizing similar lexical and semantic examination methods.
**KEYWORDS***: Cyber Security, Logistic*

## 1 Introduction

Cyber security is the act of shielding basic frameworks and touchy data from advanced assaults. Otherwise called data innovation (IT) security, online protection measures are intended to battle dangers against arranged frameworks and applications, regardless of whether those dangers begin from inside or outside of an association.

In 2020, the normal expense of an information break was USD 3.86 million universally, and USD 8.64 million in the United States. These expenses incorporate the costs of finding and reacting to the break, the expense of vacation and lost income, and the long haul reputational harm to a business and its image [1]. Cybercriminals focus on clients' by and by recognizable data (PII) - names, addresses, public ID numbers (e.g., Social Security numbers in the U.S., monetary codes in Italy), charge card data - and afterwards sell these records underground advanced commercial centres. Compromised PII regularly prompts a deficiency of client trust, administrative fines, and surprisingly lawful activity.

Security framework intricacy, made by unique advances and an absence of in-house skill, can enhance these expenses. In any case, associations with a far-reaching network safety system, administered by best practices and robotized utilizing progressed examination, man-made reasoning (AI), and AI, can battle digital dangers all the more successfully and decrease the lifecycle and effect of breaks when they happen.

Delivery and coordinated factors are, in numerous ways, the foundation of our lives and organizations. What business doesn't profit from new food or a convenient conveyance? Tragically, this industry is available to cyberattacks very much like any other person. Fortunately, bunches in the shipping and planned operations industry aren't feeble to address these difficulties.

## 2 Methodology

### *What is cyber security?*

In recent years, 'Cyber security' has arisen as a generally utilized term with expanded reception by specialists and lawmakers the same. Be that as it may, likewise with numerous popular languages, there is by all accounts almost no comprehension of what the term involves. Albeit this is may not be an issue when the term is utilized in a casual setting, it might lead to extensive issues with regards to hierarchical methodology, business targets, or peaceful accords. In this work, we concentrate on the current writing to distinguish the principle definitions that accommodated the term 'Network protection by legitimate sources. We then, at that point, direct different lexical and semantic examination strategies trying to all the more likely comprehend the degree and

setting of these definitions, alongside their pertinence. At last, in light of the examination directed, we propose another further developed definition that we then, at that point, show to be a more delegated definition utilizing similar lexical and semantic investigation techniques[2].

It is being ensured by web associated frameworks, including equipment, programming, and information, from digital assaults. In a figuring setting, security includes network protection and actual security both being utilized by endeavours to save against unapproved admittance to the server farm and other electronic frameworks. Security, which is intended to keep up with the secrecy, honesty, and accessibility of information, is a subset of network safety.

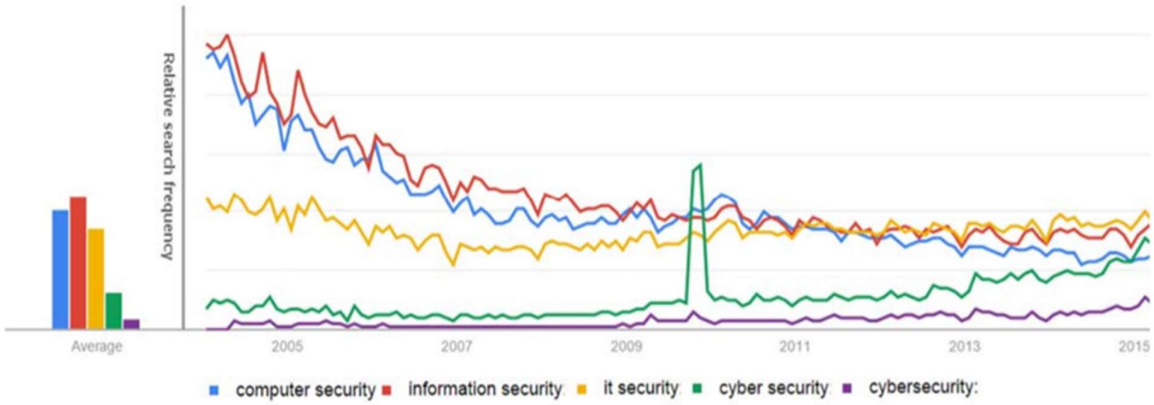



Figure 1 Google search trends for security 2004 – 2015

### *Why do we need cyber security?*

The scope of activities of network safety includes shielding data and frameworks from major digital dangers. These dangers take many structures. Thus, staying up with digital protection methodology and tasks can be a test, especially in government and undertaking networks where, in their most imaginative structure, digital dangers regularly focus on confidential, political and military resources of a country, or its people[3]. A portion of the normal dangers are:

- Cyber terrorism intimidation It is the inventive utilization of data innovation by fear monger gatherings to additional their political plan. It appeared as assaults on networks, PC frameworks, and media transmission foundations.
- Cyberwarfare It includes country states utilizing data innovation to go through something one more country's organizations to cause harm. In the U.S. what's more numerous others who live in the general public, digital fighting has been recognized as the fifth space of fighting. Cyberwarfare assaults are executed by programmers who are very much prepared in the utilization of advantage the nature of subtleties PC organizations and work under the good and backing of country states. Rather than shutting an objective's key organizations, a digital fighting assault might power to place into a circumstance into organizations to think twice about information, debase interchanges, hinder such infrastructural administrations as transportation and clinical benefits, or intrude on business.
- Digital undercover work It is the act of utilizing data innovation to acquire privileged intel without authorization from its proprietors or holders. It is the most normal used to acquire vital, monetary, military benefit, and is directed utilizing breaking methods and malware.

### *Who are Cyber Criminals?*

It includes such exercises as youngster printed sexual organs or movement; charge card extortion; cyberstalking; criticizing another web-based; acquiring unapproved admittance to PC frameworks; overlooking copyright, programming authorizing and brand name protected to ensure; superseding encryption to make unlawful duplicates; programming robbery and taking one more's character to perform criminal demonstrations. Cybercriminals are the individuals who direct such demonstrations. They can be arranged into three gatherings that mirror their inspiration.

**Type 1: Cybercriminals – hungry for recognition:**
- Hobby hackers.
- IT professionals (social engineering is one of the biggest threats)
- Politically motivated hackers.
- Terrorist organizations.

**Type 2: Cybercriminals – not interested in recognition**
- Psychological prevents
- Financially motivated hackers (corporate espionage)
- State-sponsored hacking (national espionage, sabotage)
- Organized criminals.

**Type 3: Cybercriminals – the insiders:**
- former employees seeking revenge.
- Competing companies use employees to gain economic advantage through damage and/or theft.

### *How To Maintain Effective Cyber Security?*

All things considered, associations and states have taken a receptive, "point item" way to deal with fighting digital dangers, creating something along with individual security advances – one on top of one more to save their organizations and the significant information inside them. Not exclusively is this strategy costly and complex, yet insight about harming digital breaks keeps on ruling features, delivering this technique insufficient. Indeed, given the space of a gathering of individuals of information breaks, the subject of network protection has dispatched to the highest point of the need list for sheets of chiefs, which they appeared similar to a safer way. All things being equal, associations can consider a locally incorporated, mechanized Next-Generation Security Platform that is explicitly intended to give steady, counteraction put together insurance – concerning the endpoint, in the server farm, on the organization, out in the open and private mists, and across Saab's surroundings. By zeroing in on avoidance, associations can forestall digital dangers from affecting the organization in any case, and less in general network protection hazard to a reasonable degree.

### *Types of Cyber Security Threats*

The utilization of staying aware of new advancements, security patterns and danger insight is a difficult errand. Notwithstanding, it ought to be to shield data and different resources from digital dangers, which take many structures.
- Ransomware is a type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them.
- Malware is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses, and spyware.
- Social engineering is an attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.
- Phishing is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, these emails intend to steal sensitive data, such as credit card or login information.

### *What are the consequences of a cyber-attack?*

Cyber-attacks will cause more harm monetarily and reputationally even to the most enduring association. The association which experiences a digital assault should confront losing resources, business notoriety, and possibly the association needs to confront administrative fines and making a legitimate move and the expenses of remediation. A study taken by the UK government about digital protection in 2017, observed that the normal expense for an enormous business is £19,600 and for a little to medium-sized business is £1,570.

### *What does a security analyst do?*

A data security examiner ensures to safe the organization's frameworks and organizations by arranging and doing proportions of safety. They make problematic answers to keep basic data from being taken, harmed, or compromised. Their essential obligation is to keep a business or association's information, customers, representatives, and any virtual put away data protected from digital assaults or hacking of any kind.

***What are managed cyber security services?***

Numerous associations presently try to re-appropriate parts or all of their online protection capacities to a confided in security supplier. Overseen security administrations (MSS) is an assistance model or capacity given by network safety specialist organizations to screen and oversee security gadgets, frameworks, and even programming as-a-administration (SaaS) applications

An oversaw security administrations supplier (MSSP) offers nonstop (frequently 24x7or 8x5 help) data security checking and the executives. A worldwide, proactive assurance conveyance model identifies emergency malevolent security occasions.

The manuscript is relevant for the Acta logistical journal.

- Manuscript is new, interesting, original, and high quality.
- Manuscript is prepared, logically, and correctly.
- Language of the manuscript is clear and understandable.
- Figures, diagrams, charts, and tables of the manuscript are readable, clear, and high quality.
- References of the manuscript are used correctly.

The survey cycle proceeds of notice for creators if the original copy is feasible to acknowledge without alteration, acknowledge later adjustment or reject. The survey cycle closes with checking of last pdf article form and affirming the article for distributing in the diary by the writers (if the composition was acknowledged by the editorial manager and commentators for distributing). The supervisor of the diary has the option to oversee and, in specific conditions, change the companion audit process at his caution.

## 3 Recent Cyberattacks on the Logistics Sector

In the year 2020, shipping and logistics businesses were hit by a large number of digital assaults. A flatbed shipping organization in the United States reported in October 2020 that one of its running organizations had been assaulted by ransomware. They declared later the Continental ransomware bunch delivered documents on the dull web professing to be from the functional organization.

A shipping and cargo transportation strategies organization experienced a Hade malware contamination in December 2020. Accordingly, the organization had to take all of its IT frameworks disconnected while it managed the attack [4].

The COVID-19 vaccination inventory network has additionally been focused on, with phishing messages being utilized this time. A dangerous entertainer accessed a German biomedical firm that is indispensable to the COVID-19 virus chain. They then, at that point, sent phishing messages to the organization's accomplices who were engaged with shipping the inoculation.

### IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain

IBM Security X-Force formed a hazard talent task pressure centred on searching down COVID-19 cyber threats in opposition to companies that keep the vaccination provide chain going at the beginning of the pandemic. Our team has discovered a world phishing try concentrated on corporations involved in the COVID-19 cold chain as a phase of these efforts. The cold chain is a thing of the vaccine grant chain that ensures the safe storage and shipping of vaccines in temperature-controlled stipulations.

According to our research, this projected operation started in September 2020. The COVID-19 phishing marketing campaign cantered groups likely linked with Gavi, The Vaccine Alliance's Cold Chain Equipment Optimization Platform (CCEOP) program, which we talk about in more detail in this blog. While unique attribution for this marketing campaign ought to not be established, the targeted targeting of leaders and sizeable global companies ought to be hallmarks of nation-state tradecraft.

### Some details from IBM Security X-Force's analysis of this activity include:

The Cover Story — The foe mimicked a business chief from Haier Biomedical, a valid and genuine part organization of the COVID-19 immunization production network and qualified provider for the CCEOP program.

The organization is purportedly the world's just finished virus chain supplier [5]. Masked as this worker, the foe sent phishing messages to associations accepted to be suppliers of material help to address transportation issues inside the COVID-19 virus chain. We survey that the reason for this COVID-19 phishing effort might have been to reap qualifications, conceivably to acquire future unapproved admittance to corporate organizations and delicate data identifying with the COVID-19 antibody conveyance.

The Targets — The objectives incorporated the European Commission's Directorate-General for Taxation and Customs Union, just as associations inside the energy, producing, site creation, and programming and web security arrangements areas. These are worldwide associations settled in Germany, Italy, South Korea, the Czech Republic, more noteworthy Europe, and Taiwan.

**The How — Spear-phishing emails were sent to select executives in sales, procurement, information**

Technology, and finance positions, likely involved in company efforts to support a vaccine cold chain. We also identified instances where this activity extended organization-wide to include help and support pages of targeted organizations [6].

IBM Security X-Force has followed responsible disclosure protocols and notified the appropriate entities and authorities about this targeted operation [7].

## 4 Cybersecurity Challenges Abound

A few advanced difficulties face shipping and coordinated operations organizations simultaneously. One of the most vital is joining security with contemporary innovation. Sensors and other Internet of things (IoT) gadgets are utilized by most endeavours in this area to help them to screen and deal with their production network activities [8].

From one perspective, these devices yield helpful associations. On the other, they confuse things by adding savvy items into the organization that frequently need security by the plan. Malevolent entertainers could mishandle programming defects inside those gadgets to upset business.

The inventory network is likewise in danger. Numerous strategies and shipping organizations, similar to firms in different enterprises, give their sellers, accomplices, and providers network access. This choice lifts network and productivity, permitting these associations to adhere to their timetables. Be that as it may, it likewise builds the assault surface. A hurtful entertainer could utilize this admittance to think twice about those outsiders. They would then be able to exploit their organization admittance to think twice about shipping and coordinated factors accomplice.

### The Human Element

In conclusion, many shipping and operations substances come up short on the ability to protect themselves against these kinds of computerized dangers. In a 2019 report, for example, Eye for Transport (EFT) saw that less than half (43%) of shipping and coordinated operations associations had a central data security official (CISO). That didn't trouble most respondents, nonetheless, just 21% of them told EFT they believed they required a CISO's aptitude. These discoveries feature two issues. In any case, an organization without a CISO is probably not going to have an unmistakable arrangement set up for managing assaults. Second, most associations verifiably disregard the need for a decent safeguard since they accept they needn't bother with a CISO. You will not acquire a specialist to manage it on the off chance that you don't accept that you want it in any case [9]. Nonetheless, protecting themselves in any significant way is not a feasible choice. It permits vindictive entertainers to enter through any window or entryway.

### Best Practices for Cybersecurity in Logistics

Adopting an essential strategy incorporates searching for suppliers who approach the security of their shrewd products seriously. Assuming that they disperse firmware updates from a distance and let customers adjust the default administrator accreditations, you'll know they're not kidding. To isolate IoT gadgets, you ought to likewise consider utilizing network division. Subsequently, an expected trade-off of one of these shrewd things will be more averse to spread to the remainder of the IT network [10].

Continuing to store network security, substances need to painstakingly pick their sellers and construct a stock of their chosen accomplices. They would then be able to utilize administration level arrangements to necessitate that sellers complete a danger evaluation to keep up with their business organization. With those outcomes close by, shipping and coordinated operations elements can remediate specific shortcomings by drawing on the strength of their associations with their sellers, providers, and accomplices. This will empower them to execute information encryption and other security best practices just as to form an episode reaction plan if and when an inventory network security occurrence happens.

At last, shipping and coordinated operations associations can achieve these ideas and more by working with a believed oversaw security administrations supplier. Doing as such won't just guide your online protection program yet will likewise assist with building a positive security culture inside the work environment. You probably won't have a CISO, however with the right supplier, you'll have the security aptitude your business needs to adjust to the changing danger scene and limit advanced security hazards going ahead.

## Navigating Rising Cyber Risks in Transportation and Logistics

Transportation and logistics (T&L) companies have embraced digitization, which has improved the industry's upstream and downstream operations. This method has resulted in previously unheard-of efficiencies aimed at increasing revenue sources.

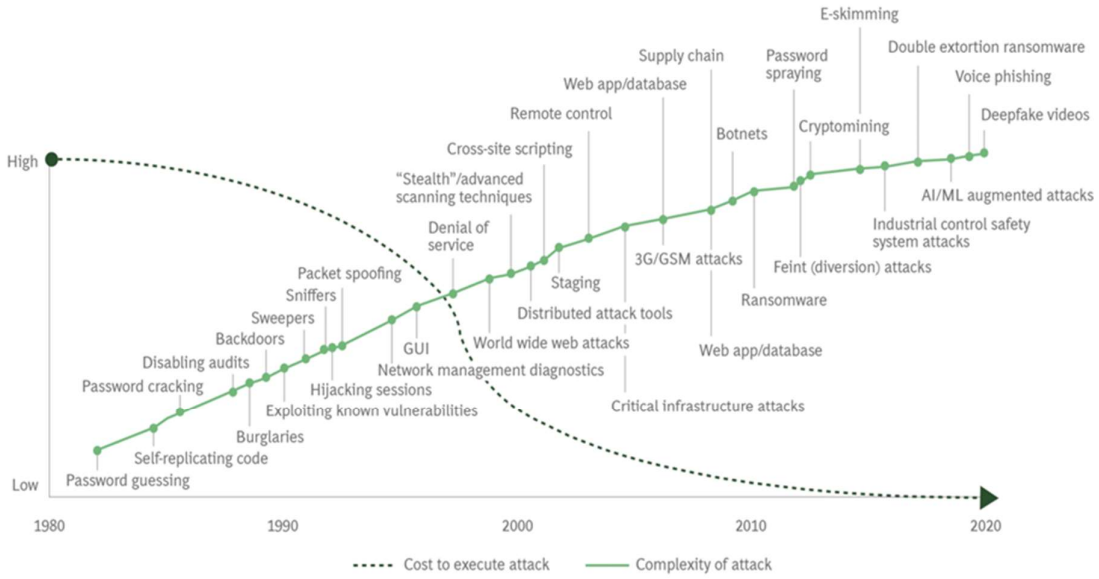
The good news is that this is the case. The negative is that digitization has revealed several flaws in T&L firms, making them very vulnerable to cyber-attacks. Every aspect of the industry is affected, including maritime, rail, trucks, logistics, and package delivery. The expense is high, operations are disrupted, and there is the possibility for additional liability, especially if sensitive customer data is compromised.

The increasing threat is due to several factors. For one thing, the increased usage of operational technology (OT), which provides new communications and wireless channels that are directly related to the digital ecosystems of T&L enterprises, is a soft target for hackers. Furthermore, the T&L business faces a lack of cyber legislation and standards, as well as a lack of cybersecurity knowledge and cyber-defence personnel.

In the T&L industry, cyber assaults used to happen every few years. There appear to be one or two each month now. Some are well-known. For example, in May 2021, a cyber-attack successfully shut down the Colonial Pipeline, which supplies gasoline to about half of the US east coast, for about a week. According to the corporation, the ransom and business disruption might cost upwards of $50 million. Other cyberattacks, including those aimed at major shippers who have been repeatedly targeted, are less well-publicized, but they frequently impair email and logistics systems [11].

The cost of a break-in has decreased dramatically as the potential cyber-attack surface in the T&L sector expands and the nature of risk continues to spread. (As an example, see Exhibit 1.)

Exhibit 1 - Cyber Attack Complexity Increases as Difficulties and Cost to Break-In Decreases




Sources: Information Security Incorporated; BCG analysis.

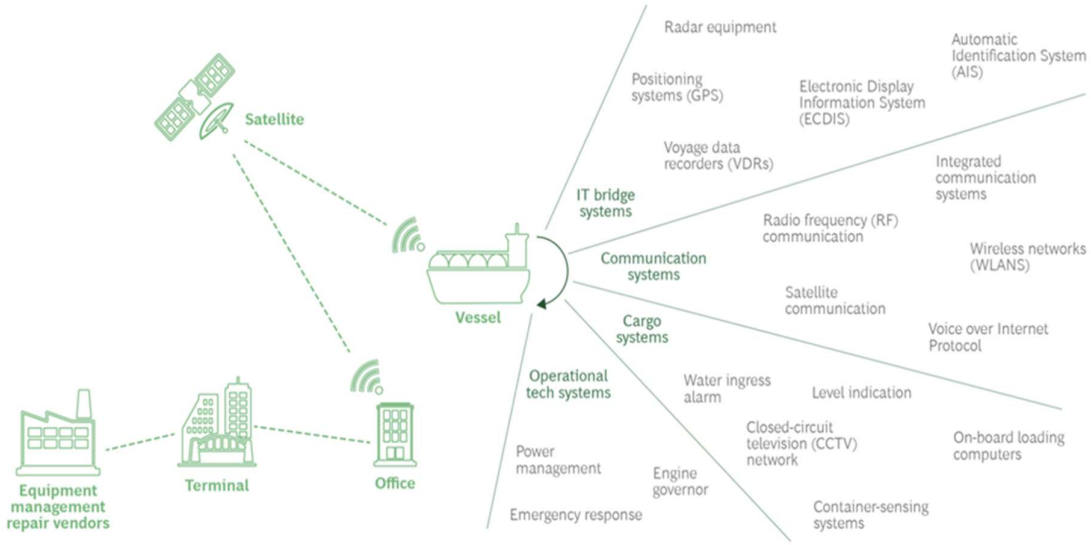
Note: GUI = graphical user interface; GSM = Global System for Mobile Communications.

**Where the weaknesses are?**

The easiest way to look at the dilemma facing T&L companies is to separate their cyber vulnerabilities into three categories: technology, regulation, and people and processes. Each of these categories needs to be considered carefully to address the emerging threats impacting the broader industry.

Technology. In every segment of the T&L industry, the widened cyber-attack surface is evident. For instance, among maritime companies, relatively simple distress-and-safety systems have been replaced by full-fledged, cloud-based, local area networks, like the International Maritime Organization's (IMO) e-navigation program. These networks are a tempting target for hackers because they collect, integrate, and analyze onboard information continuously to track ships' locations, cargo details, maintenance issues, and a host of oceanic environmental considerations. (See Exhibit 2.)

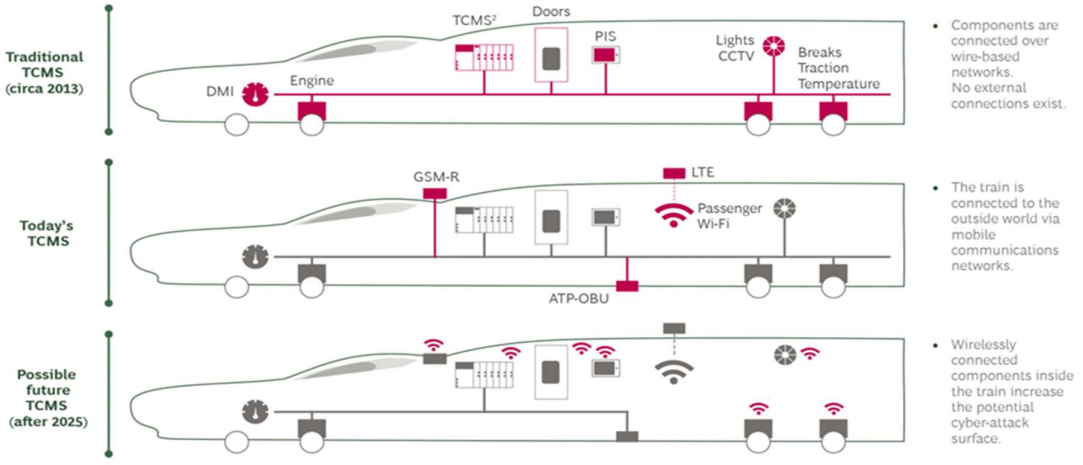
## Exhibit 2 - Cargo Ships Are Increasingly Connected To Communications Systems That Leave Them Vulnerable




Source: BCG analysis.

Similarly, traditional wire-based train control and management systems (TCMS), which had limited communication with external systems, are losing way to wireless standards such as GSM-Railway, a rather large network linking trains to railway regulation control centres. (Exhibit 3 is an example.) T&L companies, like all mobility providers these days, use vehicle infotainment services and other equipment that add another layer of internet-connected communications to their operations.

## Exhibit 3 - Wireless Network Connectivity Is Making Railroads Easy Targets for Hackers




Source: BCG analysis.

Note: DMI = driver machine interface; TCMS = train control and management system; PIS = passenger information system; GSM-R = Global System of Mobile Communications-Railway; LTE = Long-Term Evolution; ATP = automatic train protection; OBU = on-board unit

## 5 How To Address Cybersecurity Risks

Companies withinside the T&L area have to begin riding a cybersecurity schedule with the aid of using analyzing the extent of cyber safety of their OT and IT gadget and programs. They can then place safeguards in the vicinity withinside the maximum important and inclined apps and networks. Models and methods, including cyber danger control and quantification program, can assist in map publicity to cyber threats and set up a portfolio of shielding efforts. Companies have to prioritize the possibility and effect of safety threats on vital belongings whilst sorting their vulnerabilities through the use of a danger-primarily based approach. Companies might also additionally then compare initiatives primarily based totally on their capability to grow resiliency vs. cost, letting them effectively optimize their cybersecurity funding budgets [12].

T&L companies have to recognition on adopting extra complex cyber safety concepts, including zero-agree with architecture, after taking those preventive measures. Every device, user, or software trying to talk with the community is taken into consideration a likely chance beneath neath this paradigm. DMZ (demilitarized zone) technology, which offers tightly regulated surroundings that video display unit's connections inside and out of the business, may be used to create a zero-agree with approach with the aid of using segmenting and segregating networks. When possible, the identical idea must be implemented to inner procedures, including confirming the identity of people, programs, and endpoint gadgets earlier than granting get admission to statistics or belongings.

## 6 Conclusions

In the past years, we observed important shifts in the threat landscape. We observed new malware variants and new versions of well-known legacy exploits. We observed many security breaches due to misconfiguration errors, and we saw this trend extend further into cloud-hosted software and services. Cloud services offer nearly instant access to a wide variety of scalable platforms and services, but with that speed comes a rapidly expanding attack surface, and more opportunities for human error.

The logistics industry has introduced digital innovations at a slower pace compared to other industries that are revolutionized by digital technology. In such a scenario, early detection of vulnerabilities and the ability to monitor systems will help to have a quick and efficient response to breaches, Cybersecurity should be a strategic decision that organizations must implement to maintain high safety standards across the T&L industry.

## REFERENCES


1. DANIEL, SCHATZ, JULIE, WALL. "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 2017.
2. ROUSE, MARGARET. Social engineering definition. Tech Target. Archived from the original on. Retrieved 6 September 2021.
3. SCHATZ, DANIEL; BASHROUSH, RABIH; WALL, JULIE "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 2017.
4. Reliance spells the end of the road for ICT amateurs", 7 May 2013.
5. Description of Cyber Security in organizations. https://www.bombessays.com/description-of-cyber-security-in-organizations/ Retrieved 21 November 2021
6. "Computer Security and Mobile Security Challenges". researchgate.net. Archived from the original. Retrieved 4 November 2021.
7. "Distributed Denial of Service Attack". csa.gov.sg. Archived from the original. Retrieved 12 November 2021.
8. GRUBER, B. Wireless mice leave billions at risk of computer hack: Cyber security firm. Retrieved from https://www.reuters.com/article/us-usa-wireless-mouse-idUKKCN0WP21I 2013.
9. "Multi-Vector Attacks Demand Multi-Vector Protection". MSSP Alert. 2018.
10. DAVID BISSON Cybersecurity Gaps and Opportunities in the Logistics Industry. 2021.
11. MILLMAN, RENEE "New polymorphic malware three-quarters quarters of AV scanners". SC Magazine UK. 2017.
12. SUGAR CHAN, EITAN YEHUDA, RUSSELL SCHAEFER, ALAIN SCHNEUWLY, SHARON ZICHERMAN, STEFAN DEUTSCHER, AND OR KLIE. Navigating Rising Cyber Risks in Transportation and Logistics. 2021.

**Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 15-22 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)**

# ASSESSMENT OF THE TECHNICAL CONDITION OF THE OBJECT CYBERNETIC PROTECTION SYSTEM
# ОЦЕНКА ТЕХНИЧЕСКОГО СОСТОЯНИЯ СИСТЕМЫ КИБЕРНЕТИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТА

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

**Volodymyr Vasko Taras Shevchenko National University of Kyiv, Doctor of Engineering Science, Full Professor, Kiev, Ukraine**
**Владимир Васько, Киевский национальный университет имени Тараса Шевченко (г. Киев).**

**Vasily Kuzavkov, Taras Shevchenko National University of Kyiv, Doctor of Engineering Science, Full Professor, Kiev, Ukraine**
**Кузавков Василий Викторович, доктор технических наук, профессор, профессор Киевского национального университета имени Тараса Шевченко (г. Киев).**

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

**Khokhlachova Yulia, National Aviation University of Kiev, PhD in Technical Sciences, Associate Professor Kiev, Ukraine**
**Хохлачова Юлия Евгеньевна, кандидат технических наук, доцент, доцент Национального авиационного университета (г. Киев).**

**ABSTRACT:** The functioning of infrastructure facilities in such a specific environment as cyberspace associated with vulnerability and threats, therefore, requirements are put forward for the development of new tools for ensuring cyber resilience in the face of cyber attacks. The management of the cybersecurity stability of the functioning of infrastructure facilities is based on knowledge of the state of both the protected objects and the technical system of cyber protection of the objects themselves. That is, the technical state of the cyber defense system has become the dominant threat to industrial and important infrastructures. The paper considers the possibility of using Petri nets to assess the technical state of the object's cyber protection system. The presented method, built on associative principles, makes it possible to predict the technical state of the technical assessment system with a given accuracy, which makes it possible to provide the required level of object cyber security.

