ELEKTROTEHNIŠKI VESTNIK 92(3): 104-114, 2025
ORIGINAL SCIENTIFIC PAPER

Risk Assessment and Mitigation of Information Security Threats in 5G Networks

Ivan A. Smirnov, Yevgeni Koucheryavy

HSE Tikhonov Moscow Institute of Electronics and Mathematics, Moscow, Russia
E-mail: i.smirnov@hse.ru

Abstract. The 5G communication networks have been destined to become one of the pillars of the digital economy, driven by artificial intelligence (AI), machine learning (ML), Big Data, Internet of Things (IoT) and robotization. The 5G networks have inherited many vulnerabilities from the preceding systems. In this regard, the issue of a proper information security (IS) is one of the highest priorities. Our aim is to assess the risks of realizing some IS threats in 5G wireless networks and propose security measures to mitigate them. In particular, we analyze vulnerabilities for the 5G networks related to the user device (UE), wireless interface (Air Interface), core network (CN), application server, open-source applications, AI, physical layer threats, threats from a poorly secured 4G/LTE network, SDN security related to vulnerabilities in SSH using various attacks such as Terrapin attack, as well as regulatory requirements. We propose measures to reduce by some 16% the threat probabilities and their impacts benefitting from ISPs and telecoms to avoid problems related to the data availability, leakage and compromise.

Keywords: IMT-2020, 5G, wireless technologies, technical specification, information security, CASE.

Ocena tveganj in omilitveni ukrepi proti grožnjam informacijski varnosti v omrežjih 5G

Komunikacijska omrežja 5G so temeljni steber digitalnega gospodarstva, ki ga poganjajo umetna inteligenca, strojno učenje, veliki podatki, internet stvari in robotizacija. Omrežja 5G so podedovala številne ranljivosti od prejšnjih sistemov, zato je vprašanje ustrezne informacijske varnosti (IV) ena izmed najvišjih prioritet. Naš cilj je oceniti tveganja uresničitve določenih groženj IV v brezžičnih omrežjih 5G in predlagati varnostne ukrepe za njihovo omilitev.
Posebej analiziramo ranljivosti v omrežjih 5G, povezane z uporabniško napravo, brezžičnim vmesnikom, osrednjim omrežjem, aplikacijskimi strežniki, odprtokodnimi aplikacijami, umetno inteligenco, grožnjami na fizičnem nivoju, grožnjami zaradi slabo zavarovanih omrežij 4G/LTE, varnostjo programsko definiranih omrežij ter zakonodajnimi zahtevami. Predlagamo ukrepe, s katerimi bi verjetnosti in vplive groženj zmanjšali za okoli 16 %, da bi se ponudniki internetnih storitev in telekomunikacijska podjetja izognili težavam, povezanim z razpoložljivostjo podatkov, njihovim uhajanjem ali kompromitiranjem.

1 INTRODUCTION

Information plays a key role in daily life of a person. Provision of services to ensure information exchange is carried out by providers and telecom operators with appropriate technologies developed in accordance with international standards, which have their own features in the speed of data transmission and its security. Today, the secure information exchange is the most difficult and urgent task not only for providers, but also for users of this service. This is due to the annual increase in the number of cyberattacks against individuals and legal entities, with the aim of financial and material enrichment. However, not all existing and working standards of wireless networks can provide information security against modern cyber threats. It is generally believed that the 5G network is able to provide a reliable and secure information exchange at an appropriate level [1].

Despite the prevailing 3G and 4G/LTE technologies, the world moves to a wide deployment of 5G [2]. This is due to the growing number of subscribers, the number of devices these subscribers have, the speed of the provided information and a lot of other factors. It is worth noting that the 5G network was originally developed for the high-performance Internet of Things (IoT), allowing operators to help their corporate clients automate business processes in manufacturing, construction, logistics, and other areas. Thus, industry companies are showing great interest in 5G, trying to find and implement their business inflection points by leveraging advanced radio communication standards, cloud development in wireless networks, artificial intelligence (AI) and machine learning (ML), robotization, etc.