**АННОТАЦИЯ:** Функционирование объектов инфраструктуры в такой специфической среде, как киберпространство, связанное с уязвимостью и угрозами, поэтому выдвигаются требования по разработке нового инструментария обеспечения киберстойкости в условиях кибератак. Управление стойкостью кибербезопасности функционирования объектов инфраструктуры базируются на знаниях состояния как защищаемых объектов, так и самой технической системы киберзащиты самих объектов. То есть, доминирующей угроз для промышленных и важных инфраструктур стало техническое состояние системы киберзащиты. В работе рассмотрена возможность применения сетей Петри для оценки технического состояния системы киберзащиты объекта. Представленный метод, построенный на ассоциативных принципах, дает возможность прогнозировать техническое состояние технической системы оценок с заданной точностью, что позволяет обеспечить требуемый уровень киберзащищенности объекта.

**KEYWORDS***: Petri models, cyber security technical systems, cyber resilience*

**КЛЮЧЕВЫЕ СЛОВА:** *модели Петри, технические системы кибербезопасности, киберстойкость.*

**Введение**

События конца XX- начала XXI веков проходят на фоне трансформации общества от постиндустриального к информационному. В мире происходит бурное развитие информационных технологий и их проникновение во все сферы деятельности человека. При этом, к основным характеристикам процесса информатизации общества на современном этапе следует отнести глобализацию и интенсификацию информационных процессов, изменение современной картины мира.

Согласно революции, в области информатизации и коммуникации происходят изменения в управлении государства, отраслей этого государства и определенных объектов инфраструктуры.

На современном этапе развития государства, когда управление информатизацией становится функцией, критично важной для бизнеса, а объемы информации постоянно увеличиваются, все острее становятся вопросы информационной безопасности, в целом, и кибербезопасности в частности [1,2].

При этом функционирование объектов инфраструктуры в такой специфической среде, как киберпространство, связанное с уязвимостью и угрозами, выдвигаются требования по разработке нового инструментария обеспечения киберстойкости в условиях кибератак. Управление стойкостью кибербезопасности функционирования объектов инфраструктуры базируются на знаниях состояния как защищаемых объектов, так и самой технической системы киберзащиты самих объектов. То есть, доминирующей угроз для промышленных и важных инфраструктур стало техническое состояние системы киберзащиты [3].

Разработка и исследование математической модели технической системы кибербезопасности (ТСКБ) требует значительных затрат времени. Как показывает опыт, применение сетей Петри (СП) для таких целей ускоряет процесс их создания. Однако их математический аппарат несколько громоздкий и при реализации на ПЭВМ занимает большие объемы памяти. Для решения практических задач требуется компактная отражающая сущность поведения и функционирования ТСКБ модель. Особенно остро этот вопрос стоит для моделирования в реальном масштабе времени при эксплуатации систем.

Известные на сегодняшний день интерпретации расширения и модификации сетей Петри [4,5] позволяют в основном моделировать параллельные процессы в программном (алгоритмическом) обеспечении вычислительных систем (на разных уровнях – от системного до микропрограммного) т.е., для выполнения двух и более различных алгоритмов на одной и той же вычислительно-управляющей системе требуется при известных подходах создание двух и более сетей Петри для изучения алгоритмов. Кроме того, в таких случаях традиционно присутствует требование отсутствия критических свойств в построенных моделях. В случае обнаружения какого-либо критического свойства делается вывод о неработоспособности рассматриваемого алгоритма и выполняются действия по такому изменению алгоритма, чтобы во вновь построенной адекватной модели критические свойства не были обнаружены. Основной недостаток такого подхода заключается в большой трудоемкости процесса многократного построения моделей алгоритмов для изучения их работоспособности.

**Цель работы.**

Целью работы является рассмотрение возможности применения сетей Петри для оценки технического состояния системы киберзащиты объекта.

**Основная часть.**

Таким образом, опыт использования модификации сетей Петри для моделирования сложных систем и оценки технического состояния их позволяет утверждать, что средства моделирования должны обладать следующими свойствами [6,7,8]:

- иерархическое представление моделей;
- единые средства построения и описания моделей на всех уровнях иерархии;
- простота детализации моделей;
- легкость машинного представления создаваемых моделей;
- возможность концентрации внимания только на необходимых (анализируемых) состояниях и режимах работы системы;
- возможность использования одной модели в разных целях;
- возможность моделирования до уровня логических элементов;
- использование формальных методов оптимизации процессов моделирования и анализа;
- наличие способов контроля корректности построения модели и исследования свойств модели;
- возможность представления всего моделируемого и анализируемого процесса в динамике;
- простота и наглядность при формулировании проблемы или алгоритма оценки технического состояния объекта исследования (в нашем случае ТСКБ).

В результате проведения анализа известных попыток использования сетей Петри для анализа технического состояния ТСКБ была разработана оригинальная модифицированная система – аппаратные сети Петри [8].

Для эффективного использования широкого спектра возможностей аппаратных сетей Петри (АСП) необходимо на базе АСП-системы специального математического обеспечения с набором средств описания, ввода, вывода, трансляции, компоновки, имитации модели, обработки результатов моделирования и анализа.

В настоящее время известны ряд способов описания исходных моделей и внутримашинного представления моделей ТСКБ для проведения имитационных экспериментов на базе СП.

При построении системы имитационного моделирования на СП существенную роль играет выбор:

способа описания исходных моделей;

способа внутримашинного представления описанной модели и на его основе – организации алгоритма моделирования.

Внутримашинное представление СП может быть организовано в виде матриц, либо в виде списков структур.

В нашем случае внутримашинное представление организовывается матриц. Поэтому СП может быть описана двумя типами матриц: матрицей инцидентности E размерностью n x m, где n – число вершин мест, m – число вершин переходов модели, и матрицей движения меток F размерностью, которые определяются следующим образом:

1) $E(i,j) = 1, \text{если } P_i \in P_{ij}^I;\ E(i,j) = 0, \text{если } P_i \notin P_{ij}^I;$

2) $F(i,j) = \alpha + \beta$, где $\alpha = 1$, если $P_i \in P_{ij}^I$;

$\alpha = 0$, если $P_i \notin P_{ij}^I$; $\beta = -1$, если $P_i \in P_{ij}^0$

$\beta = 0$, если $P_i \notin P_{ij}^0$.

Обозначим $A^j$ - j-й столбец матрицы A. Тогда можно утверждать:

а) переход $t_j$ может быть запущен, если $E^j - m_0^{-(k)}$;

б) последующая разметка после срабатывания t вычисляется по формулам

$m_0^{-(k+1)} = m_0^{-(k)} + F^{(I)}$,

$-\left[E_j \longrightarrow m_0^{-(k)}\right] \equiv \left[E^j m_0^{-(k)}\right] = \left[E^j \Big/ m_0^{-(k)} = 0\right]$.

Следовательно, условие запуска переходов $t_j$ состоит в выполнении условия $E^j m_0^{-(k)} = 0$, а последующая разметка вычисляется следующим образом:

$m_0^{-(k+1)} = m_0^{-(k)} \oplus B^{(j)}$, где $\oplus$ - обозначение операции, исключающей ИЛИ; B(i,j) =1, если F(i,j)≠0; B(i,j) =0, если F(i,j)=0.

Здесь все операции выполняются над векторами булевых переменных, что позволяет достаточно эффективно реализовывать этот способ на ПЭВМ.

Недостаток указанного способа заключается в необходимости проверки на каждом шаге моделирования разметки всех входных мест каждого из переходов, что приводит к значительным неэффективным затратам времени. Более высокое быстродействие достигается путем представления каждого из переходов $t_v$ одним из мест $P_E^\tau \in P_{tv}^I$. Для запуска перехода $t_v$ необходимо (но недостаточно) выполнение $m(P_E^\tau) = 1$.

Определим вектор булевых переменных D размерностью m x 1, а также матрицы A и C размерностью m x m:

- D(j) = 1, если $m(P_i^\tau) = 1,\ P_i^\tau \in P_{ij}^I$;
- C (i,j) = 1, если $t_j$ и $t_i$ представлены одним и тем же местом $P_\varepsilon^\tau$;
- A(i,j) =1, если $t_j$ представлено местом $P_\varepsilon^\tau \in \Theta_{ij}$.

Тогда после срабатывания $t_i$ последующая разметка вычисляется по формуле $D^+ = D \oplus A^j \oplus C^j$ и модулирующий алгоритм выглядит следующим образом:

DATA INPUT

FOR j: = 1 TO m DO

IF D(j) = 1

THEN IF $m_0^{-(k)} E_j = 0$

THEN < генерация действий, соответствующих $t_j$ >

$m_0^{-(k+1)} = m_0^{-(k)} \oplus B^{(j)}$

$D^+ = D \oplus L^j$.

Здесь $L^j = A^j \oplus C^j$ позволяет экономить объем используемой памяти. При таком подходе можно сократить время выполнения программы с одновременным увеличением объема занимаемой памяти (за счет матрицы L и вектора D). Для снижения объема занимаемой памяти целесообразно внутримашинное представление моделей в виде стековых структур, так как E, F, L – разреженные матрицы. В результате размер используемой памяти линейно зависит от значений m и n, тогда как в случае матричного представления этот размер пропорционален m x n.

Одним из способов достижения компромисса между сложностью и достоверностью математической модели является упрощение эквивалентной объекту сети производящееся с помощью маршрутов функционирования системы [4] на основе аппарата нечетких множеств и нечетких отношений в пространстве, определенном расширяемой базой делимых ТСКБ. В эту

же базу данных заносятся сведения о поведении системы при внешних воздействиях. Модели, получаемые таким способом, имеют управляемую размерность и на основе строгих математических правил преобразуются либо в компактный, либо в расширенный вид. Достоверность модели ТСКБ является не выходным, а входным параметром для моделирования. Отсюда и главным достоинством такого подхода является маршрутная модель с заранее задаваемой достоверностью, позволяющая прогнозировать динамику состояния ТСКБ.

Рассмотрим принципы построения маршрутов, маршрутных моделей и моделирующей базы данных. Примем за X универсальное множество возможных состояний моделируемого объекта. Пусть X моделируется с требуемой достоверностью $\varphi$ множеством описаний $M_o$, состоящих из элементов $\overline{m}$.

Поэтому

$$M_0 \leq \chi;$$
$$M_0 = \left\{ {}^{M}/_{\overline{M}} \in X,\ \mu(\overline{M}) \geq 1 - \varphi \right\}, \quad (1)$$

где $\mu(\overline{M})$ – функция принадлежности описания $\overline{M}$ множеству X.

Маршрут, как отображение Марковского процесса с нечеткими начальными условиями по отношению к нечеткому множеству описаний $M_0$, является множеством уровня $\alpha \neq 1 - \varphi$;

$$M = \left\{ {}^{\overline{M}}/_{M_0},\ \mu(\overline{M}) > \alpha \right\}, \quad (2)$$

Однако учитывая правила упорядочения элементов в $M_0$ маршрут можно представить в виде APN = (P,T,K,S), где $M_0$ отображает характер компонента APN.

Будем считать, что множество отношений, соответствующих «нормальному» маршруту $M_н$, определяется как:

$$M_н = \left\{ {}^{\mathrm{M}}/_{\overline{\mathrm{M}}} \in \mathrm{M}_0, \mu(\overline{\mathrm{M}}) > \beta \right\}, \quad (3)$$

где $\beta$ – параметр задаваемой устойчивости ТСКБ к внешним воздействиям.

В тоже время для «экспериментального» маршрута $M_э$ справедливо следующее утверждение:

$$M_э = \left\{ {}^{\mathrm{M}}/_{\overline{\mathrm{M}}} \in \mathrm{M}_0,\ \mu_э(\overline{\mathrm{M}}) > \beta^I \right\}, \quad (4)$$

где $\beta^I$ – параметр задаваемой границы неустойчивости ТСКБ.

При расширении и сужении множеств моделирующих отношений следует руководствоваться следующими принципами расширения нормативного маршрута с учетом экспериментального маршрута:

$$M_1 = \left\{ {}^{\mathrm{M}}/_{\overline{\mathrm{M}}} \in \overline{\mathrm{M}}_0,\ \mathrm{M}_1(\overline{\mathrm{M}}) \right\}, \quad (5)$$

где

$$\mathrm{M}_1(\overline{\mathrm{M}}) = \begin{cases} 0, \text{ если } \{\mu_э(\overline{\mathrm{M}}) \mathrm{X} \mu_н(\overline{\mathrm{M}})\} < \beta \\ max[\mu_э(\overline{\mathrm{M}})] \text{ если } \left[\mu_н(\overline{\mathrm{M}}) V \mu_{ij}(\overline{M})\right] \geq \beta \end{cases}.$$

Сужение экспериментального маршрута с учетом нормативного маршрута описывается:

$$M_2 = \left\{ \overline{\mathrm{M}}/_{\mathrm{M}} \in \overline{\mathrm{M}}_0,\ \mathrm{M}_2(\overline{\mathrm{M}}) \right\}, \quad (6)$$

где

$$\mathrm{M}_2(\mathrm{M}) = \begin{cases} 0, \text{ если } [\mathrm{M}_э(\overline{\mathrm{M}}) V \mu_н(\mathrm{M})] \geq \beta \\ max[\mathrm{M}_э(\mathrm{M}), \mathrm{M}_н(\mathrm{M})] \text{ если } [\mathrm{M}_э(\mathrm{M}), \mathrm{M}_н(\mathrm{M})] \leq \beta \end{cases}.$$

Из условий (5) и (6) следует

$$\lim_{\beta \to 0} M_1 = \lim_{\beta \to 0} M_2 = M_0. \quad (7)$$

Скорость переходов и достоверность размещений для позиций моделирующей СП является мерой информативности соответствующим им отношений.

При $\beta = 1$ в СП, синтезируемую на маршрутных множествах, войдут наиболее «живые» переходы СП, построенные на $\mathrm{M}_0$ [8]. По мере роста количества узлов СП функция принадлежности перехода множеству «живых» переходов убывает. Заменив понятия скорость на экспертную оценку принадлежности перехода множеству «живых» переходов, удается отойти от непосредственного решения вопроса о возможности срабатывания того или иного перехода.

Для множества состояний типа маршрутных множеств исходное состояние обозначим через $M_p$ , а достижимое из него как $M_p^+$. Тогда прогноз как линейный оператор описывается следующим образом:

$$F = M_p^- = M_p^+, \quad (8)$$

где F - линейный оператор прогноза:

$$M_p^- \subseteq \text{ и } M_p^+ \subseteq M_1.$$

Прогноз как функция определяется в базисе $\mathrm{M}_0$ как функция принадлежности состояния $M_p^-$ множеству оценок технического состояния ТСКБ [9]. Аспекты прогноза имеют свои прогнозы в APN и формализуется как линейный оператор в пространстве, порождаемом $\mathrm{M}_0$, и как функционал, определяемый линейной формой в пространстве $\mathrm{M}_0$.

Из соотношения (8) видно, что прогноз как линейный оператор и как, функционал образуют дерево возможностей, так как по определению из выражений (5) и (6) следует, что мощность $\mathrm{M}_1$ больше, чем $\mathrm{M}_2$. При машинной реализации это приводит к решению задач комбинаторного типа и к экспоненциальному росту размерности модели. Вследствие этого проводим отсечение ветвей, т.е. принимаем к рассмотрению только те ветви дерева возможностей, функция принадлежности которых $\mathrm{M}_0$ менее $\beta$. Основой для реализации такого подхода на ПЭВМ следует выделение и анализ так называемых стационарных состояний ТСКБ. По отношению к $\mathrm{M}_0$ множество стационарных состояний определяется как

$$M_0 \leq M_c,$$

$$M_c\{\overline{M}/\overline{M} \in M_{01} M_c(\overline{M})\} \cong 1,$$

где $M_c$ – множество стационарных событий. Все элементы $\mathrm{M}_c$ являются корнями нормированного маршрута при отсутствии внешних воздействий. Внешние воздействия образуют пространство возмущений, базисом которого является элементарное воздействия [10,11]. Каждому элементу $\mathrm{M}_c$ соответствует нечетко ограниченное подпространство пространства возмущений. Иными словами, элементом $\mathrm{M}_c$ присваивается чувствительность к элементам базиса пространства возмущений, тем самым давала начало экспериментальному

маршруту. OS каждого стационарного состояния ведет свое начало множество экспериментальных маршрутов, по одному на каждый нулевой элемент базиса подпространства возмущений. Отношения между маршрутными множествами и множеством стационарных состояний поля

$$M_э \cap M_c = M_н \cap M_c = M_c.$$

Другими словами, базисные воздействия порождают символы деревьев возможностей.

Анализ стационарных состояний ТСКБ должен выявить возможность между ними. В случае большой сложности оборудования применяются экспериментальные оценки взаимосвязанности элементов $M_0$. Результат анализа – СП стационарных состояний, является основой для построения базы данных и прогнозирования технического состояния ТСКБ.

Так как СП стационарных состояний включает в себя узловые моменты функционирования ТСКБ, то она отражает характер поведения оборудования согласно заложенному алгоритму. Таким образом, СП стационарного состояния является моделью штатной работы ТСКБ. Прогнозируемость технического состояния системы опирается на марковский характер функционирования оборудования, с одной стороны и на систему оценок ТСКБ – с другой стороны.

Для корректного определения технического состояния ТСКБ необходима система оценок, которая удовлетворяла бы следующим требованиям [11]:

1) система оценок технического состояния должна содержать приоритеты (веса) соответствующих выходных ветвей СП стационарных состояний, выражающихся в виде функций принадлежностей состояний выходной ветви множества технических состояний ТСКБ;
2) глубина рассмотрений (детализации) технических состояний ТСКБ определяется задаваемой достоверностью $\varphi$.

С учетом этих требований модель системы реализуется на основании выражений (1)-(8) и представляет собой модель построенную на ассоциативных принципах. В зависимости от требуемой достоверности моделирования глубины поиска в базе данных и подключения узлов сетей Петри может изменяться в широких пределах, так как данные в базе данных упорядочены в виде множества пересекающихся деревьев. Пересечение деревьев следует понимать, как нечеткое отношение. Узел пересечения представляет собой нечеткие множества, которым придана мера в виде функции принадлежности узла дерева узлу ассоциации. В зависимости от переходных требований ассоциации требования к модели могут расширятся, распределяться или образовывать с другими ассоциациями новую, более широкую модель системы. Сведенные в базу данных маршруты организуют ассоциативный доступ к характерным состояниям ТСКБ, одновременно дополняя содержащуюся в базе данных информацию новой необходимой и при этом удаляя старую ненужную.

**Выводы**

Представленный в работе метод позволяет прогнозировать техническое состояние технической системы оценок с заданной точностью, что дает возможность обеспечить требуемый уровень киберзащищенности объекта.

**ЛИТЕРАТУРА**

1. Грищюк Р.В., Даник Ю.Г. Основи кібернетичної безпеки – Житомир: ЖНАЕУ, 2016. – 636 с.
2. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. – К: ТОВ «СІК ГРУП Україна», 2015. – 449 с.

3. Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації. – К: ЦП «Компринт», 2021. – 296 с.
4. Питерсон Дж. Теория сетей Петри и моделирующие системы. Изд. 2-е. – М.: Мир, 2001. – 266 с.
5. Котов В.Е. Сети Петри. Изд. 3-е. – М.: Наука, 2004. – 168 с.
6. Томашевский В.М. Моделирование систем. К.: Вид. Груп BHV, 2007 – 352 с.
7. Креденцер Б.П., Буточнов О.М., Міночкін А.І., Могилевич Д.І. Надійність систем з надлишковістю: методи, моделі, оптимізація. – К.: «Фенікс» 2013. 342 с.
8. Хорошко В.А., Моржов С.В. Применение сетей Петри для моделирования параллельных процессов// Проблемы управления и информатики, №2, 2004. – с. 86-94.
9. Опірський І.Р. Проблематика основного постулату прогнозування НСД // Сучасна Спеціальна Техніка, №2 (41), 2015.- с. 3-8.
10. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности – К.: Изд. ГУИКТ, 2009. – 215 с.
11. Хорошко В.А., Чирков Д.В. Исследование процессов и структур систем защиты на основе аппарата Петри // Системи обробки інформації. – Вип. 7 (88), 2010. – с.236-245.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 23-29 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

# A SURVEY ON KNOWLEDGE AND COMMONSENSE REASONING FOR NATURAL LANGUAGE PROCESSING

**Aliyu Ahmed Abubakar Kaduna State University Wuhan University**

**ABSTRACT:** People use knowledge and commonsense reasoning for daily activities and survival. However, providing machines with such humanly knowledge and commonsense reasoning experiences has remained a vague target of artificial intelligence researchers for years. This report surveys knowledge and commonsense reasoning for Natural Language Processing with the aim of providing an overview of the benchmarks, knowledge resources, state of the art and inference approach toward knowledge and commonsense reasoning for natural language processing.

**KEYWORDS –** *Commonsense Reasoning, Knowledge Resource, Natural Language Processing (NLP), Artificial Intelligence (AI)*

## 1. Introduction

Knowledge and commonsense reasoning is the cornerstone of the application of human intelligence according to (Razniewski, Tandon, & Varde, 2021). Knowledge and commonsense reasoning in artificial intelligence (AI) is a human-like ability to make assumptions regarding the kind and essence of normal situations humans encounter daily. These presumptions include decisions regarding the nature of peoples' intentions, physical objects and taxonomic properties. Knowledge and commonsense reasoning is relevant for several applications of current interest and such applications include robot and human collaboration, transparent machine-learning systems which will be able to explain their conclusions, dialogue systems, social media and story understanding software.

With the speedy improvement of Human Computer Interactions engines (such as chat, dialogue systems and QA), making use of knowledge and commonsense reasoning in natural language understanding has become a very important area in NLP, as they are necessary for conversation engines or other sorts of HCI engines to comprehend user queries, manage conversations, as well as generating responses (Zhou, Duan, Wei, Liu, & Zhang, 2018). Knowledge and commonsense reasoning have acquired repeated consideration from the natural language processing (NLP) community recently, resulting numerous exploratory research directions into automated commonsense understanding (Maarten, Vered, Antoine, Yejin, & Dan, 2020). Devlin, Chang, Lee, & Toutanova, (2019); Liu, et al. (2019), have lately, made lots of advances in large pre-trained language models where they tried pushing machines nearer to humanlike understanding capabilities, making researchers wonder if machines could directly model commonsense through symbolic integrations.

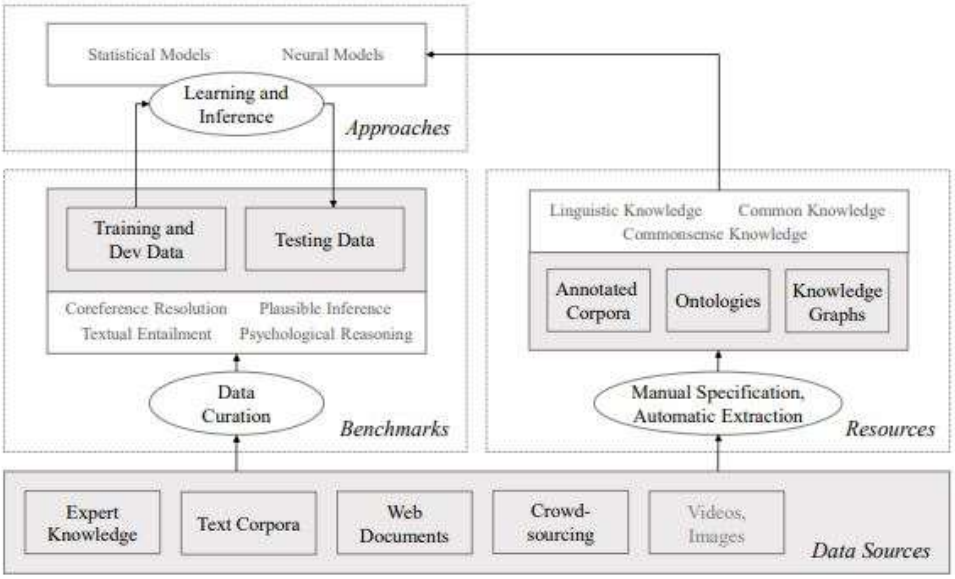
Davis & Marcus (2015) however, explained that notwithstanding these outstanding performances and advances in a multiplicity of NLP tasks, it's still imprecise whether these models are performing complex reasoning, or if they are simply learning complex surface correlation patterns (Marcus, 2018). Ye, Chen, Wang, & Ling (2020) have proposed a pre-training method for integrating commonsense knowledge into language representation models where they built a commonsense-related multi-choice question answering dataset to be used for pre-training a neural language representation model. Tandon, Varde, & Melo (2017) believe that mining knowledge and commonsense from huge amounts of data and applying it in intelligent systems, in many ways, seems to be the subsequent edge in computer science where they briefly presented an overview of the state of Commonsense Knowledge in Machine

Intelligence offers insights into Commonsense Knowledge acquisition, Commonsense Knowledge in natural language, applications of Commonsense Knowledge and conversation of related issues.

A very good survey on NLP was carried out by Gupta (2014) where he concluded that recent research in NLP shows more interest on learning algorithms which could be either semi-supervised or unsupervised in nature and available tasks of NLP are mostly: morphological separation, discourse analysis, natural language generation and understanding, machine translation, tagging of part of speech, recognition of named entities, optical characters recognitions, recognition of speech and analysis of sentiments etc.

Davis & Marcus (2015); Marcus (2018) have done an excellent job in providing a detailed account ranging from troubles in understanding and framing knowledge and commonsense reasoning for definite or general domains to difficulties in various forms of reasoning and their assimilation for the purposes of problem solving. Another interesting survey on commonsense knowledge reasoning for natural language understanding has been carried out by Storks, Gao, & Chai (2019) and the survey categorized commonsense knowledge and reasoning from the NLP community into three areas: benchmarks and tasks, knowledge resources, and learning and inference approaches as shown in the below figure.

Fig. 1.




Storks, Gao & Chai (2019)'s main research efforts in commonsense knowledge and reasoning from the NLP community in three areas: benchmarks and tasks, knowledge resources, and learning and inference approaches.

## 2. Overview of Existing Benchmarks

The NLP community has an extensive history of forming benchmarks to simplify algorithm development and evaluation for language processing tasks such as question answering, coreference resolution and named entity recognition (Storks, Gao, & Chai, 2019). Storks et. al. (2019) gave a review of broadly used benchmarks, presented by the subsequent groupings: textual entailment, question answering, plausible inference, multiple tasks, coreference resolution and psychological reasoning.

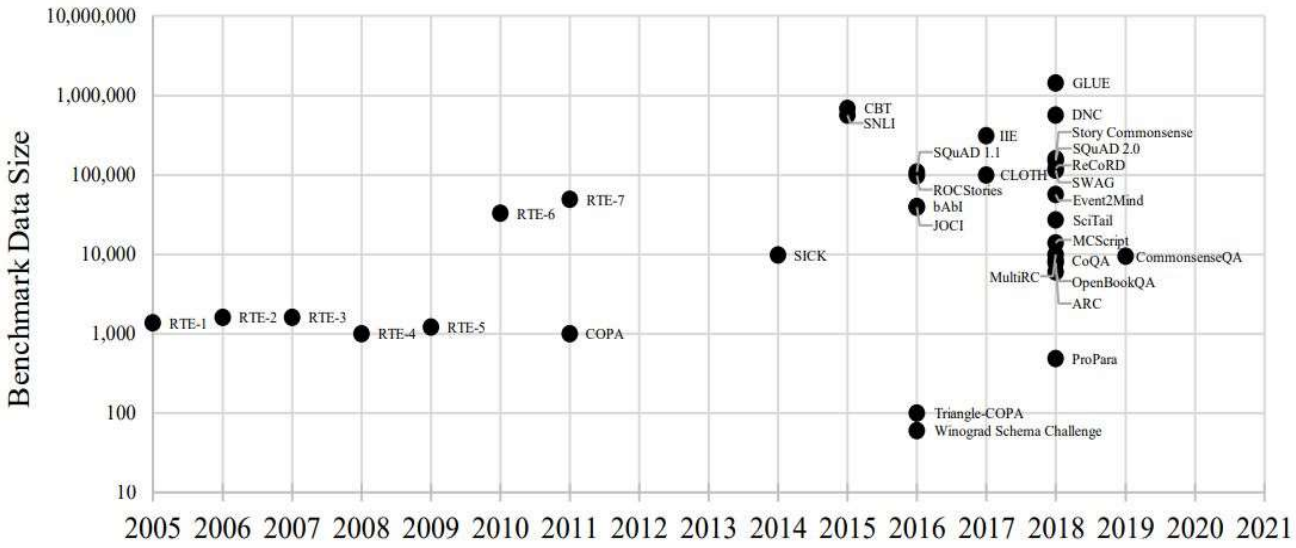



Fig. 2. Benchmark tasks between 2005 to 2021 geared towards commonsense reasoning for Natural Language Processing by (Storks, Gao, & Chai, 2019).

Ruder (2021) has defined a benchmark as it is used in NLP normally with numerous components: it entails of one or multiple datasets, one or multiple related metrics, and a means to aggregate performance where he stated that in order to continue making improvement, there is need to update and refine the metrics, to replace efficient simplified metrics with application-specific ones. The recent GEM benchmark, for instance, explicitly includes metrics as a component that should be improved over time, as shown in the figure below.

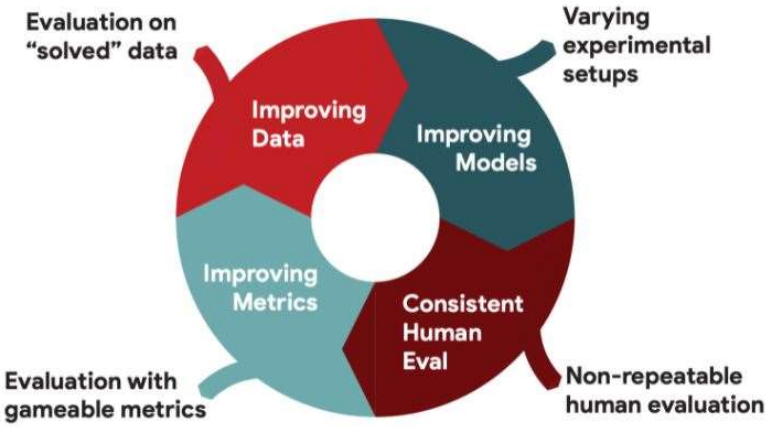


Fig. 3 Circle of challenges and opportunities of benchmark evaluation by (Gehrmann, et al., 2021).

A typical example of benchmark is the Rainbow Commonsense Reasoning benchmark. Rainbow is a worldwide commonsense reasoning benchmark spanning both social and physical common sense that brings together six existing commonsense reasoning tasks: aNLI, Cosmos QA, HellaSWAG, Physical IQa, Social IQa, and WinoGrande (Lourie, Bras, Bhagavatula, & Choi, 2021).

## 3. Knowledge Recourses

To understand human language, it is important to have linguistic knowledge resources that allow computers to identify syntactic and semantic structures from language and these structures in several cases need to be augmented with commonsense knowledge and common knowledge in order to reach a full understanding (Storks, Gao, & Chai, 2019). Chklovski (2003) has estimated that a typical human has accumulated numerous million diverse axioms of commonsense by adulthood. Baud, et al. (1996) have published a paper aiming at reviewing the problem of feeding Natural Language Processing (NLP) tools with convenient linguistic knowledge in the medical domain were he explained that a syntactic approach lacks the potential to solve a number of typical situations with ambiguities and is clearly insufficient for quality treatment of natural language.

Baud, et al. (1996) concluded that all the knowledge sources mentioned in his paper - together with others of course - are useful for NLP and when mining knowledge from various sources one is confronted with the problem of multiple or incompatible representation and one way to apparently solve this problem is to add another representation at the risk of augmenting the confusion for future users.

Some of the linguistic knowledge resources are:

I. Annotated linguistic corpora (Marcus, Santorini, & Marcinkiewicz, 1993)
II. Lexical resources. by (Miller, 1995)

Some of the common knowledge resources are:

i. YAGO by (Suchanek, Kasneci, & & Weikum, 2007)
ii. DBpedia by (Auer, et al., 2007)
iii. WikiTaxonomy by (Ponzetto & M, 2007)
iv. Freebase by (Bollacker, Evans, Paritosh, Sturge, & Taylor, 2008)

Some of the commonsense knowledge resources are:

i. Cyc by (Lenat & Guha, 1989)
ii. ConceptNet from (Liu & Singh, 2004)
iii. AnalogySpace (Speer, Havasi, & Lieberman, 2008)
iv. SenticNet by (Cambria, Speer, Havasi, & & Hussain, 2010)
v. ATOMIC by (Sap, et al., 2019)

There are several approaches to creating knowledge resources ranging from manual encoding to web documents text mining and crowdsourcing collection (Davis & Marcus, 2015) (Storks, Gao, & Chai, 2019).

### 3.1 Knowledge and Commonsense SOTA

There are several recent commonsense reasoning datasets that motivated researches in several aspects and domains which include: temporal, abductive, physical and social (Bhagavatula, et al., 2020). According Brown, et al. (2020) SOTA for most of them have achieved the close to human accuracy of

over 80%. Conversely, their success is said to be due to larger pre-trained corpora as well as much more parameters, which would be challenging to be followed for most researchers.

## 4. Inference Approaches

Subsequently, Natural Language Inference is considered a benchmark task for testing the natural language understanding ability of the model by GLUE, Natural Language Inference has been well researched, and the language models have attained performance beyond humans on some Natural Language Inference datasets (Huang, He, & Liu, 2021). Additionally, by influencing transfer learning from large Natural Language Inference datasets, great performances have been achieved in numerous tasks, like in story ending prediction Li, Ding, & Liu (2019) and intent detection (Zhang, et al., 2020).

Huang, He, & Liu (2021) have proposed a framework that converts various commonsense reasoning tasks to a common task, Natural Language Inference and used a pre-trained language model, RoBERTa in solving it. By influencing transfer learning from large Natural Language Inference datasets, QNLI and MNLI, and adding vital knowledge from some knowledge bases like ATOMIC and ConceptNet, and their framework achieved state of the art unsupervised performance on the two commonsense reasoning tasks: CommonsenseQA and WinoWhy. Results from the experiments show that knowledge from QNLI and extracted from either ConceptNet or ATOMIC can complement one another to improve the model's performance on commonsense reasoning.

## 5. Conclusion and Recommendations

This survey explores the impact and importance of knowledge and commonsense reasoning in NLP. The survey provided a synopsis of the benchmarks, knowledge resources, state of the art and inference approach toward knowledge and commonsense reasoning for NLP. Devlin, Chang, Lee, & Toutanova (2019); Liu, et al. (2019), were the researchers who lately, made lots of advances in large pre-trained language models where they tried pushing machines nearer to humanlike understanding capabilities, making other researchers wonder if machines could directly model commonsense through symbolic integrations. Ye, Chen, Wang, & Ling (2020) have also proposed a pre-training method for integrating commonsense knowledge into language representation models where they built a commonsense-related multi-choice question answering dataset to be used for pre-training a neural language representation model. Storks, Gao, & Chai (2019) categorized commonsense knowledge and reasoning derived from the NLP community into three areas: benchmarks and tasks, knowledge resources, and learning and inference approaches as shown in the below figure. According Brown, et al. (2020) SOTA for most of them have achieved the close to human accuracy of over 80% but their success is said to be due to larger pre-trained corpora as well as much more parameters, which would be challenging to be followed for most researchers. Huang, He, & Liu (2021) have proposed a framework that converts various commonsense reasoning tasks to a common task, Natural Language Inference and used a pre-trained language model, RoBERTa in solving it.

There is need to revisit many implicitly accepted benchmarking practices such as depending on simplistic metrics such as BLEU and F1-score to keep up with improvements in modelling through taking motivation from real-world applications of language technology and considering the constraints and requirements that such settings pose for the models as recommended by (Ruder, 2021). Another emphasis should be put more rigorously in the assessment of models and rely on multiple metrics and statistical importance testing, contrary to present trends.

## REFERENCES


1. Auer, S., Bizer, C., Kobilarov, G., Lehmann, J., Cyganiak, R., & Ives, Z. (2007). DBpedia: A Nucleus for a Web of Open Data. *The Semantic Web Challenge* (pp. 722-735). Busan, Korea: Springer Berlin Heidelberg.

2. Baud, R. H., Rassinoux, A. M., Lovis, C., Wagner, J., Griesser, V., Michel, P. A., & Scherrer, J. R. (1996). Knowledge sources for Natural Language Processing. *Proceedings of the AMIA Annual Fall Symposium* (pp. 70-74). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2233211/.

3. Bhagavatula, C., Bras, R. L., Malaviya, C., Sakaguchi, K., Holtzman, A., Rashkin, H., . . . Choi, Y. (2020). Abductive commonsense reasoning. *8th International Conference on Learning Representations, ICLR* (pp. 26-30). Addis Ababa: OpenReview.net.

4. Bollacker, K., Evans, C., Paritosh, P., Sturge, T., & Taylor, J. (2008). Freebase: A Collaboratively Created Graph Database for Structuring Human Knowledge. *The 2008 ACM SIGMOD International Conference on Management of Data* (pp. 1247–1250). NY, USA: SIGMOD .

5. Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., . . . Child, R. (2020). Language models are few-shot learners. In Advances in Neural Information Processing Systems. *33: Annual Conference on Neural Information Processing Systems 2020.* Virtual: NeurIPS 2020.

6. Cambria, E., Speer, R., Havasi, C., & & Hussain, A. (2010). SenticNet: A Publicly Available Semantic Resource for Opinion Mining. *AAAI Fall Symposium on Commonsense Knowledge.* Menlo Park, CA, USA: AAAI Press.

7. Chklovski, T. (2003). Learner: A System for Acquiring Commonsense Knowledge by Analogy. *The 2nd International Conference on Knowledge Capture (K-CAP '03), K-CAP '03* (pp. 4-12). New York, NY, USA. : ACM.

8. Commonsenseknowledge. (n.d.). *http://commonsensereasoning.org*. Retrieved December 04, 2021, from www.commonsensereasoning.org: http://commonsensereasoning.org/

9. Davis, E., & Marcus, G. (2015). reasoning and commonsense knowledge in artificial Commonsense intelligence. *Commun. ACM*, 92–103.

10. Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2019). Bert: Pre-training of deep bidirectional transformers for language understanding. *In NAACL-HLT*.

11. Gehrmann, S., Adewumi, T., Aggarwal, K., Sasanka, P., Ammanamanchi, Anuoluwapo, A., . . . Emezue, C. (2021). *The GEM Benchmark: Natural Language Generation, its Evaluation and Metrics.* New York: Amelia R&D.

12. Gupta, V. (2014). A Survey of Natural Language Processing Techniques. *International Journal of Computer Science & Engineering Technology (IJCSET), 05*(01).

13. Huang, C., He, W., & Liu, Y. (2021). Improving Unsupervised Commonsense Reasoning Using Knowledge-Enabled Natural Language Inference. *Findings of the Association for Computational Linguistics*, 4875-4885.

14. Lenat, D. B., & Guha, R. V. (1989). *Building Large Knowledge-Based Systems; Representation and Inference in the Cyc Project.* Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

15. Li, Z., Ding, X., & Liu, T. (2019). Story ending prediction by transferable BERT. *Twenty-Eighth International Joint Conference on Artificial Intelligence, IJCAI* (pp. 1800-1806). Macao China: ijcai.org.

16. Liu, H., & Singh, P. (2004). ConceptNet — A Practical Commonsense Reasoning Tool-Kit. *BT Technology Journal*, 211-226.

17. Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M. S., Chen, D., . . . Stoyanov, V. (2019). Roberta: A robustly optimized bert pretraining approach.

18. Lourie, N., Bras, R. L., Bhagavatula, C., & Choi, Y. (2021). *Rainbow: A Commonsense Reasoning Benchmark*. Retrieved 12 06, 2021, from www.allenai.org: https://allenai.org/data/rainbow

**Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 30-37 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)**

# ИГРОМАНИЯ КАК ФАКТОР НАРУШЕНИЯ РАБОТНИКАМИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ЛИЧНОЙ И ВЕДОМСТВЕННОЙ КИБЕРБЕЗОПАСНОСТИ
# GAMBLING AS A FACTOR OF VIOLATION OF PERSONAL AND DEPARTMENTAL CYBER SECURITY BY EMPLOYEES OF CRITICAL INFRASTRUCTURE FACILITIES

**д.т.н., профессор Хлапонин Юрий Иванович, Киевский национальной университет строительства и архитектуры, г. Киев, Украина**
**Doctor of Technical Sciences, Professor Yuri Khlaponin, Kiev National University of Civil Engineering and Architecture, Kiev, Ukraine**
**к.т.н., Лукянчук Юрий Анатолиевич, Луцкий национальный технический университет, г. Луцк, Украина**
**Candidate of Engineering Sciences, Yuri Lukyanchuk, Lutsk National Technical University, Lutsk, Ukraine**
**к.т.н., Козубцова Леся Михайловна, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина**
**Candidate of Engineering Sciences, Lesya Kozbtsova, Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine**
**д.п.н., профессор Козубцов Игорь Николаевич, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина**
**Doctor of Pedagogical Sciences, Professor, Igor Kozubtsov, Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine**

**АННОТАЦИЯ.** Актуальность темы исследований обусловлено необходимостью обеспечения стабильностью функционирования объектов критической информационной инфраструктуры в условиях постоянно возрастающей уязвимости. Для этого следует проводить работы с повышения уровня киберосведомленности всех участников киберпространства. Основные аспекты работы. В работе изучены истоки возникновения проблемы личностной и ведомственной кибербезопасности, источником которой является распространенная игровая зависимости человека. Научная новизна. Подтверждено предположение, что игромания с использованием терминалов сотовой связи и геолокаци является одним из факторов, которые вызывают нарушения личной и ведомственной кибербезопасности.
**КЛЮЧЕВЫЕ СЛОВА**: *игромания, геолокация, игры, кибербезопасность, объект критической информационной инфраструктуры*.

**ABSTRACT.** The relevance of the research topic is due to the need to ensure the stability of the functioning of critical information infrastructure facilities in conditions of constantly increasing vulnerability. To do this, work should be carried out to increase the level of cyber awareness of all participants in cyberspace. The main aspects of the work. The paper examines the origins of the problem of personal and departmental cybersecurity, the source of which is the widespread gambling addiction of a person. Scientific novelty. The assumption is confirmed that gambling using cellular terminals and geolocation is one of the factors that cause violations of personal and departmental cybersecurity.
**KEYWORDS**: *gambling addiction, geolocation, games, cybersecurity, critical information infrastructure object*.

## ВВЕДЕНИЕ

Исследования [1] позволили установить, что люди ежедневно проводят более четырех часов со своими смартфонами. Согласно отчету comScore 2017 Cross Platform Future in Focus, средний взрослый американец (18+) ежедневно проводит за своим смартфоном 2 часа 51 минуту. Это примерно 86 часов в месяц. В других странах пользователи смартфонов проводили, в среднем по крайней мере час в день, приклеенные к своим устройствам – и часто гораздо дольше [2]. Эти цифры варьируются в разных странах, но в среднем человек уделяет своим гаджетам очень много внимания и порой доверяем им частную информацию (рис. 1) [3].

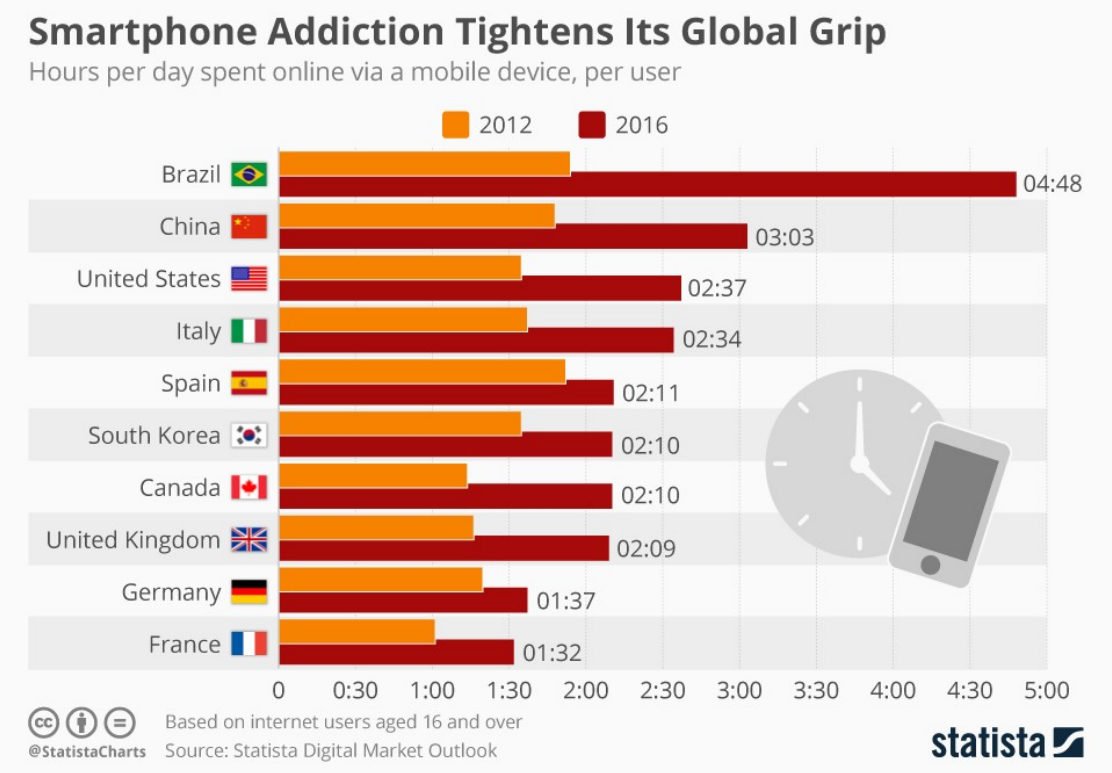



Рисунок 1 – Зависимость людей в разных странах от средств сотовой связи (смартфонов)

Следует конституировать тот факт, что смартфоны становятся все более мощными и способными делать больше вещей, и как следствие заложен подсознательно смысл, чтобы люди тратили на них все больше личного времени. Несмотря на возрастающую опасности от искусственного интеллекта, дополненной реальности и другими футуристическими технологиями, многие люди не задумываются над проблемою, все еще живут в мире смартфонов. Смартфонная зависимость, которую иногда называют «номофобиєю» (страх остаться без мобильного телефона) часто вызывается проблемой чрезмерного использования Интернета или расстройством интернет-зависимости. Сам телефон или планшет не создает у человека ощущение принуждения. Зависимость все чаще возникает от игры, игровой программы, онлайн-игр, с которыми он связывает пользователя [4]. В самих смартфонах нет ничего особенного, что вызывало б зависимость, но настоящей движущей силой нашей привязанности к этим устройствам возникает вследствие гиперсоциальной среды в которой пребывает человек в современном мире [5].

Игромания – болезнь XXI века, что предполагает неуправляемый чрезмерное влечение к азартным играм. Игра также является средством психологической разгрузки после длительного обучения. Однако это средство зачастую превращается в самоцель, и тогда развивается игровая зависимость. Зависимость от игр исчерпывающее описана Американской психиатрической ассоциации в Руководстве по диагностике и статистике психических расстройств (Diagnostic and Statistical Manual of Mental Disorders DSM-5), которое используется специалистами для диагностики психических расстройств и психического здоровья человека. На момент опубликования руководства DSM-5 в 2013 году не было достаточных доказательств, чтобы определить, является ли это состояние человека уникальным психическим расстройством. Однако в разделе интернет-игр значится игромания как расстройство, которое подлежит дальнейшим медицинским исследованием [6].

Опубликованные исследование [7] свидетельствуют, что по статистике, около 75 процентов игроков – это школьники и студенты (рис. 2). И это не может настораживать.

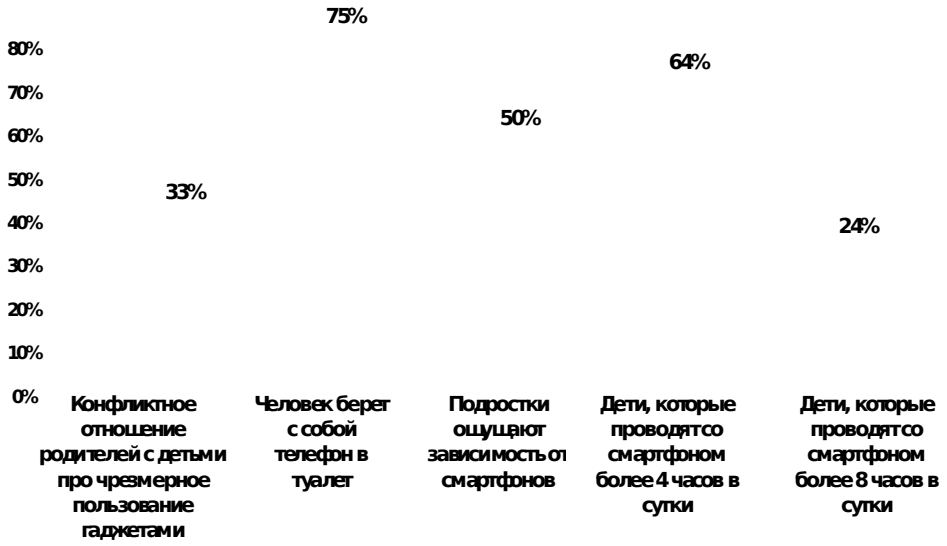



Рисунок 2 – Зависимость детей от средств сотовой связи (смартфонов)

**АНАЛИЗ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ**

Работа [8] указывает на то, что компьютерные игры все чаще становятся современными сказками. Опасность которых заключается в массовом эмоциональном, психологическом восприятии игры. Это один ракурс проблемы подробно изучено следующих научных работах и в результате формируется целостная картина мира.

В работе [9] установлено влияние компьютерных игр, как нового фактора культуры на становление личности. При чрезмерном увлечении ими может привести человека к агрессивному проявлению [10]. В дальнейших исследованиях систематизированы симптомы компьютерной зависимости [11]. Что примечательно, они коррелируют с результатами исследований с коллегами [4]. На основании обзора особенностей ценностных ориентаций пользователей компьютерной техники автор исследования [12] приходит к выводу, что распространение новых компьютерных технологий приводит к появлению новых слоев реальности – виртуальной реальности. Виртуальное пространство – это новый тип культурного пространства, что характеризуется свободой творчества, иллюзорности, динамичностью, возможностью ускорять или поворачивать время [13]. На основе этой виртуальной реальности появились новая субкультура – субкультура – геймеров. Основные участники субкультуры геймеров – подростки и студенты. Это тот возраст, доминантой которого является выбор субъективно важных ценностей, построение системы ценностей. Создана на базе ценностей система принципов превращается в дальнейшем в жизненную стратегию. Поэтому особенно важно изучать систему ценностных ориентаций именно молодые – игроков в компьютерные игры.

В работе [14] предложено социально-педагогическую профилактику игровой зависимости. Описаны методы и формы профилактической деятельности социального педагога по предупреждению игровой зависимости. Изучение указанного опыта социально-педагогической профилактики игровой зависимости является интересным с позиции проверки гипотезы о возможности применения аналогичной профилактики работниками объектов критической инфраструктуры. Возможно потребует корректировки социально-педагогической профилактики, осведомленности.

Результаты исследования Национальной ассоциации США по проблемам азартных игр свидетельствуют, что среднестатистический житель любой страны мира может стать уголовником с достоверностью 6%, наркоманом – 32%, алкоголиком – 34%, игроманом – 48% [15].

О наличии проблемы игровой зависимости от игры в Pokémon отмечено в исследовании [16]. Особого внимания приобретает проблема игромании среди военнослужащих и работников объектов критической инфраструктуры. К сожалению, статистических данных о игровой зависимости военнослужащих и работников объектов критической инфраструктуры в

открытом доступе отсутствуют, поэтому об ее уровне можно судить лишь косвенно, например, из открытой публикации [17]. Следует отметить, что с появлением игр устанавливаемые на терминалы сотовой связи и дополнительной реальности в киберпространстве приобрело развитие игромании. Игромания среди работников объектов критической инфраструктуры превратилась в потенциальную опасность, связанную с утечкой конфиденциальной информации относительно персональных данных «игроков», места их постоянной дислокации и многое другое об объектах критической инфраструктуре. О проблеме говорится и в средствах массовой информации со ссылкой на Министерство обороны США, которое запретило своим военнослужащим пользоваться функцией геолокации в приложениях и на любых устройствах в местах проведения военных операций [18].

**Постановка задачи и связь ее с важными научными заданиями.** За результатами анализа работ [8 – 18] установлено, что из общей картины упущено внимания изученности решения проблемы предотвращения, возможной опасности личной и ведомственной кибербезопасности, которая таится в геолокационных играх. Значимость проблемы усиливается в следствии увеличения числа зависимости работников объектов критической инфраструктуры от игромании на средствах сотовой связи. Поэтому, учитывая потенциальную опасность игромании среди работников объектов критической инфраструктуры, считаем за необходимость, проведения данного исследования по изучению феномена психолого-педагогической проблемы, которая напрямую или косвенно влияет на личную и ведомственную кибербезопасности.

**ЦЕЛЬ СТАТЬИ**

Изучение проблемы личностной и ведомственной кибербезопасности в следствии распространения игровой зависимости работников объектов критической инфраструктуры.

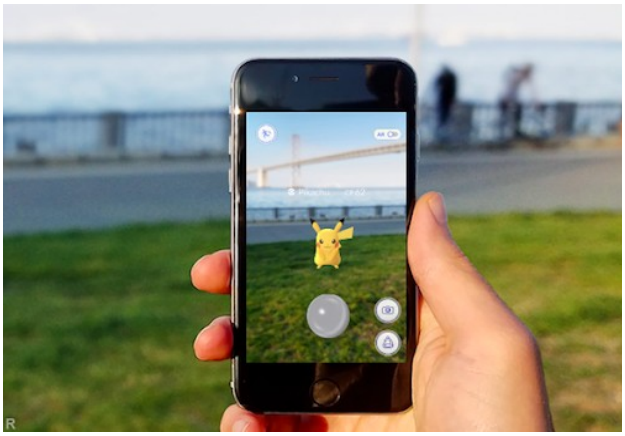
**ОСНОВНОЙ РЕЗУЛЬТАТ ИССЛЕДОВАНИЯ**

В настоящей работе рассмотрим проблему кибербезопасности возникшую вследствие игромании с использованием гелогационных игр дополненной реальностью и привлекательностью. Дополненная реальность – это не только Google Glass и виртуальные персонажи, танцующие на реальных объектах вокруг нас. В более широком смысле дополненная реальность – это любая проекция виртуальных объектов на реальный мир. Популярная игра Pokémon Go, как и ее предшественник Ingress, является приложением, основанным на технологии дополненной реальности. Создатели игры нацелили своих игроков на поиск виртуальных покемонов в реальном мире. А чтобы все это работало, смартфон должен непрерывно проверять свое местоположение и синхронизировать его с картой.

Навязывание работникам объектов критической инфраструктуры геолокационных игр имеет очень опасные последствия, которые скрыты под ярким психологическим удовольствием. Во время игры человек погружается как бы в настоящие спортивные соревнования. Это погружение нацелено на вскрытие системы личностной и ведомственной кибербезопасности, и утечки геоинформационной информации из расположения объектов критической инфраструктуры их натуральный вид. Для этого условный противник использует целую систему компьютерных и игровых приложений, устанавливаемых на средства сотовой связи. Прежде всего, данные игры адресованы и рассчитаны на игроманов, которые не представляют тратить свое свободное время вне игры. Онлайн игры расширяют возможность утечки геоинформационной информации из расположения объектов критической инфраструктуры по сравнению с играми установленных для автономной игры, то есть без выхода в сеть Интернет.

Рассмотрим несколько отдельных наиболее опасных образцов геолокационных игр, интерфейс которых изображен на рис. 1.

Игра №1 «сфотографируй покемона» (рис. 3, а). Девиз игры «сфотографируй покемона – станешь чемпионом». Азарт игры настолько воодушевляет игрока, что тот и не задумываясь фотографируют все объекты критической инфраструктуры. Далее эти фотографии из телефона с лёгкостью автоматически отправляются на вражеские серверы.



а)

б)


в)

г)

Рисунок 3 – Пример отдельных образцов геолокационных игр

Игра №2 «сфотографируй здание, улицу, позицию или другой объект» (рис. 3, б). Мотивационный лозунгом «сфотографируй здание, улицу, позицию и другой объект» – стань первым кто создал интересную карту. Аналогичным образом, приложение автоматически направляет на неизвестный сервер фотографии объектом критической инфраструктуры, которые игроманы с азартом фотографируют.

Игра №3 «Ingress» – Google сделал шаги в направление к популяризации гєолокационных игр. Считается, что «Ingress» – это не игра, а замаскированный сборник «троп» – путей, по которым перемещаются люди ездят, созданный для навигационного графа Google maps (рис. 3, в). Приложение Ingress the Game было запущено разработчиком Niantic Labs в ноябре 2012 года. Изначально доступ к игре предоставлялся по приглашениям. Приобрёл широкую зависимости у игроков создатели с октября 2013 года доступ к игре сделали открытым. В июле 2015 г. игра насчитывала 12 млн пользователей [19]. Задача игрока – в режиме реального времени передвигаться по городу, подходить к локациям, которые на карте города внутри приложения-сканера отмечены как «порталы», захватывать их, перекрашивая в цвет своей команды, получая очки и артефакты.

Игра №4 «Shadow Cities» мобильная онлайн игра про захват реальных городов. Сюжет игры, следующий. В мире идет конфликт двух сторон, постоянно поддерживаемый внутренне игровыми событиями, турнирами и эпическими задачами. Очень стильный визуально проект, первым из всех геолокационных игор сделал хорошую трехмерную карту (на основе OpenStreetMap) (рис. 3, д).

Особую опасность имеют гєолокационные игры типа «Pokémon Go» от объединения компаний Pokémon Company, Google и Nintendo. Опасность заключается в массовом эмоциональном, психологическом восприятии игры и потенциальному утечки информации относительно окружения игроков, местности и объектов.

Общая концепция геолокационных игр предусматривает применением

геоинформационных данных пользователя и преследует следующую цель:

1. Создание у человека зависимости от «игромании» на основе как бы естественного спортивного соревнования;

2. Сокрыть замысла сбора конфиденциальной информации (фотографий) под поиск скрытых, например, Pokémon, которые отображаются на главном экране средства сотовой связи;

3. Формирование целостной геолокационной картины пространства, путем сбора на первый взгляд чисто случайной открытой информации (фотографий);

4. Формирование целостной геолокационной картины пространства объектов критической инфраструктуры объектов путем привлечения игроманов к сбору такой конфиденциальной информации (фотографий).