With the emergence of new technologies, new attack vectors and vulnerabilities in developed and implemented solutions have appeared. The new 5G network architecture is markedly different from the

Received: 16 November 2024
Accepted: 2 April 2025

architectures of previous generations of mobile networks due to new security requirements. However, against the background of a number of advantages of the technology itself, attackers will make every effort to find backdoors and zero-day vulnerabilities to attack critical infrastructure objects (hereinafter referred to as CII).

An example of such attacks on CII can be seen in a study conducted by the European Union Cybersecurity Agency (hereafter ENISIA) [3] which reveals that between January 2022 and August 2023 there were 310 confirmed DoS incidents. 46% per cent of them were in the public administration sector. The most sensitive ones were:

•25 August 2023 – attack on the Polish railway, resulting in disruption of the train emergency stopping mechanisms;

•7 June 2023 – attack on the AZURE Microsoft cloud services led to a service degradation and minor outages;

•February 2023 – attack on the AKAMAI Technologies;

•30 January 2023 – attack on the US civilian healthcare providers;

•24 February 2024 – attack on the international satellite provider KA-SAT, enabling attackers to control satellite modems that provide Internet access. This attack affected over 5,000 wind turbines in Germany that used the KA-SAT network to transmit data for maintenance and upgrades (the ENISA threat landscape for DOS attacks, 2023).

In order to avoid such incidents or minimize their consequences as much as possible, it is customary to conduct a risk assessment. The problems of the 5G risk assessment have been addressed in such works as "Security Risk Assessment for the 5G Networks: National Perspective" [4] and "Power 5G Hybrid Networking and Security Risk Analysis" [5]. Despite the weighty scientific contribution and research work done by the authors of these papers, the effectiveness of the measures they propose is difficult to assess, which suggests that the results are not applicable to a wide range of small and medium-sized businesses, the reasons are as follow

• [4] provides a lot of hope for risk mitigation on the regulator, but in practice it is a very long and labor-intensive process, because at the state level it is first necessary to develop, agree and approve regulatory documents, mechanisms for compliance and control for the legislative, executive and judicial branches of government. And while this process is being developed by regulators, different companies will build their defense mechanisms in different ways within the existing legal framework, their competences and awareness in the field of IS, which will be successfully used by attackers.

• [5] focuses on business risks and conduct risk assessment of the power 5G hybrid networking, which is of great interest for modern business. It proposes solutions for mitigating these risks to enable business to take measures to avoid them

.

2 Materials and Methods

Understanding the existing problems, our aim is to assess and mitigate the risks of realizing some IS threats in 5G wireless networks. To solve the task we apply scientific methods of research and theoretical synthesis, according to which we review and analyze the 5G architecture, analyze the threats and propose measures to reduce them, assess the risks and evaluate the quality of the proposed risk mitigation measures. For the risk assessment we use the CASE-methodology, which we will consider in Part 4.

For the 5G wireless network, be to secure the its architecture should be studied from an IS perspective in order to avoid the risks of implementing IS threats during its operation [6, 7]. In the paper, the general architecture of 5G/IMT-2020 is considered, it is based on the sources [8; 9; 10; 11; 12] and shown in Fig.1