Разработчики игры все больше стремятся создавать альтернативу реальности, подобную проблему компьютерных игр [20].

Ввиду опасности геолокации Министерство обороны США запретило своим военнослужащим пользоваться функцией геолокации в приложениях и на любых устройствах в местах проведения военных операций [18]. Поскольку геолокация может раскрыть не только личную информацию, местонахождение, повседневную активность и численность военных, а также потенциально создать непреднамеренные риски для безопасности и повысить опасность для объединенных сил и миссий. В перечень потенциально опасных программ и устройств, руководство Пентагона, добавили, фитнес-трекеры, смартфоны, планшеты и смарт-часы.

Учитывая бесперспективность существующих мер по борьбе с игроманией среди военнослужащих по данным источника [21] в Министерстве обороны США разработаны указания по безопасному охоты на покемонов среди которых рекомендовано:

загружать только официальную версию Pokemon GO от разработчика (Niantic), с Google Play Store или Apple App Store;

для воспроизведения применять GPS и соединение для передачи данных (Wi-Fi или сотовой (3G/4G));

избегать игры в тех областях, где запрещено, чтобы пользователя обозначали географическими тегами.

Таким образом, исходя из выше рассмотренного следует рекомендовать включить игроманию с ипользованием геолокации и терминалов сотовой связи в группу факторов риска, которые вызывают нарушения как личной, так и ведомственной кибербезопасности.

Для преодоления фактора, необходимо системно подойти к его решению на основе осознания каждым человеком причины и механизма вследствие которого возникает нарушения личной и ведомственной кибербезопасности. Нарушения кибербезопасности возникает в результате действий человеком за концепцией игры, в которую заложен механизм утечки конфиденциальной информации.

Агенты киберугроз чтобы не вызвать срабатывания системы киберзащиты, создают угрозы, которые используют на игровые приложения-трояны. В результате установки игры с помощью приложения-трояна не осознает какой риск несет именно эта игра. После удачной инсталляции (установки) игры на терминалы сотовой связи, в автоматическом или в полуавтоматическом режиме программа делает запрос доступа к фотокамере, карты памяти, фотографий и важное условие ее работоспособности является включение геолокации с доступом к сети Интернет. Есть исключения, когда доступ к сети интернет не требует. Однако при первом же подключении к сети все файлы (активы) автоматически отправляются на сервер. Пользователь всю работу за шпиона сделал собственноручно. По нашему мнению, игромания является частичным механизмом всей великой стратегии игры ее участников в киберпространстве, что приводит к нарушению кибербезопасности (утечки конфиденциальной информации об объектах критической инфраструктуры [22]. Кто на какой стороне противостояния в киберпространстве все зависит от мотивационных портретов их участники [23]. Этот мотивационный портрет необходимо периодически изучать дабы пресечь предпосылки нарушения кибербезопасности [24].

**ВЫВОДЫ**

Таким образом можно сформулировать следующие выводы:

1. Средства сотовой связи представляют наибольшую угрозу в использовании работниками объектов критической инфраструктуры, а именно способствуют слежению и раскрывают местонахождение пользователя. Мобильный телефон дает заинтересованной стороне противнику намного больше возможностей контроля, чем компьютер или ноутбук. На мобильном телефоне труднее изменить операционную систему, исследовать атаки вредоносных программ, удалять нежелательные приложения, помешать посторонним лицам (например, оператору связи) следить за тем, как пользователь использует свое устройство. Более того, производитель телефона может объявить модель устаревшей и перестать обновлять программное обеспечение, в том числе то, которое отвечает за безопасность.

2. Прямой запрет относительно использования работниками объектов критической инфраструктуры как свидетельствует современная мировая практика не является действенной, а наоборот стимулирует к правонарушению. Поэтому требует все большего привлечения внимания к изучению относительно новой психолого-педагогической проблемы современности.

3. Постоянно включена функция определения геолокации – это огромный минус для безопасности и конфиденциальности данных, поэтому ее нужно отключать для безопасности и конфиденциальности данных.

4. Необходимо максимально использовать только те средства связи, в которых не позволяют производителем, помимо голосовой телефонной связи функций, фото- видео-звукозаписи, передачи данных через сеть интернета. Современная концепция производителей можно усложнить выполнение этих требований, навязывания всего и сразу.

**НАУЧНАЯ НОВИЗНА**

Подтверждено предположение, что игромания с использованием терминалов сотовой связи и геолокации является одним из факторов, которые вызывают нарушения личной и ведомственной кибербезопасности.

**ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ НАУЧНЫХ ИССЛЕДОВАНИЙ**

Представленное исследование не исчерпывает всех аспектов обозначенной проблемы. Теоретические и практические результаты, полученные в процессе научного поиска, составляют основу для дальнейшего ее изучения в различных аспектах.

**СПИСОК ЛИТЕРАТУРЫ**


1. How Much Time Do People Spend on Their Mobile Phones in 2017? URL: https://hackernoon.com/how-much-time-do-people-spend-on-their-mobile-phones-in-2017-e5f90a0b10a6.
2. ‘Smartphone addiction’ seems to only be getting stronger. URL: https://www.businessinsider.com/people-spending-more-time-on-smartphones-chart-2017-5.
3. Smartphone Addiction Tightens Its Global Grip. URL: https://www.statista.com/chart/9539/smartphone-addiction-tightens-its-global-grip.
4. Smartphone Addiction. URL: https://www.helpguide.org/articles/addictions/smartphone-addiction.htm#quiz.
5. Smartphone Addiction. URL: https://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time.
6. Ranna Parekh. Internet Gaming. (n.d.). All Rights Retrieved August 2, 2021, from. American Psychiatric Association. URL: https://www.psychiatry.org/patients-families/internet-gaming.
7. Інтернет та гаджетозалежність. Вийтівський опорний заклад загальної середньої освіти. Офіційний веб-сайт. URL: https://wishkola.org.ua/internet-zal.
8. Чайка Г.В. Компьютерные игры как современные сказки // Практична психологія та соціальна робота. 2009. № 4. С. 65–67.
9. Чайка Г.В. Вплив комп'ютерних ігор як нового чинника культури на становлення особистості // Актуальні проблеми психології. 2006. Т. 3. Вип. 3. С. 218–296.
10. Чайка Г.В. Агресивні прояви комп’ютерних гравців // Проблеми загальної та педагогічної психології: зб. наук. пр. Ін-ту психології ім. Г.С.Костюка АПН

України. К.: Гнозіс, 2008. Т. 8. Ч. 3. С. 481–489

11. Чайка Г.В. Симптоми комп’ютерної залежності // Практична психологія та соціальна робота. 2009. № 10. С. 52–55.
12. Чайка Г.В. Огляд особливостей ціннісних орієнтацій користувачів комп’ютерної техніки // Проблеми загальної та педагогічної психології. Зб. наук. праць Ін-ту психології ім. Г.С. Костюка. 2013. №(15). С. 302–330.
13. 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.
14. Дідик Н.М. Соціально-педагогічна профілактика ігрової залежності // Молодий вчений. 2015. №2(17). С.226–229.
15. Ігрова залежність (гемблінг). Напрямки профілактики. Сумський обласний наркологічний диспансер. https://narkosumy.lic.org.ua/statti/igrova-zalezhnist-gembling-napryamky-profilaktyky.
16. Frith J. The digital "lure": Small businesses and Pokémon Go // Mobile Media and Communication. 2017. Vol. 5. № 1. Pp. 51–54.
17. Андреев Д. Игромания цвета хаки // Красная звезда. 2006. http://old.redstar.ru/2006/11/21_11/2_03.html.
18. В США запретили военным пользоваться приложениями с геолокацией. URL: https://www.dw.com/ru/в-сша-запретили-военным-пользоваться-приложениями-с-геолокацией/a-44978170.
19. Suckley M. Why Google's Niantic Labs is taking Ingress' success and scaling up to an open platform // Pocketgamer. 27 July 2015. URL: http://www.pocketgamer.biz/news/61650/niantic-labs-platform-play.
20. Перепелиця А.В. Проблема комп’ютерних ігор, як альтернатива реальності // Актуальні проблеми психології: Збірник наукових праць Інституту психології імені Г.С. Костюка НАПН України. Том XIV: Методологія і теорія психології. Випуск 1. Київ–Ніжин. Видавець «ПП Лисенко М.М.». 2018. С. 265–279.
21. Defense Department Issues Opsec Guidelines For Safe And Secure Pokemon Hunting. URL: https://www.techdirt.com/articles/20160718/02171135002/defense-department-issues-opsec-guidelines-safe-secure-pokemon-hunting.shtml.
22. Козубцов І.М., Козубцова Л.М Стратегія гри в кібернетичному просторі // Матеріали Міжнародної науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» (Київ, 17–20 листопада 2015 р.). Київ. Державний університет телекомунікацій, 2015. Том ІІІ Розвиток інформаційних технологій С. 52–54.
23. Козубцов І.М. Про мотиваційний портрет учасники кібернетичного протистояння // Актуальні проблеми розвитку науки і техніки: Матеріали першої міжнародної науково-технічної конференції. Збірник тез. К.: ДУТ, 2015. С. 208–211.
24. Козубцов І.М., Козубцова Л.М., Живило Є.О., Куцаєв В.В. Про необхідність дослідження мотиваційної характеристики військовослужбовців при допуску їх до кібернетичного протистояння // Науково-практична конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» (Харків, 17–18 березня 2016 р.). Харків: Національна академія Національної гвардії України, 2016. С.35–36.

Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 38-47 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

# CONCEPTS, APPLICATIONS, AND CHALLENGES OF THE INTERNET OF THINGS

**Nauryzbek Amangeldiyev, Master student, Mechanical engineering faculty, Hungarian University of Agriculture and Life Sciences.**
**Patrick Siegfried, Professor, Doctor, Doctor, MBA, Logistics & Supply Chain Management, ISM International School of Management GmbH – Gemeinnützige Gesellschaft, Guest Professor at the Hungarian University of Agriculture and Life Sciences.**

**ABSTRACT:**The main aim of the study is to give the reader the basic meaning of an “Internet of Things” itself, evaluate its main concepts, types, trends, and areas of application, as well as challenges.
The study is a basic and fresh literature review from general sources and researches on the topic that has been done recently by the scientific community. Qualitative and quantitative methods of data collecting have been used. As a result, this paper can offer new interpretations, theoretical approaches, or other ideas. Mendeley referencing application was used to cite and give credits to the authors of a raw material used in this study.
This term paper will give an excellent understanding to other researchers who are trying to build basic concepts within the topic, or to those who wish to begin their researches on “IoT” furthermore and will provide effective and accumulation knowledge. Also, can be useful as a raw material to the introductory courses regarding “IoT”.
**KEYWORDS** – *IoT; Internet of things; IoT security; IoT vision; Internet of nano-Things; IoT architecture; Layers of IoT; Smart Planet; Smart Home; Smart Transport; Smart Healthcare; Smart Transportation; Smart City; Smart Energy Grid; Internet of People; IoP; IoE; Internet of Everything*

## INTRODUCTION

The Internet of Things – (IoT) is a new concept in which the Internet is evolving from the unification of computers and people to the unification of (smart) objects/things (Gubbi et al., 2013). With the continuous advancement of Internet of Things technologies, potential innovations are "crashing down" on us, growing to a global computing network where everything and everyone will be connected via the Internet. IoT is constantly evolving and is a hot topic for research at the moment. The usual form of the Internet is moving into its modified and integrated version. The number of devices using Internet services is growing every day and connecting them all with wires or wireless technology will give us a powerful source of information at our fingertips. The concept of empowering interactions between smart machines is cutting-edge technology. But the technologies that make up the Internet of Things are nothing new.

IoT is an approach to connecting information received from various sources on any virtual platform or existing Internet infrastructure. The concept “Internet of Things” appeared in 1982, when a modified soda machine was connected to the Internet and was able to report the presence of drinks in it and their temperature. Later, in 1991, Mark Weiser was the first to give a modern assessment of the Internet of Things.

Moreover, in 1999, Bill Joy gave a hint about the connection between devices in his Internet taxonomy (Said & Masud, 2013). In the same year, Kevin Ashton proposed the term "Internet of Things" for connected devices. The basic idea of IoT is to provide the possibility of autonomous exchange of useful information. These devices are equipped with the latest technology such as radio frequency identification (RFID) and wireless sensor networks (WSN) and in the ability to get the opportunity to make independent decisions depending on which automated execution is being performed.

## CONCEPT

In 2005, the International Telecommunications Union (ITU), heralds an era of pervasive networks, the main hallmark of which is connectivity networks among themselves. The main concept of the Internet of Things is the

environment in which things can obey control, and data about things can be processed to perform the desired task by training the devices (Alam et al., 2020). Practical implementation of IoT is well demonstrated in Twine, compact and low-power hardware that works melting with real-time network software and allowing make this concept a reality (Arndt, 2017).

However, different people and organizations have differing concepts of the Internet of Things. In connection with the rapid development of packet-switched networks, and above all the Internet, in the early 2000s, the global telecommunications community first developed, and then it began to implement a new paradigm for the development of communications – next-

generation networks (NGN). NGN technologies have already passed the evolutionary path of development from flexible switches (Softswitch) to multimedia communication subsystems IMS (IP Multimedia Subsystem) and long-term wireless networks evolution of LTE. It has always been assumed that the main users of NGN networks will be people and, therefore, the maximum number of subscribers in such networks will always be limited by the population of planet Earth (Singh et al., 2020). However, in recent years, RFID (Radio Frequency Identification) methods, WSN (Wireless Sensor Network), short-range communications NFC (Near Field Communication) and M2M (Machine-to-Machine) communications have received significant development. integrating with the Internet, they make it possible to provide a simple connection between various technical devices ("things"), the number of which can be huge.

Thus, there is an evolutionary transition from the "Internet of people" to the "Internet of things" (Miranda et al., 2015). In the general case, the Internet of Things is understood as a set of various devices, sensors, devices connected into a network through any available communication channels using various protocols of interaction with each other and a single protocol for accessing the global network. The Internet is currently used in the role of the global network for the Internet of Things. The common protocol is IP.

## ARCHITECTURE

Cisco believes that in 2020 there will be more than 50 billion connected objects with a population of 7 billion people (Cisco, 2015). The existing Internet architecture with its TCP/IP protocols cannot cope with such a large network as IoT. Therefore, there is a need for a new open architecture that can send reports on the safety, quality, and class of data transmission services with quality of services (QoS) provided, while at the same time supporting existing network applications using open protocols. The Internet of Things cannot be implemented without proper security guarantees. Therefore, data protection and privacy are key tasks for IoT.

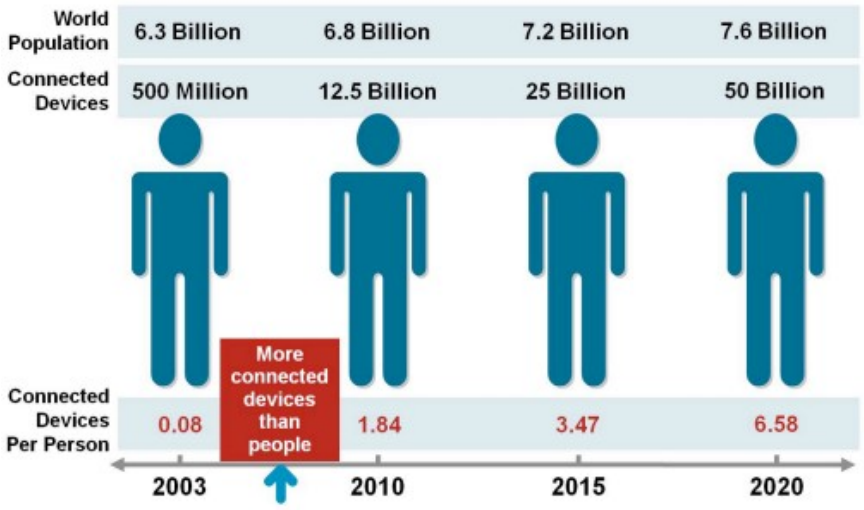



FIGURE 1
TIMELINE OF CHANGES IN THE NUMBER OF PEOPLE AND OBJECTS, CONNECTED TO THE INTERNET (Evans, 2011)

For further development, IoT offers several multi-level architectures. The Internet of Things conceptually belongs to the next generation of networks, so its architecture is in many ways similar to the well-known four-layer of NGN architecture (Singh et al., 2020). IoT consists of a set of various information and communication technologies that ensure the functioning of the Internet of Things, and its architecture shows how these technologies are connected. The architecture includes four functional layers (Figure 2) described below.

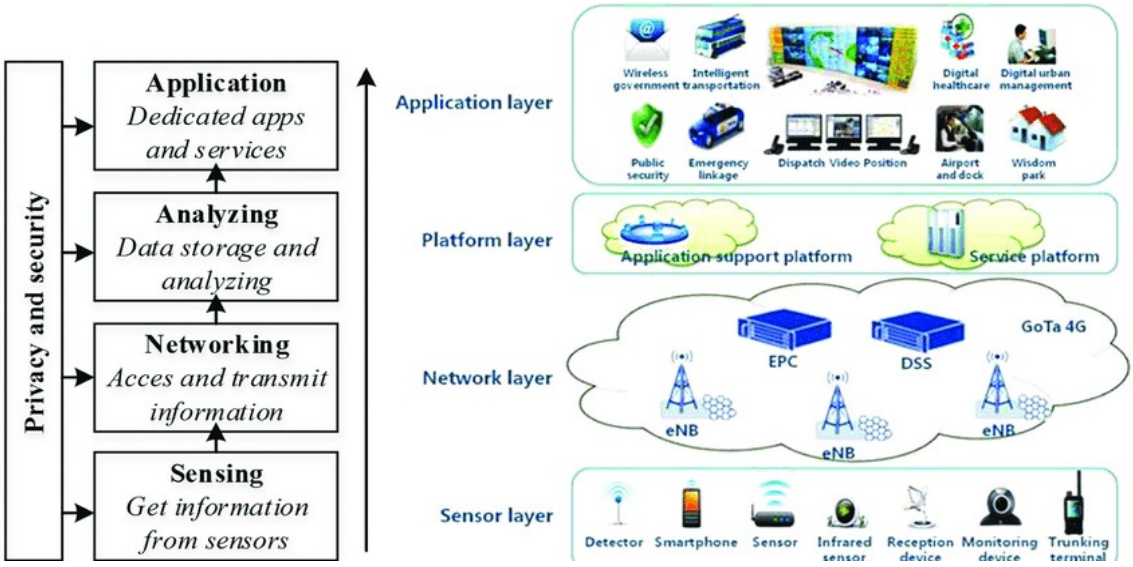



FIGURE 2
FOUR FUNCTIONAL LAYERS OF IOT (RAD ET AL., 2015)

**The level of sensors and sensor networks.** The lowest level of the IoT architecture consists of smart objects integrated with sensors (sensors). Sensors realize the connection of the physical and virtual (digital) worlds, providing the collection and processing of information in real-time. Miniaturization, which led to a reduction in the physical size of hardware sensors, made it possible to integrate them directly into objects of the physical world. There are various types of sensors for specific purposes, for example, for measuring temperature, pressure, speed, location, etc. Sensors can have small memory, making it possible to record several measurement results. The sensor can measure the physical parameters of the monitored object/phenomenon and convert them into a signal that can be received by the corresponding device. Sensors are classified according to their purpose, for example, environmental sensors, body sensors, home appliance sensors, vehicle sensors, etc. (Ratnaparkhi et al., 2020). Most sensors require a connection to a sensor aggregator (gateway), which can be implemented using a Local Area Network (LAN) such as Ethernet and Wi-Fi or a Personal Area Network (PAN) such as ZigBee, Bluetooth, and Ultra-Wide Band Wireless (UWB). For sensors that do not require a connection to the aggregator, their connection to servers/applications can be provided using wide-area wireless WANs such as GSM, GPRS and LTE. Sensors, which are characterized by low power consumption and low data rates, form the well-known Wireless Sensor Networks (WSN). WSNs are gaining in popularity as they can contain many more battery-enabled sensors and cover large areas.

**Gateway and network layer.** The large amount of data generated at the first layer of the IoT by multiple miniature sensors requires a reliable and high-performance wired or wireless network infrastructure as a transport medium. Existing networks communications using different protocols can be used to support M2M machine-to-machine communications and their applications. To implement a wide range of services and applications in the IoT, it is necessary to ensure that many networks of different technologies and access protocols work together in a heterogeneous configuration. These networks must provide the required values of the quality of information transmission, and above all in terms of delay, bandwidth, and security. This level consists of converged network infrastructure, which is created by integrating heterogeneous networks into a single network platform. Converged Abstract Network Layer in IoT allows multiple users to share resources on the same network independently and jointly through appropriate gateways without compromising privacy, security, or performance (Divarci & Urhan, 2018).

**Service level (Analyzing).** The service level contains a set of information services designed to automate technological and business operations in the IoT: support for operational and business activities (OSS / BSS, Operation Support System / Business Support System), various analytical processing of information (statistical, data mining and text mining, predictive analytics, etc.), data storage, information security, business rule management (BRM), business process management (BPM), etc.

**Application layer.** At the fourth level of the IoT architecture, there are various types of applications for the respective industrial sectors and spheres of activity (energy, transport, trade, medicine, education, etc.). Applications can

be "vertical" when they are specific to a particular industry, as well as "horizontal" (eg, fleet management, asset tracking, etc.) that can be used in different sectors of the economy.

## INTERNET OF "NANO" THINGS

Nanotechnology has led to the development of miniature devices, the sizes of which range from one to several hundred nanometers. At this level, nano-machines consist of nano components and represent themselves as separate functional units capable of performing simple measuring, regulating, or controlling operations. Coordination and information exchange between nano-devices allow the formation of so-called nano-networks. In the case of connecting nano-devices to existing networks and a new network paradigm is emerging on the Internet, called the "Internet of Nano-things". The interaction of nano-devices with existing networks and the Internet require the development of new network architectures (Nayyar et al., 2017). Figure 3 shows the architecture of the Internet of nano-things in two different implementations – a network on the human body for monitoring health indicators and sending them to a medical centre, and a modern office network connecting many different devices.

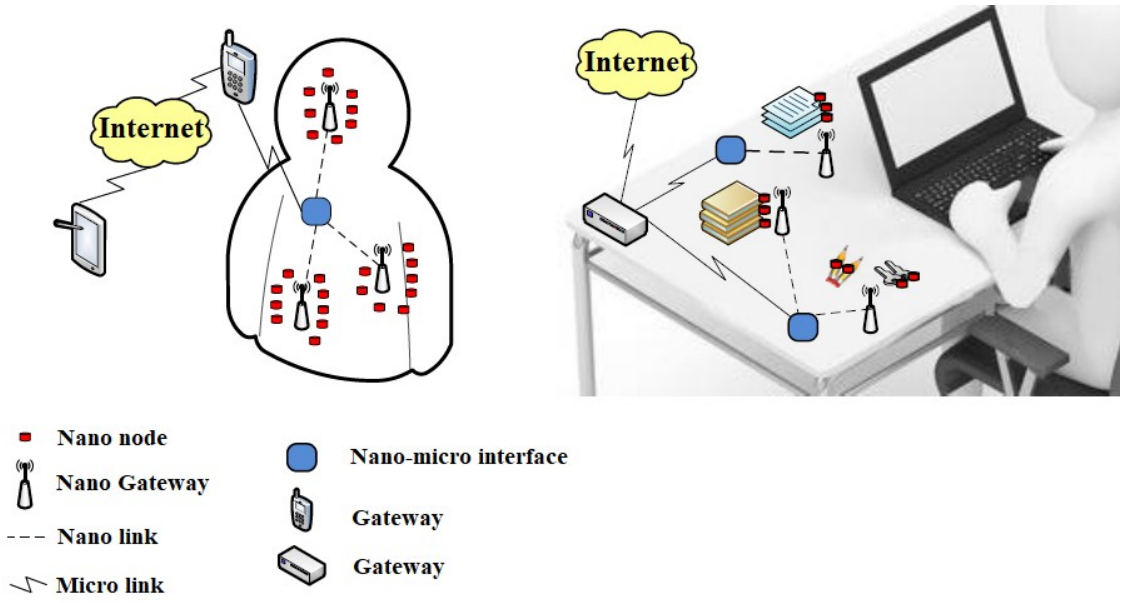



FIGURE 3
INTERNET OF NANO-THINGS EXAMPLE ARCHITECTURE

The network on the human body consists of nano-sensors and nano actuators that can send information through an external gateway to a medical facility. In this case, at the nano-level, molecules, proteins, DNA, organic substances, and basic components of cells. Thus, biological nano-sensors and nano-actuators provide an interface between the human biological environment and electronic nano-devices that can be used in a new network paradigm - the Internet of Nano-Things. The intraoffice network connects many even the smallest devices with nano-transceivers that provide an Internet connection. As a result of this interaction, the user can track the status and location of things, without any effort and time. When developing new miniature devices, the most advanced energy-saving technologies can be used to obtain mechanical, electromagnetic, and other types of energy from the environment.

Regardless of the field of application, the main components of the architecture of the Internet of nano-things are:

1. Nano-nodes are miniature and simplest nano-devices. They allow us to perform the simplest calculations, have limited memory and a limited signal transmission range. Examples of nano-nodes can be biological nano-sensors on or inside the human body or nano-devices embedded in everyday things around us – books, watches, keys, etc.
2. Nano-gateways - these nano-devices have relatively high performance compared to nano-nodes and perform the function of collecting information from nano-nodes. In addition, nano-gateways can control the behaviour of nano-nodes by executing simple commands (on/off, sleep mode, transmit data, etc.).

3. Nano-micro interfaces are devices that collect information from nano-gateways and transmit it to external networks. These devices include both nano-communication technologies and traditional technologies for transmitting information to existing networks.
4. Gateway – this device monitors the entire nano-network via the Internet. For example, in the case of a network with sensors on the human body, this function can be performed by a mobile phone that transmits information about the necessary indicators to a medical institution.

### DIRECTIONS OF THE PRACTICAL APPLICATION OF IOT

Based on the Internet of Things, all kinds of "smart" applications can be implemented in various spheres of human activity and life (Figure 4):

- "Smart Planet" - a person can literally "keep his finger on the pulse" of the planet: respond promptly to omissions in household planning, pollution, and other environmental problems, and therefore effectively manage non-renewable resources. Individual large-scale projects in the direction of creating a "smart" planet, a kind of "Intranet of things", have been developing vigorously in recent years. Thus, the US National Aeronautics and Space Administration (NASA), with the support of Cisco, is creating a system for global data collection about the Earth - the "Skin of the Planet" (Planetary skin) (NASA, Cisco Partnering for Climate Change Monitoring Platform, n.d.). It is planned to develop an online platform for collecting and analyzing data on the environmental situation coming from space, air, sea, and ground sensors scattered throughout our planet. This data will be made available to the general public, Governments, and commercial organizations. They will make it possible to measure, report and verify environmental data in near real-time, to recognize global climate changes promptly and adapt to them (NASA, Cisco Partnership on Climate Change Monitoring Platform | The Network, n.d.). The development of the platform began with a series of pilot projects, including the Rainforest Skin project (lit. - "the skin of the tropical jungle"), during which the process of destruction of tropical forests on a global scale will be investigated. Individual large-scale projects in the direction of creating a "smart" planet, a kind of "Intranet of things", have been developing vigorously in recent years. Thus, the US National Aeronautics and Space Administration (NASA), with the support of Cisco, is creating a system for global data collection about the Earth - the "Skin of the Planet" (Planetary skin) (*How NASA, Cisco, And A Tricked-Out Planetary Skin Could Make The World*, n.d.). It is planned to develop an online platform for collecting and analyzing data on the environmental situation coming from space, air, sea, and ground sensors scattered throughout our planet. This data will be made available to the general public, Governments, and commercial organizations. They will make it possible to measure, report and verify environmental data in near real-time, to recognize global climate changes promptly and adapt to them. The development of the platform began with a series of pilot projects, including the Rainforest Skin project (lit. - "the skin of the tropical jungle"), during which the process of destruction of tropical forests on a global scale will be investigated (Juan Carlos Castilla-Rubio & Simon Willis, 2009).
- "Smart City – urban infrastructure and related municipal services, such as education, healthcare, public safety, housing, and communal services, will become more connected and efficient. In recent years, information systems have been intensively created in cities to automate certain areas of urban life: urban environment security, transport, energy and housing, healthcare, education, public and municipal administration, etc. The principles and technologies of IoT make it possible to create a fully connected integrated solution necessary for the functioning of the urban and accessible to all residents of the city, employees of city services, officials, and managers of different levels (Javed et al., 2020). The most effective U-systems (connected based on the Internet of Things) are municipal, transport, parking services, as well as the service for combating street and domestic crime. These are, in fact, the key problems of urban life that can be solved based on a unified monitoring and control system. So, in a Korean city, Yeonpyeong New Town effectively operates a U-system in the field of trade in the form of a portal with information about shops, cafes, etc., as well as a system for monitoring the location of children, designed for parents.
- "Smart home" - the system will recognize specific situations occurring in the house and respond to them accordingly, which will provide residents with safety, comfort, and resource conservation. "Smart home" is

designed for the most comfortable life of people through the use of modern high-tech tools. The principle of operation of the smart home system is to automate everything that a residential building consists of lighting, air conditioning, security system, electricity, heating, water supply and sanitation, and so on. The main subsystems of the "smart home" include climate control, lighting, multimedia (audio and video), security systems, communications, and others (Al-Mutawa & Eassa, 2020).

- "Smart energy" – reliable and high-quality transmission of electrical energy from the source to the receiver will be provided at the right time and in the required amount. Currently, the most developed application of IoT technologies is "Smart Grids" in the energy sector (Abir et al., 2021). The operation of such a network is based on the fact that the supplier and the consumer get an objective picture of the use of energy resources through monitoring all sections of the network and, as a result, get the opportunity for operational management. In case of accidents, such networks can automatically identify problem areas and, within a short time, direct electricity through backup circuits, restoring the power supply. For consumers, "smart" networks mean opportunities for flexible regulation of electricity consumption, both in "manual" and automatic mode.
- "Smart transport – moving passengers from one point of space to another will become more convenient, faster and safer. Intelligent transport systems (ITS) based on IoT technologies allow for automatic interaction between infrastructure facilities and a vehicle V2I (Vehicle to Infrastructure) or between different vehicles V2V (Vehicle to Vehicle) (Dey et al., 2016). V2V systems exchange data wirelessly between machines at a distance of up to several hundred meters. V2I systems carry out the exchange between the vehicle and traffic control centres, road operators and service companies. The data transmitted by infrastructure objects are integrated into a common system and transmitted to nearby vehicles. Technologies of both groups can significantly increase the safety and efficiency of transport (Gupta et al., 2020).
- "Smart Medicine– - doctors and patients will be able to get remote access to expensive medical equipment or electronic medical history anywhere, a remote health monitoring system will be implemented, the delivery of medicines to patients will be automated, and much more. "Smart medicine" based on the Internet of Things is usually implemented in practice in the form of human health monitoring systems using a variety of biosensors and sensors and remote medical care systems. Possible applications of sensor network-based monitoring systems in medicine:

  1. Monitoring of the physiological state of a person: physiological data collected by sensory networks can be stored for a long period and can be used for medical research. Installed network nodes can also track the movements of the elderly, disabled people and, for example, prevent falls. These nodes are small and provide the patient with greater freedom of movement, while at the same time allowing doctors to identify the symptoms of the disease in advance. In addition, they contribute to providing a more comfortable life for patients in comparison with hospital treatment.
  2. Monitoring of doctors and patients in the hospital: each patient has a small and light network node. Each node has its specific task. For example, one can monitor the heart rate, while the other takes blood pressure readings. Doctors may also have such a node; it will allow other doctors to find them in the hospital.
  3. Monitoring of medicines in hospitals: sensor nodes can be attached to medicines, then the chances of issuing the wrong medicine can be minimized. So, patients will have nodes that determine their allergies and the necessary medications. (Farahani et al., 2018)

Computerized systems have shown that they can help minimize the side effects of erroneous drug administration. One of the stages of improving modern medicine is the personalization of data and increasing communication between doctors. Easy access to the medical history, allows you to prescribe timely effective treatment. The management of medical records may gradually move to the network. "Cloud" solutions are used to store large amounts of information on the Internet. Thanks to the Internet, doctors from different clinics get access to patient data. Electronic medical records make it possible to find out about the patient's health promptly, prescribe effective treatment. Linking the equipment of a medical institution into a single network will allow you to receive the necessary data on portable devices of doctors, which receive information about the patient: what medications are prescribed, test results, etc. The introduction of Internet technologies saves time for the patient and the doctor. There is no need to get to the polyclinic, it is only necessary to turn on the computer and you can

contact the medical institution. Video calls make it possible not only to make a survey but also to make a general examination, which is often enough for a general idea of human health. If you still need to see a doctor, then you can also make an appointment via the Internet. Pressure measuring devices, scales and other portable equipment are equipped with wireless transmitters that allow you to immediately transfer data to a computer and keep records of your health. A "smart clothing" is being developed that collects data on a person's condition: heart rate, body temperature, respiratory rate. Chips are sewn into such smart clothes at the development stage, which not only carries out measurements but also allows transmitting data to a mobile phone (Espinosa et al., 2021).

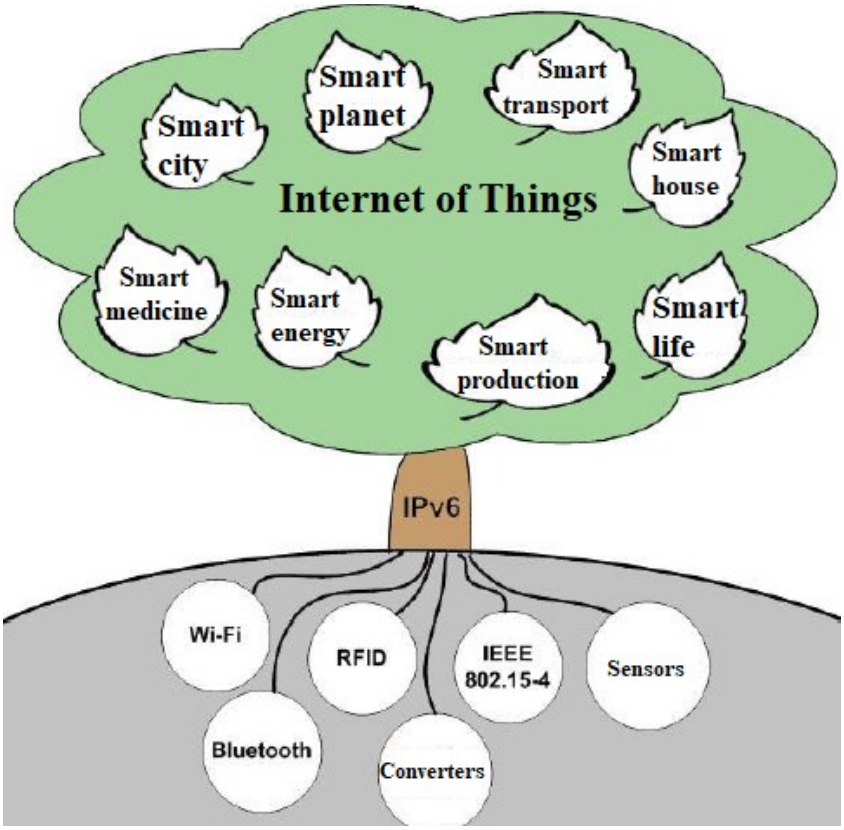



FIGURE 4
SMART APPLICATIONS ON THE BASE OF THE INTERNET OF THINGS

You have many acknowledgements. Please put the sponsor acknowledgements in this section; do not use a footnote on the first page.

## PROBLEMS OF IOT IMPLEMENTATION

The widespread adoption of the Internet of Things is hindered by complex technical and organizational problems, in particular, related to standardization. There are no uniform standards for the Internet of Things yet, which makes it difficult to integrate the solutions offered on the market and largely constrains the emergence of new ones. The vagueness of the formulations of the concept of the Internet of Things and a large number of regulators and their regulations hinder global implementation the most.

The factors slowing down the development of the Internet of Things include the difficulties of the transition of the existing Internet to the new, 6th version of the IP network protocol, primarily the need for large financial costs on the part of telecommunications operators and service providers to modernize their network equipment. *If technological platforms for the Internet of Things have already been practically created, then, for example, legal and psychological ones are still only in the formative stage, as well as problems of interaction between users, data, devices.* One of the problems is data protection in such global networks. There is also a serious problem associated with the invasion of privacy by the Internet of Things. The ability to track the location of people and their property raises the question of who will have this information at their disposal.

*Who will be responsible for storing the information collected by "smart things"? To whom and under what conditions will this information be provided? Is it possible to collect it without a person's consent?* All these questions remain open for now. Also, for the full functioning of such a network, the autonomy of all "things" is necessary, i.e., sensors must learn to receive energy from the environment, and not work from batteries, as is happening now. In addition, with the advent of the Internet of Things, there will be a need to change generally accepted and proven business processes and strategies, which can lead to significant financial costs and risks (Kao et al., 2019). The main drivers and problems of implementing the Internet of Things are given in Table 1. However, all of these disadvantages are not significant compared to what opportunities the Internet of Things can provide for humanity. Therefore, sooner or later humanity will inevitably make extensive use of IoT technologies. But to successfully implement these technologies, we need to know them. As a present future scope, it is highly recommended to develop italicized ideas and answer the questions.

TABLE I
DRIVERS AND BARRIERS OF IOT (INGLE & GHODE, 2017; PADYAB ET AL., 2020)

| Drivers | Barriers |
|---|---|
| The rapid development of info-communication technologies | The need to adopt common standards |
| Fashion for smartphones, tablets, and other mobile devices | Slow transition to IPv6 |
| Logistics and supply management | Risk of closure of private networks |
| Improving the safety and convenience of vehicles | Incompatibility of several components |
| The need to preserve the environment and reduce energy costs | The problem of personal data protection and security |
| Development of the sphere of control over counterfeit products and protection against theft | Relatively high cost of implementation |
| State support and actions of innovators | |

## CONCLUSION

The Internet of People (IoP) that exists today brings real benefits to many individuals, companies, and entire countries. The web drives economic growth through e-commerce and accelerates business innovation by fostering collaboration. The Internet has helped improve the education system by democratizing access to information resources (Siegfried, 2015, Siegfried, 2014). Almost all of our daily life (work, education, leisure, entertainment and much more) is already unthinkable without the Web. But today we are entering an era when the new Internet of Things (IoT) can radically improve the lives of everyone on our planet - to help solve climate problems, heal serious diseases, improve business processes, and make every day of our lives happier.

Cisco predicts that we will inevitably move to the Internet of Everything (IoE), where all sorts of inanimate objects will begin to take into account the context and take advantage of wider computing resources and sensory capabilities. Cisco defines IoE as connecting people, processes, data, and things that add value to network connections to unprecedented levels. IoE transforms information into concrete actions that create new opportunities, enhance the user experience, and create an enabling environment for the development of countries, companies, and users.

This definition highlights an important aspect of IoE that distinguishes it from IoT - the so-called "network effect". As we connect to the Internet, more and more new items, of people and data, the power of the Internet (as a network of networks) grows, according to Matcalfe's law, in proportion to the square of the number of users. This means that the value of the network is a higher arithmetic sum of its components. Because of this, the possibilities of the Universal Internet IoE should become truly limitless, and **this is currently the biggest challenge for IoT, to become IoE**.

## REFERENCES

1. Abir, S. M. A. A., Anwar, A., Choi, J., & Kayes, A. S. M. (2021). Iot-enabled smart energy grid: Applications and challenges. *IEEE Access*, *9*, 50961–50981. https://doi.org/10.1109/ACCESS.2021.3067331

2. Alam, M., Shakil, K. A., & Khan, S. (2020). Internet of things (IoT): Concepts and applications. In the *Internet of Things (IoT): Concepts and Applications*. Springer International Publishing. https://doi.org/10.1007/978-3-030-37468-6
3. Al-Mutawa, R. F., & Eassa, F. A. (2020). A smart home system based on the internet of things. *International Journal of Advanced Computer Science and Applications*, *2*, 260–267. https://doi.org/10.14569/ijacsa.2020.0110234
4. Arndt, R. Z. (2017). Bridging the healthcare gap through digital coaching, online resources. *Modern Healthcare*, *47*(49), 30. https://search.ebscohost.com/login.aspx?direct=true&AuthType=athens,cookie,ip,uid&db=cin20&AN=126780107&site=ehost-live
5. Cisco. (2015). The Internet of Things : Reduce Security Risks with Automated Policies. *Cisco White Paper*.
6. Dey, K. C., Rayamajhi, A., Chowdhury, M., Bhavsar, P., & Martin, J. (2016). Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network - Performance evaluation. *Transportation Research Part C: Emerging Technologies*, *68*, 168–184. https://doi.org/10.1016/j.trc.2016.03.008
7. Divarci, S., & Urhan, O. (2018). Secure gateway for network layer safety in IoT systems. *26th IEEE Signal Processing and Communications Applications Conference, SIU 2018*. https://doi.org/10.1109/SIU.2018.8404785
8. Espinosa, Á. V., López, J. L., Mata, F. M., & Estevez, M. E. (2021). Application of iot in healthcare: Keys to implementation of the sustainable development goals. In *Sensors* (Vol. 21, Issue 7). MDPI AG. https://doi.org/10.3390/s21072330
9. Evans, D. (2011). How the Next Evolution of the Internet Is Changing Everything. *CISCO White Paper*, *April*.
10. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems*, *78*, 659–676. https://doi.org/10.1016/j.future.2017.04.036
11. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010
12. Gupta, M., Benson, J., Patwa, F., & Sandhu, R. (2020). Secure V2V and V2I Communication in Intelligent Transportation using Cloudlets. *IEEE Transactions on Services Computing*, 1–1. https://doi.org/10.1109/tsc.2020.3025993
13. *How NASA, Cisco, And A Tricked-Out Planetary Skin Could Make The World*. (n.d.). Retrieved November 16, 2021, from https://www.fastcompany.com/3024393/how-nasa-cisco-and-a-tricked-out-planetary-skin-could-make-the-world-a-sa
14. Ingle, A. P., & Ghode, S. (2017). Internet of Things (IoT): Vision, Review, Drivers of IoT, Sensors Nodes, Communication Technologies and Architecture. *International Journal of Advances in Computer and Electronics Engineering*, *2*(8), 1–7.
15. Javed, A., Kubler, S., Malhi, A., Nurminen, A., Robert, J., & Framling, K. (2020). BIoTope: Building an IoT Open Innovation Ecosystem for Smart Cities. *IEEE Access*, *8*, 224318–224342. https://doi.org/10.1109/ACCESS.2020.3041326
16. Juan Carlos Castilla-Rubio, & Simon Willis. (2009, March). *Planetary Skin*. A Cisco Internet Business Solutions Group (IBSG). https://docplayer.net/16234718-Planetary-skin-authors-juan-carlos-castilla-rubio-simon-willis-cisco-internet-business-solutions-group-ibsg.html

17. Kao, Y. S., Nawata, K., & Huang, C. Y. (2019). Evaluating the performance of systemic innovation problems of the IoT in manufacturing industries by novel MCDM methods. *Sustainability (Switzerland)*, *11*(18). https://doi.org/10.3390/su11184970
18. Miranda, J., Mäkitalo, N., Garcia-Alonso, J., Berrocal, J., Mikkonen, T., Canal, C., & Murillo, J. M. (2015). From the Internet of Things to the Internet of People. In *IEEE Internet Computing* (Vol. 19, Issue 2, pp. 40–47). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/MIC.2015.24
19. *NASA, Cisco Partnering For Climate Change Monitoring Platform*. (n.d.). Retrieved November 16, 2021, from https://www.nasa.gov/home/hqnews/2009/mar/HQ_09046_NASA_Cisco.html
20. *NASA, Cisco Partnership on Climate Change Monitoring Platform | The Network*. (n.d.). Retrieved November 16, 2021, from https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=4802571
21. Nayyar, A., Puri, V., & Le, D.-N. (2017). Internet of Nano Things (IoNT): Next Evolutionary Step in Nanotechnology. *Nanoscience and Nanotechnology*, *7*(1), 4–8. http://article.sapub.org/10.5923.j.nn.20170701.02.html
22. Padyab, A., Habibipour, A., Rizk, A., & Ståhlbröst, A. (2020). Adoption barriers of IoT in large scale pilots. *Information (Switzerland)*, *11*(1). https://doi.org/10.3390/info11010023
23. Rad, C.-R., Hancu, O., Takacs, I.-A., & Olteanu, G. (2015). Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture. *Agriculture and Agricultural Science Procedia*, *6*. https://doi.org/10.1016/j.aaspro.2015.08.041
24. Ratnaparkhi, S., Khan, S., Arya, C., Khapre, S., Singh, P., Diwakar, M., & Shankar, A. (2020). Smart agriculture sensors in IOT: A review. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2020.11.138
25. Said, O., & Masud, M. (2013). Towards internet of things: Survey and future vision. *International Journal of Computer Networks*, *5*(1), 1–17. http://www.cscjournals.org/csc/manuscript/Journals/IJCN/volume5/Issue1/IJCN-265.pdf
26. Siegfried, P. (2015) Die Unternehmenserfolgsfaktoren und deren kausale Zusammen-hänge, Zeitschrift Ideen- und Innovationsmanagement, Deutsches Institut für Betriebs-wirtschaft GmbH/Erich Schmidt Verlag, ISSN 2198-3143, S. 131-137. https://doi.org/10.37307/j.2198-3151.2015.04.04
27. Siegfried, P. (2014) Analysis of the service research studies in the German research field, Performance Measurement and Management, Publishing House of Wroclaw University of Economics, ISBN: 978-83-7695-473-8, Band 345, pp. 94-104. DOI: 10.15611/pn.2014.345.09
28. Singh, S., Sheng, Q. Z., Benkhelifa, E., & Lloret, J. (2020). Guest Editorial: Energy Management, Protocols, and Security for the Next-Generation Networks and Internet of Things. In *IEEE Transactions on Industrial Informatics* (Vol. 16, Issue 5). https://doi.org/10.1109/TII.2020.2964591

**Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 48-60 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# მოწყობილობის მდებარეობასთან დაკავშირებული საფრთხეების შეფასება 5G ქსელის მაგალითზე

# ASSESSMENT OF LOCATION BASED THREATS FOR DEVICES- A CASE STUDY OF 5G NETWORK

**გიორგი ახალაია, კავკასიის უნივერსიტეტი. პ. სააკაძის ქუჩა, თბილისი, საქართველო მაქსიმ იავიჩი კავკასიის უნივერსიტეტი. პ. სააკაძის ქუჩა, თბილისი, საქართველო სერგი გნატიუკი, ეროვნული საავიაციო უნივერსიტეტი, უკრაინა, კიევი**

**Giorgi Akhalaia , Caucasus University , P.saakadze st1. Tbilisi, Georgia**

**Maksim Iavich, Caucasus University , P.saakadze st1. Tbilisi, Georgia**

**Sergiy Gnatyuk , National Aviation University, Kyiv, Ukraine**

**აბსტრაქტი:**ბოლო წლებია 5G ტექნოლოგია საკომუნიკაციო სფეროს ერთ-ერთი უმნიშვნელოვანესი განხილვის თემა გახდა, განსაკუთრებით კიბერ უსაფრთხოებაში მომუშავე საზოგადოებისთვის. 3 ძირითადი კონცეპტით (გაუმჯობესებული მობილური ბროუდბენდი; ულტრა-საიმედო და დაბალი დაყოვნება; მანქანების მასიური რაოდენობით მიერთება), 5G ტექნოლოგია ცდება მობილური ქსელის ეკოსისტემას და ამით იწყება ახალი ეპოქა უკაბელო კომუნიკაციებში. ბუნებრივია, რომ ახალი ტექნოლოგიები, ფუნქციონალი წარმოქმნის ახალ საფრთხეებს - დაწყებული პროგრამული უზრუნველყოფიდან, დიზაინისა და იმპლემენტაციის პროცესის ჩათვლით. გამომდინარე იქიდან, რომ ვირტუალიზაცია იქნება 5G ქსელის ერთ-ერთი ძირითადი ელემენტი, მეხუთე თაობის ქსელი იქნება უფრო მეტად მოწყვლადი პროგრამულ უზრუნველყოფის საფრთხეების მიმართ. გაუმჯობესებული უსაფრთხოების მიუხედავად, 5G ქსელში მაინც რჩება დაუცველი ნაწილები, საიდანაც თავდამსხმელს შეუძლია გარკვეული მანიპულაციების ჩატარება. MITM (Man In The Middle - კაცი შუაში) ტიპის შეტევის გამოყენებით შესაძლებელი ხდება მომხმარებლის მოწყობილობის მოსმენა და სხვადასხვა მახასიათებლების, პარამეტრების შეცვლა. კვლევის მიზანი იყო დაგვედგინა რამდენად მარტივია MITM ის განხორციელება და გვეპოვა გადაწყვეტილება, უსაფრთხო დიზაინი, რომელიც შეამცირებდა MITM_ის რისკს. ასევე შეგვეფასებინა MITM ისგან გამოწვეული მოწყობილობის მდებარეობასთან დაკავშირებით არსებული საფრთხეები და კვლევის მაგალითზე დაგვედგინა, რომელი საფრთხეა შედარებით უფრო მაღალი რისკის შემცველი. კვლევის ფარგლებში, ვიპოვეთ კონცეპტუალური გადაწყვეტილება, რომლითაც შემცირდება რისკები. კვლევის მეორე ნაწილი ორიენტირებულია მდებარეობასთან დაკავშირებული საფრთხეების ექსპერიმენტულ შეფასებაზე.

**საკვანძო სიტყვები:** *5G ქსელის უსაფრთხოება, უსაფრთხო კომუნიკაცია, ლოკაციასთან დაკავშირებული საფრთხეები*

**ABSTRACT:** Over the last years, 5G technology has become one of the most significant topic for people working in network security industries. With the 3 key concept (enhanced mobile broadband; Ultra-reliable and low-latency communications and Massive machine type communications), 5G network will overcome the limitations of telecom and will arise ა new era of wireless communications. Upcoming functionalities, protocols, standards and services, as always, arise new vulnerabilities: starting from software, design, architecture and implementation processes too. Being virtualization a core component of 5G network, makes it more vulnerable to software-based attacks. Despite of some improved security mechanisms, there are left some weaknesses, that gives ability attackers to conduct various cyber attacks. Using MITM (Man In The Middle), attacker is able stand and sniff the traffic shared between user equipment and cell-towers. The goal of our research was to assess chances of making MITM in 5G network and find the solution, new design to minimize the risk. The second main goal was to determine location based threats in terms of user equipment, raised after MITM and analyze which of them is more dangerous and has the highest probability of

happening. In the framework of research, we have found conceptual solutions, that will lower the risk of MITM and it results. The second part of our study is oriented on experimental work.

**KEYWORDS**: *5G Network Security, Secure Communications; Location-Based Threats*

## 1. შესავალი

ტექნოლოგიურად განვითარებულმა და ძლიერი ეკონომიკის მქონე ქვეყნებმა უკვე დაიწყეს მეხუთე თაობის ქსელის დანერგვა. 2021 წლის 14 იანვარს, 5G ქსელის უსაფრთხოებასთან დაკავშირებით ამერიკის შეერთებულ შტატებსა და საქართველოს შორის გაფორმდა ურთიერთგაგების მემორანდუმი. რომლის თანახმად ქვეყნებს მჭიდრო კომუნიკაცია ექნებათ და ამერიკის შეერთებული შტატები დაეხმარება საქართველოს მეხუთე თაობის ქსელის დანერგვასა და მისი უსაფრთხოების უზრუნველყოფაში.

განვითარება, მითუმეტეს ტექნოლოგიური ევოლუცია არასდროსაა წრფივი. მისი მიმართულება და პროგრესის ხარისხი დამოკიდებულია ახალ საჭიროებაზე, გადაუდებელ აუცილებლობაზე. ხელოვნური ინტელექტის განვითარებამ კიდევ უფრო დააჩქარა ავტომატიზაციის, თვითმართვადი და სხვადასხვა ტიპის დისტანციური სერვისების განვითარება. შესაბამისად, უკვე გამოიკვეთა პრობლემა, როცა ინფორმაციის სწრაფი გადაცემა(მინიმალური დაყოვნება - Extremely Low Latency) იყო შემაფერხებელი, მაგალითად დისტანციური პროცესების რეალურ დროში სინქრონიზაციისათვის, ასევე მნიშვნელოვნად გაიზარდა ქსელზე მიერთებული მოწყობილობების (მაგ: IoT ) რაოდენობა მჭიდრო პერიმეტრზე, რაც არსებული სისტემებისთვის პრობლემას წარმოადგენდა. შესაბამისად დაიწყეს მეხუთე თაობის ქსელზე მუშაობა. 5G ($5^{th}$ Generation) ქსელი არის არამარტო მობილური ინტერნეტის განვითარების ერთ-ერთი საფეხური არამედ უკაბელო ქსელის ახალი ეპოქის დასაწყისი. ხელოვნური ინტელექტის გამოყენებითა და 5G ქსელის საშუალებით სინქრონში იქნება შესაძლებელი მონაცემთა ანალიზი და გადაწყვეტილებების სწრაფი მიღება, გადაცემა და სინქრონიზაცია სხვადასხვა სისტემას შორის.

მეხუთე თაობის ქსელი თავისი უპირატესობიდან გამომდინარე მნიშვნელოვნად განავითარებს/შექმნის ახალ IoT ეკოსისტემას, ავტოპილოტიანი ავტომობილების ინდუსტრიას, ჯანდაცვის სისტემის სერვისებს (მაგ: დისტანციური ოპერაციები); დრონებისა და სხვადასხვა ჭკვიანი მოწყობილობების ფუნქციონალის გაზრდა/ავტომატიზაციას. ხელს შეუწყობს ისეთი სერვისების შექმნას, რომლისთვისაც კრიტიკულად მნიშვნელოვანია ინფორმაციის სწრაფად, მინიმალური დაყოვნებით გადაცემა და/ან სხვა სისტემასთან სტაბილური და სწრაფი კომუნიკაცია.

5G ქსელის განვითარებაზე მუშაობს 3GPP (3rd Generation Partnership Project). რომელიც წარმოადგენს სხვადასხვა ორგანიზაციის კონსორციუმს. პერიოდულად ხდება წევრი ორგანიზაციების შეკრება და სამოქმედო გეგმის დასახვა. ITU_მ მეხუთე თაობის ქსელის KPI_დ დაასახელა:

- > 10Gb/s - არანაკლებ 10 გიგაბიტ/წამი პიკური სიჩქარე (eMBB)

- > 1M/km$^2$ - არანაკლებ 1 მილიონი მოწყობილობის დაკავშირების შესაძლებლობა კვადრატულ კილომეტრზე. (mMTC). ასეთი სიმჭიდროვე აღებულია IoT მოწყობილობებიდან გამომდინარე.
- < 1ms Latency - არაუმეტეს 1 მილიწამი დაყოვნება.(URLLC) [1]

რაც შეეხება 5G_ის სამუშაო სპექტრს, შემდეგნაირად არის დაგეგმილი:

1. Low-band -- < 1 GHz
2. Mid-band -- 1 GHz – 6 GHz
3. High-band(mmWave) – 6 GHz – 100 GHz

**Low-Band** - მოიცავს 1GHz მდე სპექტრს. მისი უპირატესობაა მჭიდროდ დასახლებული რეგიონის დაფარვა. ნაკლებ პრობლემა უქმნის შენობა/ნაგებობები. მაგრამ Peak Data Speed დაახლოებით 100 Mbps_ია.

**Mid-Band** - იგულისხმება 1GHz დან 6GHz მდე სპექტრს. Low-band ისგან განსხვავებით უფრო მეტი გამტარუნარიანობა და ნაკლები დაყოვნება აქვს. თუმცა შედარებით მეტ დაბრკოლებას უქმნის ნაგებობები ვიდრე Low-band_ს. პიკური სიჩქარე დაახლოებით 1 Gbps_ია.

**High-Band** - ძირითადად ამ სპექტრს მოიაზრებენ როცა 5G ქსელზეა საუბარი. ამ სპექტრის საშუალებით შესაძლებელი ხდება მინიმალური დაყოვნებით, პიკური სიჩქარის ათობით Gbps_მდე გაზრდა. ხშირად მოიხსენიებენ როგორც mmWave ტექნოლოგიად. ზემოთ ჩამოთვლილი სპექტრული დანაყოფებიდან, სწორედ High-band წარმოადგენს მთავარ რგოლს 5G ქსელის იმპლემენტაციაში.[2]

5G ქსელის ერთ-ერთი მთავარი სამიზნე კატეგორია IoT მოწყობილობებია. მნიშნელოვანი პროგრესი უნდა იყოს ქსელის ისე მუშაობა, რომ IoT მოწყობილობების ენერგო მოხმარება მინიმუმამდე დავიდეს(რა თქმა უნდა ქსელის კუთხით). თუმცა 5G ტექნოლოგიის მომხმარებლისთვის ერთ-ერთი ყველაზე შემჩნევადი პრობლემა მოწყობილობის ელემენტის სწრაფი დაცლა, ე.წ. Battery Drain_ია. CNET ის ტესტერებმა ჩაატარეს ცდა: აიღეს 5G მხარდაჭერის მქონე ორი მობილური, რომლებიც ჯერ ამუშავეს მე_5 თაობის ქსელზე და შემდეგ მის გარეშე. პირველ შემთხვევაში MOTO Z3 ის ელემენტი 5G ქსელზე გადაბმულად მუშაობის შედეგად 4 საათში ბოლომდე დაიცალა. რაც შეეხება მეორე ტესტს, გამოიყენეს Galaxy S10. ამ შემთხვევაში, 5G ზე მუშაობის შედეგად 4 საათში ელემენტის დამუხტვის პროცენტი განახევრდა, მაშინ როცა გადაბმულად ტელეფონი დამუხტვის გარეშე 18 საათი მაინც უნდა მუშაობდეს.[3]

აღნიშნული პრობლემის შესახებ წერს Samsung_იც. მიზეზად კი, სხვა ექპერტების მსგავსად, გადამრთველს ე.წ. switch_ს ასახელებს. 5G ქსელი ამ ეტაპზე გამოიყენება მხოლოდ მონაცემთა გადაცემისთვის, უფრო სამომხმარებლო ენაზე რომ ვთქვათ, ინტერნეტისთვის.[4] აქედან გამომდინარე, მობილურ ტელეფონს პარალელურ რეჟიმში უწევს 4G ან 3G/2G ქსელთან კავშირი, რათა შეუფერხებლად მიიღოს და/ან განახორციელოს სატელეფონო ზარი, მოკლე ტექსტური შეტყობინება - SMS. სტატიაში ნათქვამია ისიც, რომ ელემენტის სწრაფი დაცლის გარდა, ამან შეიძლება მოწყობილობის შესამჩნევად გაცხელება გამოიწვიოს. ასევე მნიშნელოვანი ფაქტორია ქსელის მუდმივი გადართვა 5G დან 4G/3G ზე. გამომდინარე იქიდან, რომ ალგორითმის მიხედვით ტელეფონი მუდმივად ცდილობს სტაბილური ინტერნეტ სიჩქარის შენარჩუნებას, ხოლო 5G ქსელის დაფარვა არ არის კარგი და მნიშვნელოვნად დამოკიდებულია ანძინად დაშორებულ მანძილზე, დახრის კუთხეზე(ანძასა და მიმღებ მოწყობილობას შორის) მობილური ტელეფონი ინტერნეტ სერვისის გადაცემას მუდმივად რთავს 5G დან 4G/3G ზე. აქედან გამომდინარე ხშირი

გადართვა/გადმორთვა მოიხმარს დამატებით ენერგიას, რაც საბოლოო ჯამში ელემენტის სწრაფ დაცლაში აისახება. ექსპერტების აზრით ტექნოლოგია ჯერ კიდევ დახვეწის პროცესშია და დროთა განმავლობაში გაუმჯობესდება გადართვის (Switch) მექანიზმი. თუმცა, არ უნდა დაგვავიწყდეს, რომ ერთ-ერთი მთავარი პრობლემა, საფრთხე MITM შეტევაა, რომელიც გარდა ინფორმაციის გაჟონვისა, შემდეგ სხვადასხვა ტიპის შეტევის საშუალებასაც იძლევა.

## 2. 5G_ს უსაფრთხოება

მეხუთე თაობის ქსელის უსაფრთხოება კიდე უფრო კომპლექსურია მისი არქიტექტურიდან გამომდინარე. მონაცემთა ცენტრების, cloud ტექნოლოგიებისა და თითოეული endpoint ის დაცვა კრიტიკული გახდა რადგან ქსელის დანერგვის ერთ-ერთი core კომპონენტია ვირტუალიზაცია და ქსელის ფუნქციათა ვირტუალიზაციის ინფრასტრუქტურა. გამომდინარე იქიდან, რომ 5G ქსელში ჩაირთვება სხვადასხვა კატეგორიის, მწარმოებლის, შესაბამისად firmware ისა და აპარატურული არქიტექტურის მქონე სისტემა/მოწყობილობა, რომლებიც განსხვავებულ ტექნოლოგიებს იყენებენ მათი ცალ-ცალკე არსებული სისუსტე, გადმოყვება სისტემაში და უკვე გახდება სისტემის შემადგენელი სისუსტე. ასევე ყურადსაღებია LBS(Location Based Service) ტიპის სერვისები, მომხმარებლის პერსონალური ინფორმაციაზე, მოწყობილობის სხვადასხვა სერვისის გამოყენებისას გაცემული პირადი ინფორმაცია საბოლოოდ დასაცავი აღმოჩნდება. 5G ქსელის შემთხვევაში ჩნდებიან ახალი აქტორებიც, მაგალითად - ვირტუალური მობილური ოპერატორები, კომუნიკაციების სერვის პროვაიდერები და ქსელის ინფრასტრუქტურის პროვაიდერები, რომლებთაც თავიანთ განსხვავებული უსაფრთხოების პოლისები აქვთ. შესაბამისად მათი საერთო სისტემაში მოყვანა იქნება აუცილებელი. ის ფაქტი, რომ 5G ქსელი წინა თაობებთან შედარებით უფრო მეტად software based და cloud-based ია, უკეთესი მონიტორინგის სისტემის იმპლემენტაციის საშუალებას იძლევა. ქსელის სეგმენტირება (Network Slicing) ის საშუალებით კი შესაძლებელია კატეგორიებად დაიყოს და თითოეულ მათგანზე მორგებული დაცვის მექანიზმები გაიმართოს.

მართალია 4G_სგან განსხვავებით 5G ქსელი მომხმარებლის უსაფრთხოება შედარებით დახვეწილია, მაგრამ მაინც რჩება ინფორმაციის ნაწილი, რომელიც ე.წ. clear text_ად მიმოიცვლება ქსელში ბაზასთან დაკავშრებისას. რომელიც შემდეგ სხვა ინფორმაციის მოპარვისთვის შეიძლება გამოიყენოს თავდამსხმელმა. ეს აჩენს ე.წ. Fake Base Station Attack ის საფრთხეს. ამ დროს მესამე პირი მომხმარებელს თავს აჩვენებს თითქოს ის არის რეალური cell tower, რის შედეგადაც მასთან დაკავშირებას ცდილობს მსხვერპლი. საბოლოოდ კი თავდამსხმელი შეძლებს ტრაფიკის მოსმენას და მასზე სხვადასხვა მანიპულაციას. მსგავს იმიტირებულ შეტევაზე Black Hat 2019 ის “New Vulnerabilities in 5G Networks” სესიაზე ისაუბრა Altaf Shaik. მათმა ჯგუფმა შექმნა fake base station და აკვირდებოდნენ მოწყობილობებიდან გაგზავნილ ინფორმაციას, რომელთა ნაწილი დაუშიფრავია. დაკვირვება ხდებოდა შემდეგ კატეგორიებად: მწარმოებელი, მოდელი, ოპერაციული სისტემა, ვერსია და რისთვის გამოიყენება(use case).[5] ამის შედეგად მათ ქონდათ უკვე სრული სურათი, რუკა თუ საიდან რა მოწყობილობა რა ფუნქციით დატვირთული უკავშირდებოდა ქსელს. ეს არის **MNmap (Mobile Nmap)**. შედეგად თავდამსხმელს აქვს ქსელზე მიერთებული მოწყობილობების სრული სურათი და შესაბამისად შეძლებს კონკრეტული სამიზნე კატეგორიისთვის დაგეგმოს სხვა, უფრო მაღალტექნოლოგიური შეტევა.

მანამდე სანამ Device_დან base თან გაგზავნილი ინფორმაცია ჯერ კიდევ clear text ია, ანუ დაუშიფრავია შესაძლებელია მისი hijack(გატაცება) და მისი სურვილისამებრ შეცვლა. მაგალითად კავშირის შენელება, device ის იდენტიფიკაციის შეცვლა, MIMO ფუნქციონალის ჩამოშორება, battery drain და სხვა. **MITM**_ით PSM პარამეტრის თავის არიდებაა შესაძლებელი. რომლის შედეგადაც მოწყობილობა მუდმივად სკანირების რეჟიმშია და ეძებს დასაკავშირებელ hosts. შედეგად კი ელემენტი დაახლოებით 5 ჯერ უფრო სწრაფად დაჯდება. წყაროებში ეს შეტევა მოხსენებულია როგორც **Battery Drain.**

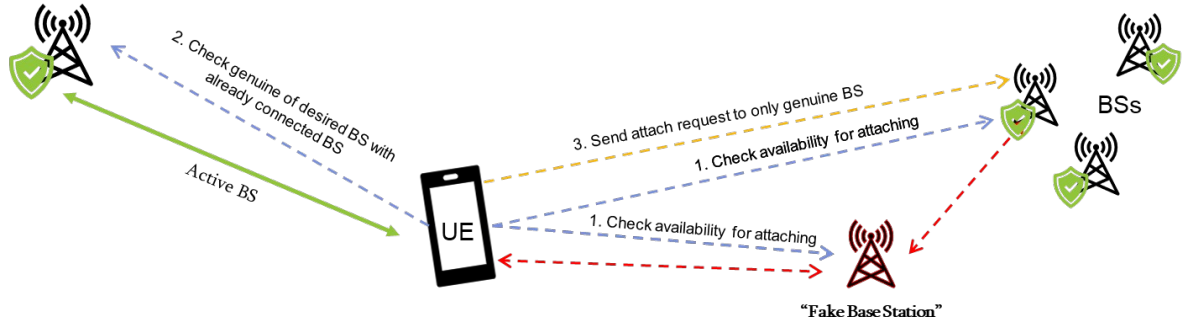
მკვლევარების საუბრობენ ასევე 5G Downgrade შეტევაზე(ზოგ წყაროში Bidding Down Attack წერია). ამ დროს სამიზნე მოწყობილობის კავშირის ჩამოქვეითება (Downgrade) ხდება 3G ან 4G ქსელზე. შემდეგ კი ამ ტექნოლოგიებზე არსებულ სისუსტეებზე უპირატესობის მოპოვება ხორციელდება.

ასევე მნიშნელოვანია ამ ტექნოლოგიების სწორი იმპლემენტაცია. რაც არ უნდა კარგად გამართონ 5G_ზე მომუშავე ორგანიზაციებმა უსაფრთხოების პროტოკოლები და სტანდარტები, თუ სერვის პროვაიდერმა/ოპერატორმა სტანდარტის დანერგვისას არასწორად შეასრულა პირობები ან არასრულად(მისი ხარჯიდან გამომდინარე) მაშინ სისტემის უსაფრთხოება ისევ რისკ ქვეშ დგება. მსგავსი ქეისები კი საკმაოდ იყო 4G ტექნოლოგიების გაშვებისას, როცა ოპერატორებმა ხარჯის შემცირების მიზნით გარკვეული პროცედურები არ შეასრულეს. მსგავსი პრობლემა დგება 5G_ს შემთხვევაშიც. თუმცა მსგავსი ტიპის პროცესი შეიძლება სახელმწიფომ დაარეგულიროს სხვადასხვა საკანონმდებლო მექანიზმით. მაგალითად USA ში, FCC (კომუნიკაციების ფედერალური კომისია) გააკონტროლებს სტანდარტის დანერგვას.

ყველა ტექნოლოგიას, სერვისს თუ ფუნქციონალს აქვს უსაფრთხოების გარკვეული პრობლემა. 5G ქსელს, კერძოდ ვირტუალიზაციის ნაწილში აქვს უსაფრთხოების საკმაოდ მნიშვნელოვანი პრობლემები. ქსელის პროცესების სამართავად გამოიყენება AI. ქსელის მასშტაბურობიდან გამომდინარე, AI Operator Hijack შეტევისას შედეგები იქნება გაცილებით მასშტაბური, ვიდრე ჩვეულებრივ შემთხვევაში. თუ ვირტუალიზაციის პლათფორმაზე განახორციელებენ შეტევას, რომელიც core მექანიზმია ქსელის, მთავარი სამართავი პანელი მაშინ წარმოიდგინეთ რა დაემართება სხვადასხვა IoT მოწყობილობას, მაგალითად ინპლანტებს, უპილოტო მანქანებს, რა მოხდება დისტანციური ოპერაციებისას.

## 3. უსაფრთხო დიზაინის კონცეპტი

არსებული დიზაინი, თეორიული კვლევისა და პრაქტიკული ექსპერიმენტების თანახმად მოწყვლადია MITM ტიპის შეტევების მიმართ. რომელიც მიიჩნევა ერთ-ერთ ყველაზე მძლავრ, ეფექტურ ქსელურ შეტევად. ჩვენი კვლევის შედეგად მიღებული ახალი, უსაფრთხო დიზაინის კონცეპტი, მნიშვნელოვნად ამცირებს ქსელში ე.წ. ცრუ ანძების ეფექტურობას.




*ილუსტრაცია 1*

ილუსტრაცია 1_ზე მოცემულია კონცეპტუალური დიზაინის მიხედვით როგორ მოხდება ქსელში მოწყობილობის ჩართვა, ოპერატორის ანძასთან დაკავშირება. მწვანე სიმბოლოთი აღნიშნულია ავტორიზებული ანძები, ხოლო წითლად მოცემული ცრუ ანძა, რომელიც ასრულებს MITM ტიპის შეტევას. ჩვენი იდეის მიხედვით, ანძებს უნდა ქონდეს წინასწარ განსაზღვრული ალგორითმი, სია, რომლითაც შეძლებენ ერთმანეთის ავთენტურობის გადამოწმებას, ამ შემთხვევაში სერვისს შეასრულებენ მომხმარებლის მოწყობილობისთვის. განხილულია შემთხვევა, როდესაც მოწყობილობას უკვე აქვს აქტიური კავშირი ლეგიტიმურ ანძასთან. ქსელის მუშაობის პრინციპიდან გამომდინარე, მუდმივად ეძებს უფრო ძლიერი სიგნალის მქონე ანძას. შესაბამისად როდესაც იპოვის ცდილობს ახალ ანძაზე გადართვას. ჩვენი დიზაინის მიხედვით, სამიზნე ანძასთან დაკავშირების მოთხოვნის გაგზავნამდე ითხოვს მაიდენტიფიცირებელ ინფორმაციას, რომელსაც ამოწმებს უკვე აქტიურ ანძასთან - რამდენად ავტორიზებულია სამიზნე ანძა ქსელში. თუ, აქტიური ანძა დაუდასტურებს სამიზნე ანძის ავთენტურობას, მაშინ მოწყობილობა დაიწყებს ახალ ანძაზე გადართვის პროცედურებს.

ამ დიზაინის ერთ-ერთი მნიშვნელოვანი შეზღუდვაა ის შემთხვევა, როდესაც არ გვაქვს აქტიური კომუნიკაცია რეალურ ანძასთან ან გვაქვს მაგრამ არასტაბილური სიგნალია. პირველი შეიძლება მოხდეს მაშინ, როდესაც ე.წ. ფრენის რეჟიმიდან გადავდივართ ჩვეულებრივ რეჟიმზე და ვიწყებთ ქსელში ჩართვას, ან მაგალითად როდესაც მობილურ მოწყობილობას ხელახლა ვრთავთ. არასტაბილური სიგნალი კი შიდა როუმინგის დროს შეიძლება მოხდეს. მაგალითად, როდესაც კარგი დაფარვა არ აქვს ოპერატორს. შესაბამისად ამ დროს ვერ მოხდება გადამოწმება სამიზნე ანძის ავთენტურობის. ამ შემთხვევაში შეიძლება იყოს წინასწარ, მოწყობილობაში ინტეგრირებული სია, დაახლოებით სერთიფიკატის მსგავსი, რომლითაც თავისივე თავთან გადაამოწმებს სამიზნე ანძის რეალურობას.

ეს დიზაინი თავის მხრივ კიბერ საფრთხეების რისკს გაზრდის მობილური ოპერატორების ანძების მიმართს. ეს ბუნებრივიცაა, რადგან ყოველი ახალი დაცვის მექანიზმი ამისამართებს შეტევის ვექტორებს, სხვა შედარებით სუსტი წერილის მიმართ. ასევე ნაკლებად ეფექტური შეიძლება იყოს საერთაშორისო როუმინგის დროს.

## 3.1.ექსპერიმენტული კვლევა

კვლევისას განვითარებული თეორიული იდეების განსახორციელებლად, ჩავატარეთ ექსპერიმენტი. მიკრო ლაბში, მიკრო კომპიუტერების - Raspberry Pi_ს გამოყენებით

განვახორციელეთ მოწყობილობის ქსელთან მიერთების სიმულაცია. პროცესის სამართავად გამოვიყენეთ კომპიუტერი, Kali OS ის ოპერაციული სისტემა და სხვადასხვა პროგრამული პაკეტი. Raspberry Pi_ს ნაწილი წარმოადგენდა მობილური ოპერატორის ანძის სიმულაციას, ხოლო ნაწილი მომხმარებლის მოწყობილობას. (ცხრილი 1) როდესაც მომხმარებლის მოწყობილობებს მივუთითეთ, რომ წინასწარ გადაემოწმებინა ბაზის ავთენტურობა, არცერთი შემთხვევა აღარ ყოფილა “fake base station” თან დაკავშირების. ფაქტობრივად, მოწყობილობები აღარ აგზავნიდნენ ცრუ ანძებთან დაკავშირების მოთხოვნას. ეს შეიძლება ჩაითვალოს როგორც ჩვენეული გადაწყვეტილების დადებით შედეგად და მოგვცეს პოზიტიური მოლოდინი ალგორითმის რეალურ შემთხვევაში მუშაობისთვის. მაგრამ, აქვე ყურადსაღებია ის ფაქტი, რომ რეალური სისტემა ბევრად დატვირთულია მოწყობილობებისა და ანძების რაოდენობის გათვალისწინებით, შესაბამისად აუცილებელია რეალურ სისტემაზეც ტესტირება. გამომდინარე იქიდან, რომ 5G ქსელი ამ შემთხვევაში არ გვაქ, ტესტირება მიმდინარეობა 4G ქსელის მაგალითზე. თუმცა, დაკავშრების პროცესი მსგავსია, ამიტომ ეს კვლევის შედეგებზე უარყოფით გავლენას არ მოახდენდა.

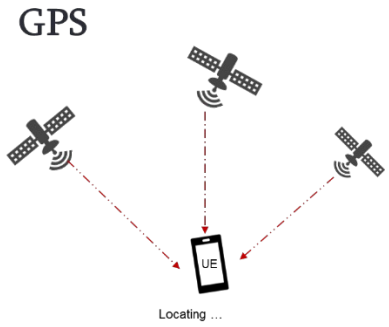
ექსპერიმენტის მეორე ნაწილში განვიხილეთ, ისეთი შემთხვევა როდესაც მოწყობილობა ე.წ. “Roaming”_შია. ანუ როდესაც აქტიური კავშირი ბაზასთან არ აქვს ან კავშირი არასტაბილურია. ამ შემთხვევაში წინასწარვე მივაწოდეთ სანდო ანძების სია. შედეგების მიხედვით, ორივე შემთხვევა შეიძლება გამოვიყენოთ ერთად, როგორც დამზღვევი სისტემა, რომელიც უზრუნველყოფს ქსელში მეტ უსაფრთხოებას. მეორე შემთხვევაში, პირველთან შედარებით პროცესი უფრო სწრაფად მიმდინარეობს, თუმცა მნიშნელოვანი კომპონენტი იქნება ახალი ანძების შესახებ ინფორმაციის მიწოდება მოწყობილობისთვის და/ან უკვე არსებული ინფორმაციის მთლიანობის/უცვლელობის დაცვა.

| **მოწყობილობა** | **რაოდენობა** | **დანიშნულება** |
|---|---|---|
| Raspberry Pi (LTE მოდულით) | 40 | 20 - ანძის სიმულატორი,<br>5 - ცრუ ანძის სიმულატორი<br>15 - მომხმარებლის მოწყობილობა |
| კომპიუტერი Kali OS_ით | 2 | პროცესის სამართავად, სიმულაციისთვის |
| | | |
| **შედეგები** | | |
| **ალგორითმის ტიპი** | **წარმატება/ ჩავარდნა** | **კომენტარი** |
| აქტიური ანძიდან აუთენთიფიკაცია | წარმატება | 15/15 |
| შიდა ცხრილიდან აუთენთიფიკაცია | წარმატება | 15/15 |
| **საბოლოო შეფასება** | | |
| ალგორითმებმა იმუშავა, თუმცა გაიზარდა დაყოვნება | | |

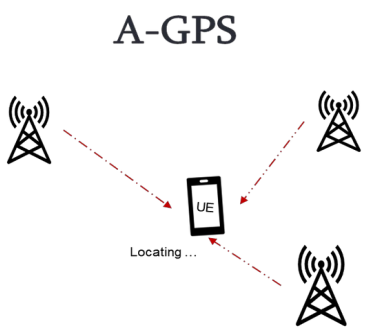
ცხრილი 1. ექსპერიმენტში გამოყენებული ინფრასტრუქტურა

## 4. ლოკაციასთან დაკავშირებული საფრთხეები

მოწყობილობის ადგილმდებარეობის დადგენის 2 ძირითადი მეთოდი არსებობს: GNSS ტექნოლოგიების გამოყენებით ან A-GPS მეთოდით. პირველი გულისხმობს GNSS სატელიტების გამოყენებით მოწყობილობის მდებარეობის განსაზღვრას, რაც არსებული მეთოდებიდან ყველაზე ზუსტია, ხოლო მეორე (A-GPS) მობილური ოპერატორის ანძების მიხედვით მომხმარებლის მოწყობილობის ადგილმდებარეობის გადათვლას/დაანგარიშებას. ორივე მეთოდს აქვს თავისი უპირატესობა და შეზღუდვები: GNSS ის შემთხვევაში, აუცილებელია მოწყობილობას პირდაპირი ხედვა ქონდეს სატელიტებთან, ანუ ე.წ. ღია ცის პრინციპი მუშაობს, მაგრამ ყველაზე მაღალი სიზუსტეს იძლევა (3-5 მ ცდომილება სამომხმარებლო მოწყობილობებში), ხოლო მეორე A-GPS, მობილური ოპერატორის მინიმუმ 3 ანძის საშუალებით ითვლის თავის მდებარეობას. ეს ნაკლებად ზუსტია, მაგრამ შეუძლია დახურულ სივრცეებშიც, მაგალითად შენობებშიც გადაითვალოს მოწყობილობის კოორდინატები. (ფიგურა 1, 2)




*ფიგურა 1. GPS მეთოდი*

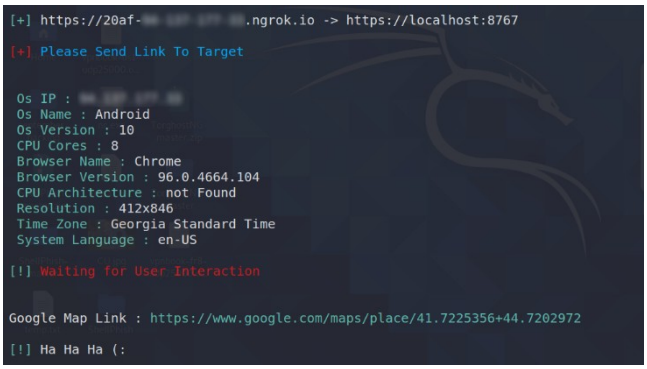



*ფიგურა 2. A-GPS მეთოდი*

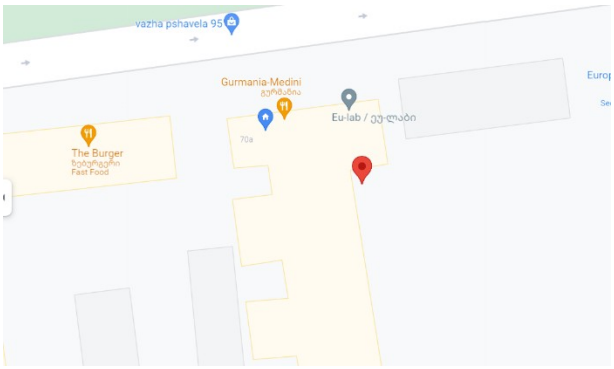
გამომდინარე იქიდან, რომ A-GPS ის შემთხვევაში მოწყობილობა იყენებს მობილური ოპერატორის ანძების დეტალებს, კოორდინატებს თავისი მდებარეობის დასაზუსტებლად, MITM ის შეტევის შემთხვევაში, როდესაც ე.წ. “Fake Base Station“_ის შეტევა ხორციელდება, დიდია საფრთხე, რომ მოწყობილობის ლოკაცია არასწორად გადაითვალოს, რადგან თუ მიწოდებული(გამოთვლისას გამოყენებული) ინფორმაცია არასწორი იქნება, მაშინ შედეგსაც არასწორს მივიღებთ. ეს კი დიდ პრობლემას შეუქმენის ე.წ. Location-Based სერვისებს, მათ შორის 911/112 სერვისებისთვის საჭირო პროცესებს. ასევე, გასათვალისწინებელია ის ფაქტიც, რომ GNSS ს მეთოდის შემთხვევაში აუცილებელია მობილურ მოწყობილობაში გააქტიურებული იყოს GPS მოდული, ხოლო A-GPS მეთოდი, ქსელის მუშაობის პრინციპიდან გამომდინარე მობილურ მოწყობილობაში ავტომატურად აქტიურია (გარდა ე.წ. ფრენის რეჟიმისა). ეს კი, შესაძლოა, რაღაც შემთხვევებში ამარტივებდეს LBS ზე შეტევას. კვლევისას სხვადასხვა სიმულაციური ექსპერიმენტი ჩავატარეთ, რომლის დეტალებიც შემდეგ თავშია აღწერილი.

## 4.1. ექსპერიმენტული კვლევა

კვლევისას ჩავატარეთ რამდენიმე ექსპერიმენტი, რათა დაგვედგინა რომელი მეთოდი, გზაა შედარებით მარტივი, რომლითაც საშუალება გვექნება დავადგინოთ მომხმარებლის მდებარეობა მათი „ნებართვის გარეშე“. (ცხრილი 2). პირველ შემთხვევაში გამოვიყენეთ მზა ხელსაწყო, Storm-braker (ფიგურა. 9, 10). [6]

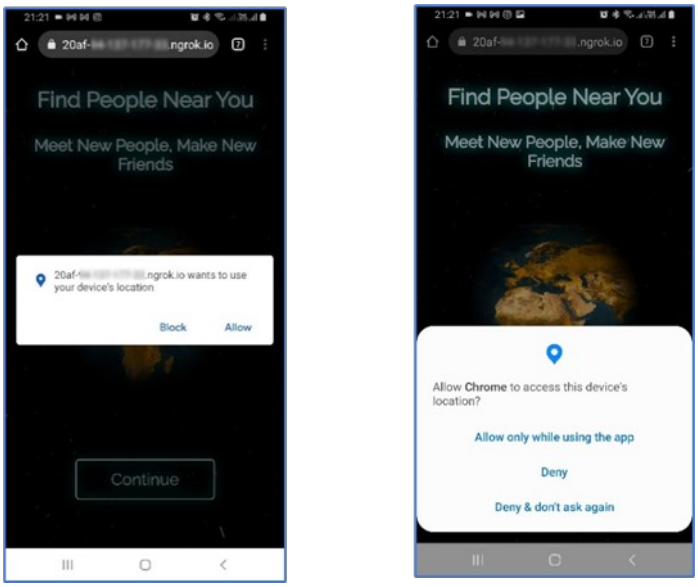



*ფიგურა. 9*




*ფიგურა. 10*

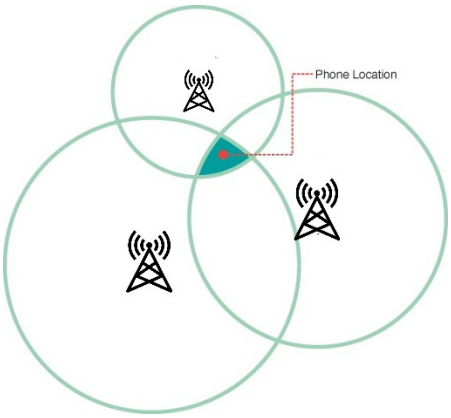
ის არის მზა პროგრამული უზრუნველყოფა, რომელიც საშუალებას გვაძლევს მომხმარებლის მოწყობილობიდან წამოვიღოთ GNSS კოორდინატები. თუმცა, კვლევამ აჩვენა, როგორც მოსალოდნელი იყო, რომ საკმაოდ „ხმაურიანია“. რადგან მომხმარებელი წინასწარ განსაზღვრულ ბმულზე გადასვლისას ღებულობს გამაფრთხილებელ შეტყობინებას, რომ აპლიკაცია/სერვისი ცდილობს მის ლოკაციაზე წვდომის მოპოვებას და ამისთვის ითხოვს ნებართვას. (ფიგურა 11)



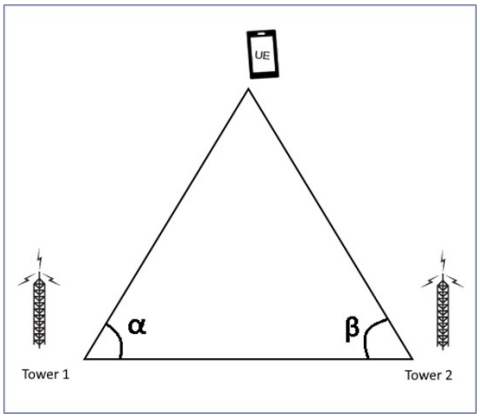

*ფიგურა 11*

გამომდინარე იქიდან, რომ მოწყობილობა მუდმივ რეჟიმში არ ითვლის თავის მდებარეობას GNSS ტექნოლოგიების გამოყენებით(საუბარია თანამგზავრებზე), აპლიკაციით ასეთი ინფორმაციის მოპარვისას, მომხმარებელი ღებულობს შეტყობინებას, რომ აპლიკაცია ცდილობს მოდულის გამოყენებას და მდებარეობის დადგენას. ამ მეთოდის უარყოფითი

მხარეა ისიც, რომ თუ GPS მოდული გამორთულია, ან მოწყობილობა დახურულ სივრცეშია (მაგალითად შენობაში) მაშინ ვერ იმუშავს. ამ შემთხვევაში უფრო ეფექტურია, მომხმარებლის მოწყობილობიდან თუ A-GPS ის მონაცემებს წამოვიღებთ. რადგან მობილური მოწყობილობის და ოპერატორების მუშაობის პრინციპიდან გამომდინარე, მოწყობილობა მუდმივად ამოწმებს დაფარვის არეალში მყოფ ანძებს, შესაძლებელია ამ ინფორმაციით, მონაცემებით და ტრიანგულაცია/ტრილატერაციის მეთოდით დადგინდეს მომხმარებლის მიახლოებითი მდებარეობა. არა ისეთივე ზუსტი როგორც GNSS ტექნოლოგიების შემთხვევაში, მაგრამ ასადევნებლად საკმარისი.

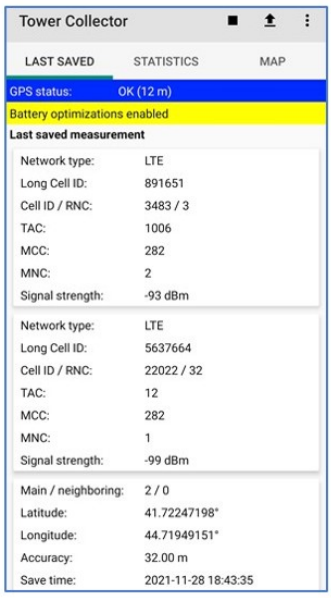



*ფიგურა 12. ტრილატერაცია*

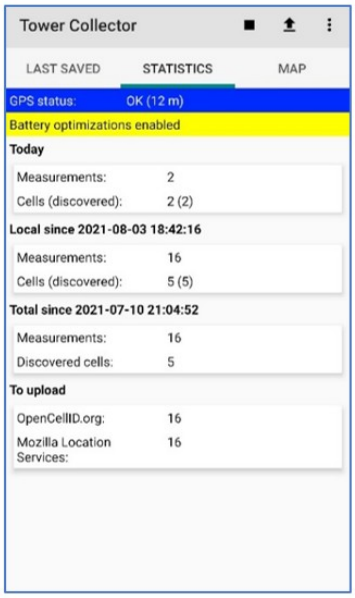



*ფიგურა 13. ტრიანგულაცია*

არსებობს მზა ხელსაწყოები, რომელიც საშუალებას გვაძლევს ოპერატორის ანძების განლაგების რუკა შევქმნათ, რომელსაც შემდეგ მომხმარებლის მოწყობილობის მდებარეობის განსაზღვრისთვის გამოვიყენებთ. მაგალითად OpenCellID პროექტი. ჩვენ გამოვიყენეთ ანდროიდის მარკეტზე არსებული პროგრამა: “Tower Collector”. (ფიგურა 12, 13)







როგორც ფიგურაზე ჩანს, საკმაოდ დეტალურ ინფორმაციას ვიღებთ ანძების შესახებ, მათ შორის რაც მთავარია ID, კოორდინატები და სიგნალის სიძლიერე. აღსანიშნავია ფაქტი, რომ საკმაო მსჯელობის საგანია სიგნალის სიძლიერე, მკვლევართა ნაწილი თვლის, რომ ამ პარამეტრით შესაძლებელია ზუსტი მოწყობილობის ადგილმდებარეობის დადგენა. თუმცა, ფაქტია, რომ იმდენად კომპლექსური მახასიათებელია, რთულია ცალსახად რაიმეს თქმა. რადგან ძალიან ბევრი ფაქტორი ახდენს გავლენას სიგნალის სიძლიერეზე, მათ შორის რელიეფი და შენობები. რაც ყველაზე მნიშვნელოვანია, 5G ქსელის შემთხვევაში იმისათვის რომ მოწყობილობამ გამოიყენოს High-Band სპექტრი, ე.წ. mmWave, აუცილებელია რომ იყოს ძალიან ახლოს, პირდაპირი ხედვით ანძასთან. რადგან ამ სიხშირეების ტალღებს ყველაზე (წინა 2 თან შედარებით) მეტად ამახინჯებს შენობები. შესაბამისად, ეს შეიძლება გახდეს იმის მიზეზი, რომ 1 ანძითაც დადგინდეს მოწყობილობის მდებარეობა. რაც დიდ პრობლემას წარმოადგენს მომხმარებლის უსაფრთხოებისთვის.

კვლევისას გამოყენებული ინფრასტრუქტურა:

| **მოწყობილობა** | **რაოდენობა** | **დანიშნულება** |
|---|---|---|
| Raspberry Pi (LTE და GPS მოდულებით) | 30 | 10 - საბაზისო სადგური,<br>15 - ცრუ საბაზისო სადგური<br>5 - მომხმარებელი |
| GPS მოდულიანი მობილური მოწყობილობები | 5 | მომხმარებელი |
| Laptop (Kali OS) | 2 | ექსპერიმენტის მონიტორინგი და მართვა |
| | | |
| **შედეგები** | | |
| **ალგორითმის ტიპი** | **წარმ/ ჩავარნა** | **კომენტარი** |
| GPS (GNSS კოორდინატების მოწყობილობიდან აღება) | წარმატებული | Success with noise if GPS module was enabled. User interaction was needed. As they were alerted by the system |
| A-GPS (ინფორმაციის მოწყობილობიდან წამოღება) | წარმატებული | 10/10 |
| MITM by Fake BS | წარმატებული | 10/10 |
| ანძების ინფორმაციის(სიხშირეების, აქტიური ანძების) წამოღება | წარმატებული | 8/10 |

*ცხრილი 2*

კვლევისას დადგინდა, რომ A-GPS ის მონაცემების წამოღება ნაკლებად ხმაურიანია, ვიდრე GNSS მონაცემების. ასევე, თუ GPS მოდული გამორთულია ან მოწყობილობა დახურულ სივრცეშია, პრაქტიკულად გამოუსადეგარია GNSS ის მეთოდი. 5G ქსელის შემთხვევაში კი, როდესაც High-Band ზე იქნება მოწყობილობა, შესაძლებელია 1 ანძით დადგინდეს მისი მიახლოებითი მდებარეობა. ასევე ყურადსაღებია ის ფაქტი, რომ Fake Base Station ების შემთხვევაში, როდესაც მოწყობილობას ანძის არასწორი კოორდინატი შეიძლება მიეწოდოს, მისი LSB სერვისები გაუმართავად იმუშავებს. რამაც ზოგ შემთხვევაში შეიძლება სავალალო შედეგამდე მიგვიყვანოს.

## 5. დასკვნა

მეხუთე თაობის ქსელის დანერგვა და განვითარება მნიშვნელოვან როლს ითამაშებს კაცობრიობის სამომავლო განვითარებაში. რაც თავის მხრივ აისახება ეკონომიკურ ფაქტორებზეც. მასშტაბებიდან გამომდინარე ცდება ტელეკომ კომუნიკაციების იდეას და ქმნის ახალ ეკოსისტემას, სადაც გაერთიანებული იქნება სხვადასხვა ინდუსტრია, მათ შორის კრიტიკული სერვისები. აქედან გამომდინარე უპირობოდ მნიშვნელოვანია სტანდარტის უსაფრთხო იმპლემენტაცია. 5G ქსელს აქვს რიგი პრობლემები, როგორც წინა სტანდარტიდან გადმოყოლილი ასევე ახალი, ცვლილებებიდან/ფუნქციონალიდან გამომდინარე წარმოქმნილი საფრთხეები. კვლევის ეს ნაწილი მოიცავს ქსელის ერთ-ერთი ყველაზე მძლავრი შეტევის - MITM ის ანალიზს მეხუთე თაობის ქსელთან მიმართებაში და შედეგად გვაჩვენებს ამ პრობლემის მოგვარების ერთ-ერთ გზას, კონცეპტუალურ მოდელს. კვლევის შედეგად მიღებული შედეგების მიხედვით, თუ წინასწარ შეაფასებს მოწყობილობა არსებული ანძების დახმარებით სამიზნე ანძის ავთენტურობას, მაშინ მნიშვნელოვნად მცირდება ცრუ ანძების პრობლემა. არსებული დიზაინს, როგორც სხვა ნებისმიერ ფუნქციონალს, აქვს თავისი სისუსტეები - მაგალითად როუმინგი, როგორც შიდა ასევე გარე ქსელში. ამ კუთხით, როგორც დამზღვევი მექანიზმი შევიმუშავეთ წინასწარ განსაზღვრული ავტორიზებული ანძების სია, რომლის ეფექტურობაც დადასტურდა ჩვენსავე ჩატარებულ ექსპერიმენტში. ბუნებრივია, ეს არ ადასტურებს ჩვენი დიზაინის სრულ ეფექტურობასა და უსაფრთხოებას. ამის მისაღწევად აუცილებელია კვლევის გაგრძელება და რეალურ სისტემაზე დატესტვა. როგორც ექსპერიმენტულმა კვლევამ აჩვენა, MITM ს გამო დიდი საფრთხის ქვეშაა LBS სერვისები. ახალი არქიტექტურიდან გამომდინარე, შესაძლებელია High-Band ზე დაკავშირების შემთხვევაში 1 ანძით დადგინდეს მოწყობილობის მდებარეობა. MITM ის გამოყენებით კი A-GPS მეთოდის დროს მდებარეობა არასწორად გამოვათვლევინოთ მოწყობილობებს, რამაც შეიძლება მნიშნელოვანი ზიანი მიაყენოს კრიტიკულ ინფრასტრუქტურას და გადაუდებელ სერვისებს. შესაბამისად, 5G სერვისის ფართო მასშტაბებისთვის მიწოდებამდე, აუცილებელია საფრთხეების შემცირება

## 6. დადასტურება/აღიარება

კვლევა PHDF-21-088 განხორციელდა შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის ფინანსური მხარდაჭერით

## ბიბლიოგრაფია

1. Huawei Technologies CO,. LTD in “5G Network Architecture – A high Level Perspective”, 2016
2. S. Asad Hussain, S. Ahmed, M. Emran, “Positioning a Mobile Subscriber in a Cellular Network System based on Signal
Strength”, IAENG International Journal of Computer Science, 34:2, IJCS_34_2_13,2007.
https://www.researchgate.net/publication/26492533

3. Qualcomm Technologies inc. “What is 5G”, in online article. https://www.qualcomm.com/5g/what-is-5g
4. M. Hanif, “5G Phones Will Drain Your Battery Faster Than You Think”, in online journal, 2020. https://www.rumblerum.com/5g-phones-drain-battery-life/
5. A. Shaik, R.Borgaonkar, S. Park, J.P. Selfert. ” New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities” in WiSec ’19: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, DOI: 10.1145/3317549, ISBN: 9781450367264, 2019.
6. Ultrasecurity, “Strom-Breaked” (Software Package), (Last access: 8.12.2021) https://github.com/ultrasecurity/Storm-Breaker
7. SK Telecom, in “5G architecture design and implementation guideline”, 2015.
8. Samsung in online report “Samsung Phone Battery Drains Quickly on 5G Service” https://www.samsung.com/us/support/troubleshooting/TSG01201462/
9. A. Purdy, “Why 5G Can Be More Secure Than 4G” in Forbes online journal, 2019. https://www.forbes.com/sites/forbestechcouncil/2019/09/23/why-5g-can-be-more-secure-than-4g/?sh=2ffcdf1657b2
10. Cell Phone Trilateration Algorithm, Online Journal “Computer Science”, 2019. (Last access: 10.12.2021) https://www.101computing.net/cell-phone-trilateration-algorithm/
11. Johhny, “How to find the Cell Id location with MCC, MNC, LAC and CellID (CID)”, 2015 https://cellidfinder.com/articles/how-to-find-cellid-location-with-mcc-mnc-lac-i-cellid-cid
12. M. Iavich, G. Akhalaia, S.Gnatyuk. Method of Improving the Security of 5G Network Architecture Concept for Energy and Other Sectors of the Critical Infrastructure, In: Zaporozhets A. (eds) Systems, Decision and Control in Energy III. Studies in Systems, Decision and Control, vol 399. Springer, Cham. https://doi.org/10.1007/978-3-030-87675-3_14,
13. M. K. Maheshwari, M.Agiwal, N. Saxena, R. Abhishek. "Flexible Beamforming in 5G Wireless for Internet of Things”, in IETE Technical Review, 36:1, 3-16, DOI: 10.1080/02564602.2017.1381048, 2017. https://doi.org/10.1080/02564602.2017.1381048
14. M. Ivezic, L. Ivezic, “5G Security & Privacy Challenges” in 5G.Security Personal Blog, 2019. https://5g.security/cyber-kinetic/5g-security-privacy-challenges/
15. Yusof, R., Khairuddin, U., and Khalid, M., ‘A New Mutation Operation for Faster Convergence in Genetic Algorithm Feature Selection’,In International Journal of Innovative Computing, Information and Control, Vol. 18, No. 10, 2012, pp 7363-7380.
16. Ibrahim S. Shehu, Olumide S, Adewale, Muhammad B.”Vehicle Theft Alert and Location Identification Using GSM, GPS and Web Technologies”, in I.J. Information Technology and Computer Sciences, 2016, 7, 1-7. Published Online July 2016 in MECS (http://www.mecs-press.org/)
17. The EU Space Programme (Last Access: 10.12.2021) https://www.euspa.europa.eu/european-space/eu-space-programme
18. Hu Z, R. Odarchenko, S. Gnatyuk “Statistical Techniques for Detecting Cyberattacks on Computer Networks Based on an Analysis of Abnormal Traffic Behavior”, in I.J. Computer Network and Information Security, 2020, 6, 1-13 Published Online December 2020 in MECS (http://www.mecs-press.org/)
19. M, Iavich, T. Kuchukhidze, S. Gnatyuk, “Novel Certification Method for Quantum Random Number Generators“, in I.J. Computer Network and Information Security, 2021, 3, 28-38 Published Online June 2021 in MECS (http://www.mecs-press.org/)
20. Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili// Novel Version of Merkle Cryptosystem// Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 4, 2017, p. 28-33
21. Giorgi Iashvili, Zhadyra Avkurova, Maksim Iavich, Madina Bauyrzhan, Avtandil Gagnidze, Sergiy Gnatyuk// Content-Based Machine Learning Approach for Hardware Vulnerabilities Identification System// International Conference on Computer Science, Engineering and Education Applications // Springer, Cham, No 23 2021, p. 117 - 126

**Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 61-72 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# კლინიკის მართვის სისტემები და უსაფრთხოება

## CLINIC MANAGEMENT SYSTEM AND SECURITY

**ლაშა შარვაშიძე; საქართველოს ტექნიკური უნივერსიტეტი**

**Lasha Sharvadze Georgian technical University**

**ABSTRACT***:* For the correct management of processes in modern medicine, as well as in all other areas, the development of electronic services is very important. We can say that it is especially important and relevant for the field of medicine, because it consists of many connected systems and components, the main goal of which is the health and life of people. This field requires maximum accuracy, correct functioning, reliability and safety of any information about the patient in relation to this type of system. In 2019, the Ministry of Health of Georgia issued orders and instructions obliging medical institutions in the country to have any type of medical record of a patient in electronic format and these records should be uploaded to the portal of the Ministry of Health of Georgia. In Georgia, state requirements for electronic processes and data are quite decentralized and include physical carriers as well. The article describes a new software inpatient module that integrates inpatient care, treatment systems, devices, portals, and medical records. The system has a web interface and is adapted to various mobile devices. The system provides security features such as password policies and user role management. The system operates in a secure network environment. Experiments have been conducted in a test environment and it has been shown that the new system increases the efficiency of61 receiving medical services and reduces service time.

**აბსტრაქტი:**პროცესების სწორი მართვისთვის თანამედროვე მედიცინაში, ისევე როგორც ყველა სხვა მიმართულებაში ელექტრონული სერვისების განვითარება ძალიან მნიშვნელოვანია. შეიძლება ითქვას, რომ მედიცინის მიმართულებისთვის ის განსაკუთრებით მნიშვნელოვანი და აქტუალურია, რადგან იგი შედგება უამრავი დაკავშირებული სისტემებისგან და კომპონენტებისგან, რომლის მთავარი მიზანი არის ადამიანების ჯანმრთელობა და სიცოცხლე. რაც ესეთი ტიპის სისტემების მიმართ მაქსიმალურ სიზუსტეს, სწორ ფუნქციენირებას, პაციენტის შესახებ ნებისმიერი ინფოს სანდოობას და უსაფრთხოებას მოითხოვს.

2019 წელს, საქართველოს ჯანდაცვის სამინისტრომ გამოსცა ბრძანებები და ინსტრუქციები, რომლითაც ქვეყანაში არსებულ სამედიცინო დაწესებულებებს გაუჩინა ვალდებულება, რომ პაციენტის ნებისმიერი ტიპის სამედიცინო ჩანაწერი იყოს ელექტრონული სახით და უნდა იტვირთებოდეს საქართველოს ჯანდაცვის სამინისტროს პორტალებზე. მაგრამ საქართველოში ელექტრონული პროცესების და მონაცემების მიმართ სახელმწიფოს მოთხოვნები საკმაოდ დეცენტრალიზირებულია და მოიცავს ასევე ფიზიკურ მატარებლებს.

სტატიაში აღწერილია ახალი პროგრამული უზრუნველყოფის სტაციონარული მოდული, რომელიც აერთიანებს სტაციონარში მოთავსებული პაციენტის მოვლა, მკურნალობის პროცესისთვის საჭირო სისტემებს, აპარატებს, პორტალებს და სამედიცინო ჩანაწერებს. სისტემას გააჩნია web ინტერფეისი და მორგებულია სხვადასხვა მობილურ მოწყობილობებზე. სისტემაში გათვალისწინებულია უსაფრთხოების ფუნქციები, ისეთები როგორც პაროლის პოლიტიკები და მომხმარებლის როლების მართვა. სისტემა მუშაობს უსაფრთხო ქსელურ გარემოში.

ჩატარებულია ექსპერიმენტები სატესტო გარემოში და ნაჩვენებია, რომ ახალი სისტემა ზრდის სამედიცინო სერვისების მიღების ეფექტურობას და ამცირებს მომსახურეობის დროს.

**Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 61-72 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

**საკვანძო სიტყვები:** უსაფრთხოება, სამედიცინო პროგრამული უზრუნველყოფა,

**KEYWORDS:** *Security, medical software, software in medicine*

## შესავალი

სამდეცინო დაწესებულების მართვა პირველ რიგში გულისხმობს, სამკურნალო დიაგნოსტიკურ პროცესებზე კონტროლის განხორციელებას. პროცესების სწორი მართვისთვის თანამედროვე მედიცინაში, ისევე როგორც ყველა სხვა მიმართულებაში ელექტრონული სერვისების განვითარება ძალიან მნიშვნელოვანია [1-4]. შეიძლება ითქვას, რომ მედიცინის მიმართულებისთვის ის განსაკუთრებით მნიშვნელოვანი და აქტუალურია, რადგან იგი შედგება უამრავი დაკავშირებული სისტემებისგან და კომპონენტებისგან, რომლის მთავარი მიზანი არის ადამიანების ჯანმრთელობა და სიცოცხლე. რაც ესეთი ტიპის სისტემების მიმართ მაქსიმალურ სიზუსტეს, სწორ ფუნქციენირებას, პაციენტის შესახებ ნებისმიერი ინფოს სანდოობას და უსაფრთხოებას მოითხოვს. უსაფრთხოების ნაწილში ერთ ერთი ყველაზე მნიშვნელოვანია, რომ ყველა მოვლენები და პროცესები უნდა ხორციელდებოდეს ისე, რომ მათი თანმიმდევრული ნახვის შესაძლებლობა გვქონდეს. სისტემაში არ უნდა იყოს ისეთი ობიექტი, ჩანაწერი, მოქმედება, ტრანზაქცია და ინფორმაციის ნახვაც კი, რომლის ლოგირებაც არ უნდა მოხდეს [5,6]. მედიცინის მიმართულებით ელექტრონული პროცესების განვითარება სულ რამოდენიმე წელია რაც დაიწყო და ჯერ კიდევ უამრავია საკვლევი და განსავითარებელი. მსოფლიოში და მათ შორის საქართველოში მედიცინის მართვის მეთოდები ძალიან დანაწევრებულია და იგი ნაწილობრივ მოიცავს ელექტრონულ პროცესებს.

ნებისმიერ სფეროში ელექტრონული პროცესების განვითარებაში ძალიან დიდი როლი აქვს სახელმწიფოს ჩართულობას და მოთხოვნებს. 2019 წელს, საქართველოს ჯანდაცვის სამინისტრომ გამოსცა ბრძანებები და ინსტრუქციები, რომლითაც ქვეყანაში არსებულ სამედიცინო დაწესებულებებს გაუჩინა ვალდებულება, რომ პაციენტის ნებისმიერი ტიპის სამედიცინო ჩანაწერი იყოს ელექტრონული სახით და უნდა იტვირთებოდეს საქართველოს ჯანდაცვის სამინისტროს პორტალებზე. მაგრამ საქართველოში ელექტრონული პროცესების და მონაცემების მიმართ სახელმწიფოს მოთხოვნები საკმაოდ დეცენტრალიზირებულია და მოიცავს ასევე ფიზიკურ მატარებლებს. რაც იმას ნიშნავს რომ ეს პროცესი არ არის ბოლომდე გამართული და კიდევ ძალიან ბევრ მუშაობს მოითხოვს, თუმცა ვფიქრობ ეს პოცესი ჩვენთან საკმაოდ სწორად ვითარდება. ამ ეტაპზე ს62ახელმწიფოს გააჩნია რამოდენიმე საკმაოდ დიდი ელ პორტალი: რეცეპტების, დაფინანსების, სამედეცინო შემთხვევების, სტაციონარული შემთხვევების, გადაუდებელი მედიცინის, მორფოლოგიური ლაბორატორიული კვლევების, კიბოს რეგისტრის და ა.შ.

## არსებული პრობლემები

მედიცინის მიმართულებით სხვა განვითარებული ქვეყნებშიც არსებობს ინფორმაციის დეცენტრალიზაციის პრობლემა და ვაწყდებით იგივე პრობლემებს, რომ ინფორმაციის ხელმისაწვდომობა არის რთული და სხვადასხვა სისტემებში, თუ მოწყობილობებში სანახავი [7,8]. ჯანდაცვის ელექტრონული პროცესების განვითარებაზე და ცენტრალიზაციის მიმართულებით ძალიან აქტიურად მუშაობენ ამერიკის შეერთებულ შტატებში, გერმანიაში, თურქეთში და იაპონიაში. სისტემების დეცენტრალიზაციის და მრავალფეროვნების გამო, ჯანდაცვის პროცესში ჩართულ სამედიცინო პერსონალს უწევს ბევრი დროის ხარჯვა სხვადასხვა სისტემების ასათვისებლად და შემდეგ ამ სისტემებში პაციენტის შესახებ ინფოს სწორ მოძიებას და გამოყენებას. თანამედროვე სამყაროში ყველაზე მნიშვნელოვანი გახდა დრო! დრო განსაკუთრებით მნიშვნელოვანია ჯანდაცვისთვის, რადგან ადამიანის ჯანმრთელობა არ/ვერ იცდის და ხშირად მოითხოვს დაუყოვნებლივ მოქმედებას, აქ შეიძლება დაკარტული თითოეული წამი და წუთი ძალიან ძვირად დაგვიჯდეს.

დაავადებების და სამედიცინო სერვისების უამრავი სახე არსებობს, რადგან მედიცინა არის საერთაშორისო და ის ჭირდება ყველას, ამიტომ იგი მარტივად გასაგები უნდა იყოს ნებისმიერ ქვეყანაში ნებისმიერ ენაზე. ამისთვის შეიქმნა საკომუნიკაციო “ენა” კოდების/კლასიფიკატორების სახით. მსოფლიოში ყველაზე ფართოდ გავრცელებულ ინსტრუმენტს პირველადი ჯანდაცვისა და საოჯახო მედიცინის კლინიკური ინფორმაციის მოსაწესრიგებლად პირველადი ჯანდაცვის საერთაშორისო კლასიფიკატორები. ძირითადად ეს მაჩვენებელები NCSP, ICD და ICPC კლასიფიკატორები განსაზღვრავენ სამედიცინო სერვისების და დიაგნოზების ერთიანი სისტემის მიხედვით აღრიცხვას, თავსებადობას და გამჭვირვალობას [9-12].ასევე არსებობს დამატებითი კლასიფიკატოები როგორიცაა, ჩივილების კლასიფიკატორები, ლაბორატორიული კლასიფიკატორები, მორფოლოგიური კლასიფიკატორები და ა.შ.

ზოგადად კლინიკური მიმართულება შედგება, შემდეგი ძირითადი ტიპებისგან: ამბულატორია - კონსულტაციები, კვლევები, დანიშნულება; დღის სტაციონარი - ისეთი ტიპის ოპერაციები, მანიპულაციები და პროცედურები, რომლის დროსაც პაციენტის კლინიკაში არ ყოვნდება 24 საათზე მეტი; სტაციონარი - ისეთი ტიპის ოპერაციები, მანიპულაციები და პროცედურები, რომლის დროსაც პაციენტის კლინიკაში ყოვნდება 24 საათზე მეტ ხანს და საჭიროებს ექიმების მეთვალყურეობის ქვეშ ინტენსიურ მკურნალობას პერიოდში; გადაუდებელი მედიცინა - არის ის მიმართულება, როდესაც პაციენტის მკურნალობა, კვლევა, ოპერაცია ხდება დაუყოვნებლივ, რადგან დრო არ იცდის და დაუყოვნებლივ უნდა გაკეთდეს ნებისმიერი საჭირო პროცედურა თუ მანიპულაცია. სამედიცინო პერსონალის გარდა კლინიკის მართვში ჩართულია ბევრი სტრუქტურული ერთეული: პერსონალის მართვა HR, მარკეტინგი, ცენტრალური აფთიაქი, სამეურნეო, ფინანსები, ბუღალერია, სამედიცინო ბილინგი, შესყიდვები, რეგისტრატურა, IT დეპარტამენტი, ინჟინერია, სტატისტიკა, ხარისხის კონტროლი და ა.შ. სამედიცინო დაწესებულების სტრუქტურა ძალიან განსხვავებული და მრავალფეროვანია. ფაქტიურად კლინიკის ყველა განყოფილება და თუ დეპარტამენტი არის ცალკე დამოუკიდებლად მდგომი ბიზნეს პროცესი, რომლებიც ერთმანეთისგან

მკვეთრად განსხვავდებიან და ასევე მჭიდრო კავშირები აქვთ. აქედან გამომდინარე მისი ერთიანი მიდგომით მართვა ფაქტიურად შეუძლებელია. ყველა ქვეყანას აქვს თავისი მიდგომები და წესები ჯანდაცვას პროცესების წარმოებასთან დაკავშრებით, მაგრამ ფაქტიურად ყველა ერთიანდება იმ აზრის და მიდგომის ქვეშ, რომ ამ ტიპის ინფორმაცია არის ძალიან პირადული და სენსიტიური, ამიტომ ესეთი ტიპის ელექტრონული მონაცემებისთვის და სისტემებისთვის ყველაზე მნიშვნელოვანი და პირველი მოთხოვნა უნდა იყოს მონაცემების უსაფრთხოება, როგორც თვითონ სისტემის შიგნით მისი მოძრაობა, ასევე მონაცემთა ბაზის, სისტემების, კავშირების და ელექტრონული გარემოს დაცვა კიბერ შეტევებისგან. საქართველოშიც და მსოფლიოშიც აუცილებელია, რომ კიდევ უფრო ინტესნიურად მოხდეს ელექტრონული სერვისების, სისტემების, ტექნოლოგიების და კიბერ უსაფრთხოების განვითარება, რადგან ადამიანების ჯანრთელობა და სიცოცხლე ყველაზე მნიშვნელოვანია და აქ მიღწეული თითოეული შედეგი, გადარჩენილი სიცოცხლე არის კაცობრიობისთვის უდიდესი მიღწევა და ნაბიჯები [13-15]. ტექნოლოგიების და ელექტრონული პროცესების განვითარება კი ყველა პროცესს ამარტივებს, აუმჯობესებს, ხდის უფრო სანდოს და ხელმისაწვდომს. გარდა სამედიცინო სერვისების და დოკუმენტაციისა სამედიცინო დაწესებულება ერთ ერთი ყველაზე დიდი და რთულად მოსაგვარებელი პროცესია, სხვადასხვა გარე სისტემებთან კავშრები, როგორიცაა: ჯანდაცვის სამინისტროს სისტემები, გადახდის სისტემები, პაციენტის პერსონალური მონაცემები, სახელწიფო სერვისები, დაფინანსება, სადაზღვეო კომპანიები, ფინანსური სერვისები, სატელეფონო ცენტრი, დისტანციური სერვისები, სტატისტიკა, cloud სერვისები და ა.შ. სამედიცინო დაწესებულებას გააჩნია დოკუმენტ ბრუნვის დიდი და რთული სტრუქტურა, რომელიც ასევე შეიძლება დაკავშირებული იყოს გარე სისტემებთან და სერვისებთან.

## ბაზრის კვლევა

საკითხის ძალიან დიდი აქტუალურობიდან, მოთხოვნიდან და საჭიროებიდან გამომდინარე 2019 წელს დავიწყეთ კვლევა. პირველ რიგში, რომ გაგვეგო რა მდგომარეობაა ამ მიმართულებით საქართველოში, შევისწავლეთ კლინიკების მართვის ადგილზე არსებული ელექტრონული სისტემები და პროგრამული უზრუნველყოფები. ამ მიმართულებით, ნამუშევარი საკმაოდ ბევრი იყო, მაგრამ აღმოვაჩინეთ, რომ საჭირო მოთხოვნებს, რომ პაციენტის ინფო და ყველა სხვა ტიპის ინფო იყოს მარტივად ხელმისაწვდომი ერთ სისიტემაში და უნდა გააჩნდეს დაცვის მაღალი დონე, ვერცერთი აკმაყოფილებდა. აღმოჩნდა, რომ ბაზარზე აქაც ისევე, როგორც საზღვარგარეთ საქმე გვაქვს მონაცემების დეცენტრალიზაციასთან და ერთ ელექტრონულ გარემოში არაა მოქცეული. კვლევის მეორე ეტაპზე დავიწყეთ დეტალურად შესწავლა სამედიცინო დაწესებულების სამუშაო პროცესში ჩართული თითოეული რგოლის თანამშრომლების სამუშაო პროცესების სრული დეტალური შესწავლა. კვლევის ეს სტილი არის საკმაოდ რთული და მოითხოვს ძალიან დიდ რესურსს და დროს, მაგრამ სხვა გამოსავალი არ იყო!

შევთანხმდით ქვეყანაში არსებულ უმსხვილეს „თოდუას კლინიკასთან“ კვლევების ჩატარების შესახებ და დავიწყეთ. კლინიკის მხრიდან ამ ინიციატივას მოყვა საკმაოდ კარგი გამოხმაურება და თვითონ სამედიცინო პერსონალის მხრიდან იყო და არის დიდი მზაობა ამ პროცესის განვითარებისთვის. მათი ჩართულობით მოვახდინეთ და ვახდენთ ჯანდაცვაში არსებული საკმაოდ ბევრი პრობლემების, ხარვეზების იდენტიფიცირებას და მათ შეძლებისდაგვარად მოგვარებას. როგორც ზემოთ ავღნიშნეთ, ქვეყანაში ძალიან დიდი როლი აქვს სახელმწიფოს ჩართულობას ელექტრონული პროცესების განვითარებაში, შესაბამისად მუდმივ რეჟიმში ვაწარმოებთ კვლევის ირგვლის კოსულტაციებს ჯანდავცის სამინისტროს სხვადასხვა სტრუქტურებთან თანამშრომლობით, ასევე კვლევის პროცესში ხდება საზღვარგარეთ არსებული გამოცდილების, სისტემების და პროგრამების შესწავლა. ყველგან გვხვდება ინფოს დეცენტრალიზაცია, რადგან ჩვენ საქმე გვაქვს ბევრი ცალკე მდგომი განსხვავებული სისტემებთან, მოდულებთან, პორტალებთან, აპარატებთან, მატარებლებთან და აგრეთვე ხშირ შემთხვევაში ფურცელ მატარებელთან. საკმაოდ დიდი ნაწილი ფიზიკურ ფურცელ, CD, USB და სხვა მატარებელზე ინახება დროებით. მათი ერთ სისტემაში მოქცევა საკმაოდ რთული პროცესია, რადგან არსებობს უამრავი სამედიცინო აპარატურა, რომელიც თავისთვის დამოუკიდებლად მუშაობს, გააჩნია თავისი გასაკუთრებული საკომუნიკაციო საშუალებები, არხები, ფორმატები და ენები, რომლებიც ერთმანეთისგან მკვეთრად განსხვავდებიან და საერთოდ სხვადასხვა სტრუქტურის მონაცემებთან გვაქვს საქმე. პაციენტის კვლევის, მკურნალობის პროცესში, ექიმისთვის ერთ ერთი ყველაზე მნიშვნელოვანი, ძვირადღირებული, რთული და განსხვავებული სტრუქტურის მქონე პაციენტის ელექტრონული მონაცემები არის რადიოლოგიური კვლევები, რომელიც საკმაოდ დიდი მოცულობისაა, გააჩნია საერთოდ განსხვავებული სტრუქტურა (DICOM format image,HL7), განსხვავებული მონაცემები, რომელიც რადიოლოგიური კვლების აპარატის და ექიმი რადიოლოგის ჰიბრიდია. ასევე თანამედროვე სისტემებში ამ პროცესში უკვე ბევრგან მონაწილეობს, ამ ეტაპზე მცირე შესაძლებლობების მქონე, მაგრამ ძალიან საჭირო და ზუსტი ხელოვნული ინტელექტის ელემენტები, რომელიც ავტომატურ რეჟიმში ახდენს თითოეული პიქსელი გაანალიზებას და წინა კვლევებთან შედარებით მიმდინარე ცვლილებების, გადახრების აღმოჩენას. რადიოლოგია მოიცავს უამრავ მიმდინარეობას და ამ მიმდინარეობებს შორისაც არის რადიკალური სტრუქტურული და ფორმატის სხვაობები. ზოგადად ყველა რადიოლოგიურ აპარატს აქვს თავისი მცირე ინფორმაციის საცავი, რომელიც მხოლოდ ერთჯერადად ჩატარებული კვლევის დროს არის ხელმისაწვდომი.

პაციენტის მკურნალობის პროცესის განუყოფელი ნაწილია ლაბორატორიული კვლევების მონაცემები. ეს არის სამყარო, სადაც შეხვდებით უამრავ ძალიან განსხვავებული სტრუტურის და შინაარსის მქონე აპარატურას, ავტომატურ სისტემებს, ნახევრად ავტომატურ სისტემებს, მოდულებს, მიკროსკოპებს, ლაბორანტებს და ა.შ. მათი სტრუქტურა იმდენად განსხვავებულია, რომ აქაც საქმე გვაქვს მონაცემების სხვადასხვა განსხვავებულ სისტემებში გაშლასთან, დეცენტრალიზაციასთან, რაც პროცესს საკმაოდ აფერხებს და ერთ ერთ ყველაზე საჭირო ინფორმაციაზე წვდომას ართულებს. ინფოს ესეთი ტიპის

გაშლა სხვადასხვა სისტემებში ართულებს და აძვირებს მათ უსაფრთხოებას. ხშირ შემთხვევებში უსაფრთხოების ნაწილი უგულებელყოფილია და სასიცოცხლოდ მნიშვნელოვანი, საჭირო ინფორმაცია არის რთულად წვდომადი, ხშირ შემთხვევებში იკარგება ან ჰაკერების მსხვერპლი ხდება. ასევე უსაფრთხოების ნაწილში ერთ ერთი ყველაზე მნიშვნელოვანია, რომ ყველა მოვლენები და პროცესები უნდა ხორციელდებოდეს ისე, რომ მათი თანმიმდევრული ნახვის შესაძლებლობა გვქონდეს. სისტემაში არ უნდა იყოს ისეთი ობიექტი, ჩანაწერი, მოქმედება, ტრანზაქცია და ინფორმაციის ნახვაც კი, რომლის ლოგირებაც არ უნდა მოხდეს.

კლინიკის ყველა სამუშაო პროცესი შევისწავლეთ ძალიან დეტალურად და ვაგრძელებთ ამ მიმართულებით მუშაობას, პროცესში ფაქტობრივად ყველა თანამშრომელი ჩავრთეთ. ასევე კვლევის პროცესში წამოვიღეთ უამრავი რეკომენდაციები და სურვილები. კვლევის შედეგებიდან იკვეთება, რომ საჭიროა ერთიანი, დიდი Enterprise - ის შექმნა, რომელშიც შეძლებიდაგვარად გაერთიანდება ყველა საჭრო დაკავშირებული სისტემა, აპარატურა, პროგრამული უზრუნველყოფა, პორტალი თუ მოდული, რომელიც საჭიროა კლინიკის პროცესების მართვისთვის.

## შეთავაზებული მეთოდოლოგია

იმის გამო, რომ მედიცინაში პროცესების დიდი ნაწილი არის დეცენტრალიზირებული და პროცესში ჩართულ ყველა რგოლს უწევს სხვადასხვა სისტემებში, პროგრამებში, აპარატურაში და ფურცელ მატარებელზეც კი, ინფოს ძიება, გამიკვეთა ძირითადი მიდგომა და პრობლემა, რომ სისტემა უნდა იყოს მაქსიმალურად “ერთი ფანჯრის პრინციპის”, “User Friendly” ყველა ტიპის ინფო მათ შორის პაციენტის შესახებ ყველა ჩანაწერის ნახვა უნდა იყოს შესაძლებელი ერთ ფანჯარაში. პაცინეტის ანამნეზი (ისტორია) უნდა იყოს თანმიმდევრული, მარტივად გასაგები, უნდა მოიცავდეს ყველას საჭირო ინფოს და მისი სანდოობის ხარისხი უნდა იყოს ძალიან მაღალი. პაციენტის ანამნეზი შედგება ყველა ზევით ხსენებული სისტემებიდან მოპოვებული მონაცემებისგან და მათი სწორი განაწილებისგან. ქვეყანაში არსებული ყველა სამედიცინო დაწესებულება, ძირითადად, არასრული სხვადასხვა ტიპის პროგრამული უზრუნველყოფით იმართებოდა და იმართება. პროცესების საკმაოდ დიდი ნაწილი კვლავ ფურცელზე იწერება. ამ სფეროში საჭირო და არსებული სისტემები ცალკე მდგომ სისტემებად გვაქვს წარმოდგენილი. განსხვავებული პროგრამების, მოდულების, აპარატების და მატარებლების სახით. აქედან გამომდინარე გამოკვეთილი ძირითადი კრიტერიუმები არის, მართვის და ადმინისტრირების ყველა პროცესის ელექტრონულად გადაყვანა, სამედიცინო ფორმების და პროცესების ელექტრონიზაცია/ავტომატიზაცია, მთლიანი სისტემის შეძლებისდაგვარად ავტომატიზაცია, დაკავშირება/ინტეგრაცია ყველა შესაძლო გარე პორტალსა და სტრუქტურასთან. კლინიკის მართვის ერთ ერთი ძალიან მნიშვნელოვანი ნაწილია კლინიკის შიგნით პაციენტებზე მედიკამენტების სახარჯი მასალების ხარჯვის და მოძრაობის ნაწილი, რომელსაც გააჩნია მკაცრი აღრიცხვა და კონტროლი ჯანდაცვის სამინისტროს მხრიდან, რადგან აქ საქმე გვაქვს ისეთი

ტიპის ნივთიერებებთან და მედიკამენტებთან, როგორიცაა მაგალითად: ნარკოტიკული და სანარკოზე საშუალებები, რადიაციული ფარმ პრეპარატები, რეაგენტები, რომლებსაც სჭირდება სპეციალური ნებართვები და რეცეპტები.

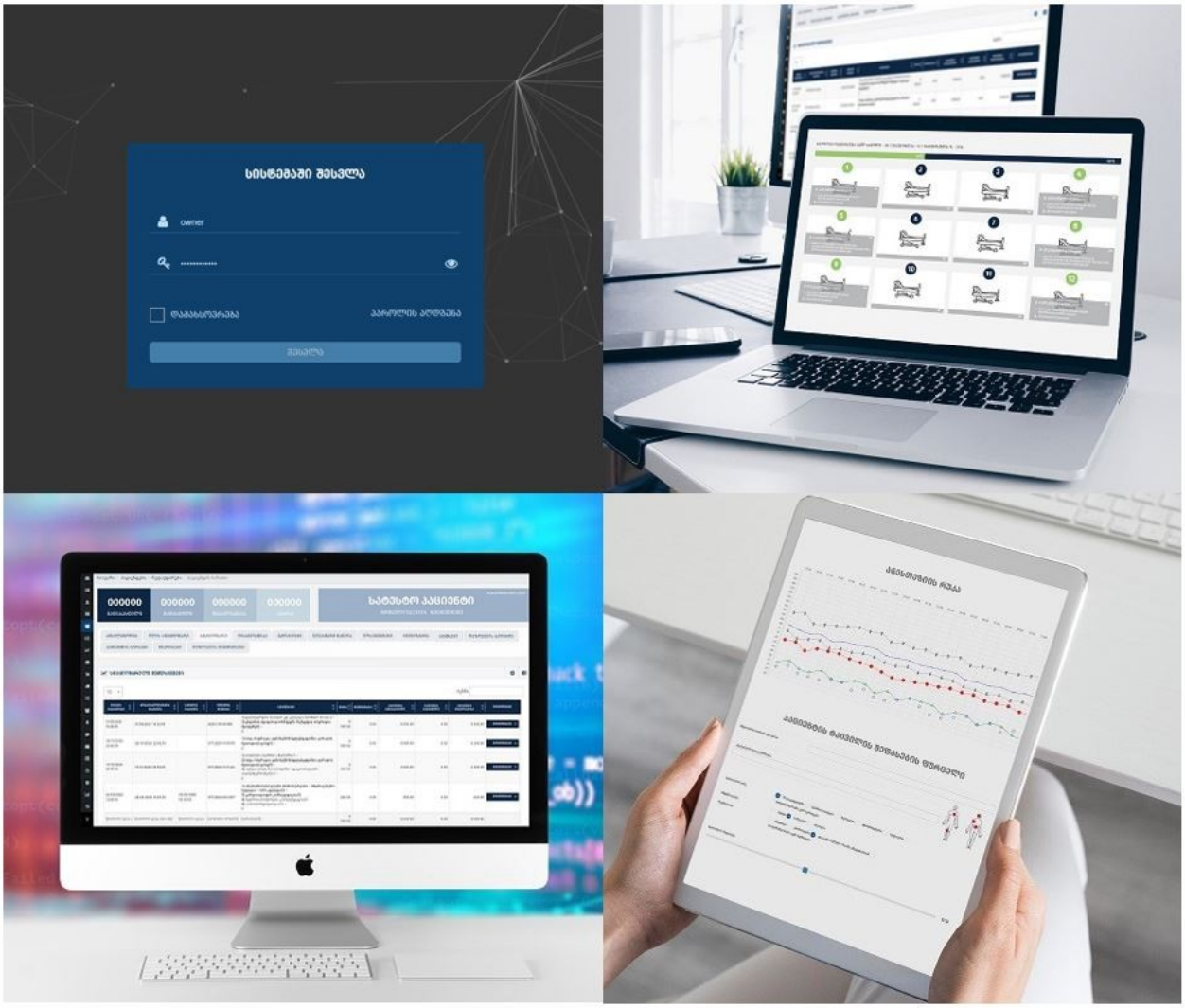
ესეთი ტიპის მედიკამენტების აღრიცხვის პროცესში ჯერ კიდევ გვხვდება საკანონმდებლო მოთხოვნებში, რომ მკაცრი აღრიცხვა უნდა ხორციელდებოდეს ძალიან დეტალურად, მისი ყოველი მოძრაობა/ხარჯვა უნდა იყოს აღრიცხული დაუყოვნებლივ, წუთების სიზუსტით. კანონი გვავალდებულებს ესეთი ტიპის მედიკამენტების მოძრაობა/ხარჯვის დოკუმენტი იყოს ფურცელ მატარებელზე და სველი ხელმოწერით შესრულებული. ასევე უნდა აღირიცხოს კონკრეტულ პაციენტს, რატომ, როდის დაენიშნა ეს პრეპარატი და როდის მოხდა ამ პრეპარატების მიღება. პროცესების კრიტიკულობიდან და მნიშვნელობიდან გამომდინარე კლინიკის მენეჯმენტს უნდა ქონდეს შესაძლებლობა „LIVE" რეჟიმში დაათვალიეროს, დააკვირდეს ყველა სახის ინფორმაციას და პროცესს. ასევე ექიმებს „LIVE" რეჟიმში უნდა ქონდეთ წვდომა ისეთ მონაცემებზე, როგორიცაა: კომპიუტერული და მაგნიტურ-რეზონანსული ტომოგრაფია, რენტგენი, ლაბორატორია, მორფოლოგია, პაციენტის სრული ანამნეზი: დიაგნოზი, დანიშნულება, ჩატარებული მკურნალობები, მანიპულაციები, ოპერაციები და სტატისტიკური მონაცემები.

ესეთი ტიპის მონაცემების გამოყენება ასევე მოხდება სამეცნიერო, საგანმანათლებლო მიზნებისთვის. მაგალითად, რეზიდენტების მომზადების პროცესისთვის, ასევე, როდესაც ექიმი ამზადებს პუბლიკაციას საერთაშორისო გამომცემლობის ან კონფერენციისთვის, ძალიან მარტივად შეუძლია, რომ სისტემაში იპოვოს მისთვის საჭირო ინფორმაცია და მასზე დაყრნობით მოამზადოს შესაბამისი მასალა და გააზიაროს გამოცდილება. ელექტრონულად დაკავშირებული სერვისებისა და ავტომატიზაციის ხარჯზე, ესეთი ტიპის Enterprise გაამარტივებს ექიმების სამუშაო პროცესს. ექიმისთვის პაციენტის სრული ანამნეზის ნახვა უნდა გახდეს მარტივად შესაძლებელი, ერთ ფანჯარაში, რაც პაციენტის მკურნალობის პროცესს უფრო სწრაფს და ეფექტიანს ხდის. მკურნალ ექიმს საშუალება უნდა ქონდეს პაციენტს დინამიკაში დააკვირდეს, უფრო მეტი ინფორმაცია დააგენერიროს და მის ირგვლივ სხვადასხვა დროს განხორციელებული კვლევებისა თუ კონსულტაციების შედეგები ერთდროულად, მარტივად ნახოს. პაციენტებისთვის კი გამარტივდება კლინიკის სერვისებით სარგებლობა: რეგისტრაცია, ექიმთან ვიზიტზე ჩაწერა, კვლევების პასუხების ელექტრონულად მიღება, დისტანციური საკომუნიკაციო არხების (SMS, mail, call, cloud) საშუალებით და რაც ყველაზე მნიშვნელობანია ექიმს ექნება უფრო მეტი ბერკეტი, დრო და შესაძლებლობა პაციენტის მკურნალობის პროცესის უკეთესად სამართავად. თუ მოვახდენთ ამ ყველაფერმა ერთ სისტემაში რეალიზებას, ექიმებს და პაციენტებს გაუჩნდებათ შესაძლებლობა, რომ სამედიცინო სერვისების მიღება უფრო სწრაფი, მარტივი და მოქნილი გახდეს. კლინიკის მართვის პროცესიც საგრძნობლად გაუმჯობესდება, რადგან ელექტრონულმა და ავტომატიზებულმა პროცესებმა უნდა შეამციროს პაციენტის მომსახურების დრო, გაჩნდება დეტალური რეპორტინგი ყველა მიმართულებით, რაც კლინიკის მართვას უფრო ეფექტურსა და მოქნილს

გახდის. ავტომატიზაციის ხარჯზე გაუმჯობესდება თანამშრომლების სამუშაო პროცესიც. კვლევებმა გვაჩვენა, რომ ჯანდაცვისთვის ერთ ერთი ძალიან მნიშვნელოვანი და საჭირო ტექნოლოგია აღმოჩნდა QR კოდები.

სტაციონარიზირებული პაციენტი საჭიროებს განსაკუთრებულ მოვლას და მეთვალყურეობას, ამ პროცესში ერთდროულად არის ჩართული რამოდენიმე სამედიცინო რგოლი (მკურნალი ექიმები, ქირურგები, რეანიმატოლოგები, ექთანები და ა.შ) ამ პროცესში სამედიცინო პერსონალს მუდმივ რეჟიმში უწევს პაციენტების მონახულება ადგილზე პალატაში თუ ინტენსიურ თერაპიაში. იქვე გასინჯვა, მონიტორინგი, დანიშნულება, პროცედურა, მანიპულაცია და ა.შ. ესეთ პირობებში კი რთულია ადამიანმა დაიმახსოვროს ყველა პაციენტის მდგომარეობა და ისტორია, ასევე რთულია ინფორმაცია პალატიდან სრულად მოახვედრო ელექტრონულ სისტემაში, ამიტომ პროცესი ითხოვდა ადგილზე პალატაში პაციენტის ანამნეზზე წვდომას და ჩანაწერის გაკეთების შესაძლებლობას. ამ საჭიროებებიდან გამომდინარე 2020 წელს, პირველად ქართულ მედიცინაში, ერთერთ უმსხვილეს კლინიკაში დავნერგეთ და ვანვითარებთ, სტაციონარული პაციენტების მართვის მოდულს (ნახ.1). შევქმენით პლანშეტზე სრულად ადაპტირებული სტაციონარის მოდული, რომელიც თავის თავში აერთიანებს ჰოსპიტალიზირებული პაციენტის მართვის სრულ პროცესს და მონაცემებს. იგი დაკავშირებული და ინფორმაციას ავტომატურ რეჟიმში აგროვებს კლინიკის შიგნით არსებული სხვადასხვა დეცენტრალიზირებული სისტემებიდან, აპარატებიდან სტაციონარიზირებული პაციეტნის მკურნალობის შესახებ ყველა ჩანაწერს და ერთ სივრცეში აერთიანებს. სტაციონარში მოთავსებულ პაციენტს ხელზე უკეთდება სპეციალური სამაჯური, რომელზეც დატანილია QR კოდი. ექიმის ან ექთნის მიერ ამ კოდის პლანშეტით დასკანერების შემთხვევაში იხსნება პაციენტის ისტორია, დანიშნულება, ფიზიკალური მონაცემები, კურსუსები და სხვა ყველა საჭირო მონაცემი. თავის მხრივ, ექიმი ან/და ექთანი მარტივად, პლანშეტზე ახდენს პაციენტის შესახებ საჭირო ჩანაწერის გაკეთებას. ესეთი ტიპის სისტემის შექმნამ და ისეთ მარტივ გადასატან ტექნიკასთან ადაპტირებამ, როგორიცაა პლანშეტი და მობილური ტელეფონი, საგრძნობლად გაამარტივა და სწრაფი გახადა სტაციონარში პაციენტების მონიტორინგის და მკურნალობის პროცესი.

(ნახ.1)




## ექსპერიმენტები

ექსპერიმენტები ჩატარდა სატესტო გარემოში. ჯერ დავთვალეთ არსებულ დეცენტრალიზირებულ გარემოში პაციენტის რეგისტრაციის დრო. გამოიკვეთა, რომ რეგისტრაციას დაჭირდა 5-7 წუთი, ხოლო შემდეგ კლინიკის იგივე რეგისტრატორების ნაწილი დავსვით ახალ სატესტო გარემოში სამუშაოდ და დავთვალეთ იგივე პროცესის შესრულების დრო, საშუალოდ გამოვიდა 1-3 წუთი.

ექსპერიმენტის საფუძველზე გამოვლინდა რომ პაციენტის რეგისტრაციის დრო შემცირდა უკეთეს შემთხვევაში 5 ჯერ. რადგან პროცესები იყო გაფანტული სხვადასხვა პროგრამებში და შესაბამისად საჭირო იყო ყველა სისტემაში პაციენტის სათითაოდ რეგისტრაცია. ამ ეტაპზე პაციენტი რეგისტრირდება ერთ სისტემაში, რადგან მოვახდინეთ ამ სისტემების მოდულებად დაშლა და შემდეგ

გაერთიანება. სამედიცინო პერსონალისთვისაც 6 ჯერ შემცირდა პაციენტის ისტორიის ნახვის და ჩანაწერის გაკეთების შესაძლებლობა.

## დასკვნა

ახალი სტაციონარის მოდულის დანერგვამ და რეალურ გარემოში რეალიზებამ გაზარდა სტაციონარული სამედიცინო სერვისების მიღების ეფექტურობა. პაციენტის ანამნეზის ერთ სისტემაში მოქცევამ გაზარდა ინფორმაციის სანდოობა, სიზუსტე და ამ ინფორმაციაზე წვდომა. ყველაზე მნიშვნელოვანი რაც მოგვცა ეს არის შემცირებული დრო, პაციენტის მდგომარეობის შესახებ უფრო სწორი და ზუსტი ანალიზის შესაძლებლობა. პროგრამის web ინტერფეისმა და სხვადასხვა მობილურ მოწყობილობებთან თავსებადობამ, სტაციონარიზირებული პაციენტის მკურნალ ექიმს მისცა შესაძლებლობა დისტანციურად მართოს პაციენტის მკურნალობის და მდგომარეობის მიმდინარეობის უმეტესობა, რადგან სტაციონარიზირებული პაციენტის მოვლა, მკურნალობის პროცესში ჩართულია ბევრი მოწყობილობა და სამედიცინო რგოლი: მკურნალი ექიმი, ქირურგი, ასისტენტი, ანესთეზიოლოგი, საოპერაციო მედდა, ექთანი, რომლებიც ახდენენ პროგრამაში პაციენტის შესახებ შესაბამისი ინფორმაციის შეყვანას და მონიტორინგს.

სისტემების ცენტრალიზებამ და ერთ სამუშაო პროგრამაში გაერთიანებამ მოგვცა შესაძლებლობა, რომ პროგრამის მომხმარებლების როლები ვმართოთ უსაფრთხოდ და ისეთ სენსიტიურ ინფორმაციაზე წვდომა, რომელიც ეხება პაციენტის ჯანმრთელობას იყოს მაქსიმალურად შეზღუდული. პროგრამაში გათვალისწინებულია პაროლების პოლიტიკა და პროგრამა მუშაობს უსაფრთხო ქსელურ გარემოში

სისტემა მუდმივ რეჟიმში ვითარდება და ფართოვდება. სამედიცინო პერსონალთან ინტენსიურად მიმდინარეობს ამ პროექტის კვლევა, განვითარება და ოპტიმიზაცია. ამ ეტაპისთვის ზემოთხსენებული სისტემის განახლება/ოპტიმიზაცია მოხდა 3 ჯერ და კვლავ ვაგრძელებთ კვლევას, სიახლეების დანერგვას და სისტემის გაფართოებას ამ მიმართულებით.

გამოყენებული ლიტერატურა:

1. RODNAN, GERALD P. M.D.; MYEROWITZ, RICHARD L. M.D.; JUSTH, GERALD O. M.D.2 Morphologic Changes in the Digital Arteries of Patients with Progressive Systemic Sclerosis (Scleroderma) and Raynaud Phenomenon, Medicine: November 1980 - Volume 59 - Issue 6 - p 393-408

2. John Eng, William K. Mysko, Gregory E. R. Weller, Regis Renard, Joseph N. Gitlin, David A. Bluemke, Donna Magid, Gabor D. Kelen, and William W. Scott, Jr.

American Journal of Roentgenology 2000 175:5, 1233-1238

3. Perc M., Hojnik J. (2022) Social and Legal Considerations for Artificial Intelligence in Medicine. In: Lidströmer N., Ashrafian H. (eds) Artificial Intelligence in Medicine. Springer, Cham. https://doi.org/10.1007/978-3-030-64573-1_266

4. Ting, D.S.W., Carin, L., Dzau, V. et al. Digital technology and COVID-19. Nat Med 26, 459–461 (2020). https://doi.org/10.1038/s41591-020-0824-5

5. Mishra, D., Mukhopadhyay, S., Kumari, S. et al. Security Enhancement of a Biometric based Authentication Scheme for Telecare Medicine Information Systems with Nonce. J Med Syst 38, 41 (2014). https://doi.org/10.1007/s10916-014-0041-1

6. Arshad, H., Teymoori, V., Nikooghadam, M. et al. On the Security of a Two-Factor Authentication and Key Agreement Scheme for Telecare Medicine Information Systems. J Med Syst 39, 76 (2015). https://doi.org/10.1007/s10916-015-0259-6

7. de Cruppé, W., Malik, M. & Geraedts, M. Minimum volume standards in German hospitals: do they get along with procedure centralization? A retrospective longitudinal data analysis. BMC Health Serv Res 15, 279 (2015). https://doi.org/10.1186/s12913-015-0944-7

8. Haeckel, R. and Fink, R C.. "Does Point-of-Care Testing Reverse Centralization in Laboratory Medicine?." LaboratoriumsMedizin / Journal of Laboratory Medicine, vol. 23, no. 1, 1999, pp. 39-49. https://doi.org/10.1515/labm.1999.23.1.39

9. Keun-Young Yoo, Cancer Control Activities in the Republic of Korea, Japanese Journal of Clinical Oncology, Volume 38, Issue 5, May 2008, Pages 327–333, https://doi.org/10.1093/jjco/hyn026

10. IM Hofmans-Okkes, H Lamberts, The International Classification of Primary Care (ICPC): new applications in research and computer-based patient records in family practice, Family Practice, Volume 13, Issue 3, 1996, Pages 294–302, https://doi.org/10.1093/fampra/13.3.294

11. M WOOD, H LAMBERTS, JS MEIJER, I M HOFMANS-OKKES, The Conversion Between ICPC and ICD-10. Requirements for a Family of Classification Systems in the Next Decade, Family Practice, Volume 9, Issue 3, September 1992, Pages 340–348, https://doi.org/10.1093/fampra/9.3.340

12. Charity, M.J., French, S.D., Forsdike, K. et al. Extending ICPC-2 PLUS terminology to develop a classification system specific for the study of chiropractic encounters. Chiropr Man Therap 21, 4 (2013). https://doi.org/10.1186/2045-709X-21-4

13. Iavich, M.; Gnatyuk, S.; Fesenko, G. Cyber security european standards in business. Sci. Pract. Cyber Secur. J. 2019, 3, 36–39.

14. Andrusiak, N., Kraus, N., Savchenko, A., Iavich, M. (2019), Practices of Using Blockchain Technology in ICT under the Digitalization of the World Economy. Proceedings of the International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019) co-located with 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks. Lviv, Ukraine, November 29. URL: http://ceurws.org/Vol-2588/paper8.pdf. P. 80–89.

15. A. Gatouillat, Y. Badr, B. Massot and E. Sejdić, "Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine," in IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3810-3822, Oct. 2018, doi: 10.1109/JIOT.2018.2849014.