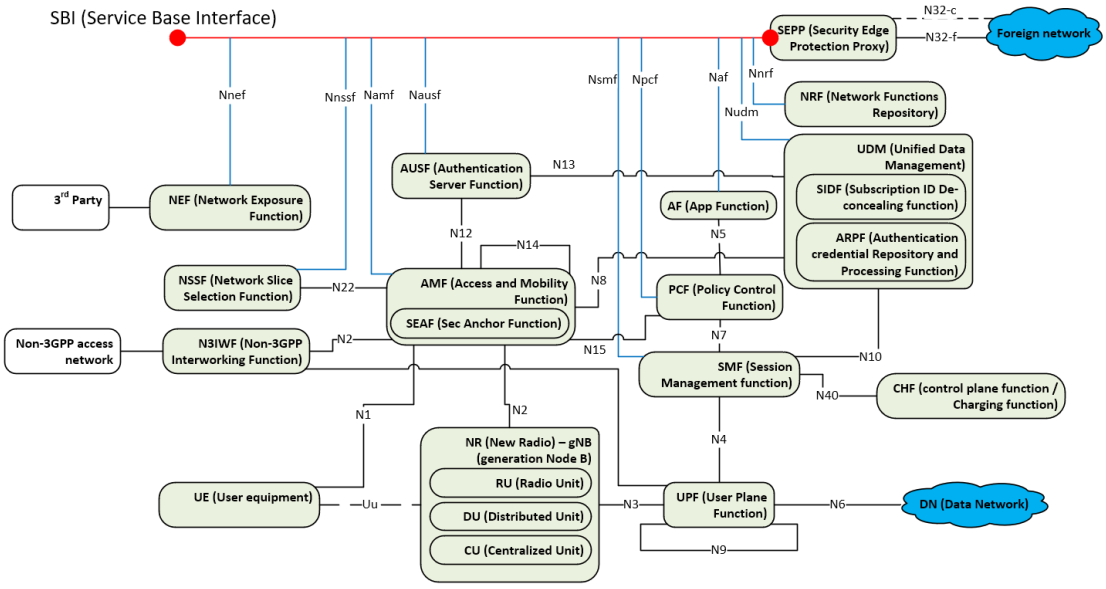

Figure 1. 5G/IMT-2020 architecture (created by authors)

Table 1. Description of the 5G/IMT-2020 network elements (created by the authors)

No	Description
1	**UE** - user equipment. Phone, smartphone, tablet, IoT and others. **Stores and/or processes data:** • **USIM**: Subscriber ID, Auth key, Encryption key, Subscriber info, Administrative data, Temp network data, Serv-related data, App data, Personal data, Master key K, SQN (Sequence Number) • **UE**: IMEI (International Mobile Station Equipment ID), RAI (Routing area ID), Users SGSN, TTL1 (Temporary Local Link ID), Radio Priority SMS, PDP context (Package data protocol), MM state, Cell ID, IMEISV (International Mobile equipment ID and Software ver), Classmark, Ciphering algorithm. **Security measures:** Advanced encryption algorithms, strong authentication procedures and protection against various threats ensure a secure and reliable connection. **Functions**: All possible functions of user equipment.
2	**gNB (Generation NodeB) / NR (Radio Network)** - a node in a cellular network which provides communication between the UE and the evolved packet core (EPC). May contain subsystems: • **RU (radio unit)** - radio node. • **DU (distributed unit)** - distributed node - supports one or more cells. • **CU (Centralised Unit)** - a logical node that controls the operation of one or more gNB-DUs. The gNB-CU completes the F1 interface associated with the gNB-DU. **Stores and/or processes data:** BSIC (Base Transceiver ID Code), LAI (Local Area Identifier), CI (Cell ID) **Functions**: RRM (Radio Resource Management), Charging, Mobility Management, Access Control, Scheduling and Measurement Configuration, Security Functions, QoS (Quality of Service), Connection Management.
3	**NRF (Network function repository)** - Network function repository provides a centralised repository of information about available network functions, their capabilities and network fragments. **Security measures**: Participates in secure interaction with NFs (Network Function) during registration and information retrieval. Screening function to whitelist/blacklist incoming NF management traffic; access token authorisation to whitelist access token requests based on NF types; authentication of NFs via TLS; supports service mesh integration that intercepts all network communications between microservices; integrated with Oracle Communications Certificate Manager (OCCM), offloading the certificate management task to OCCM; provides an NF screening function that provides additional security by restricting NFs that can use the NRF service; e.g., NFs are not allowed to use the NRF service. **Functions**: Detect and register NFs, maintain information about NF capabilities (supported features and network fragment availability).
4	**UPF (User Plane Function)** - User Plane Function is used as a functional point between the mobile network and the data network (DN). It is responsible for managing data traffic on the user plane, ensuring efficient routing and providing different services with different QoS requirements. **Security measures:** traffic inspection, data encryption **Functions:** Interfacing with external data networks, including to the global Internet; Routing user packets; Marking packets according to QoS policies; Diagnosing user packets; Providing traffic usage reports; Supporting mobility both within and between different radio access technologies.
5	**AMF (Access & Mobility Management Function)** - Access & Mobility Management Function is a sub-function of the Mobility Management Entity (MME) in the 4G EPC. Receives all connection and session information from the UE or RAN and performs connection and mobility management tasks. Includes the SEAF (Sec Anchor Function) sub-function **Security measures:** key management and encryption, SEAF, Security Context Management Function (SCMF) and Security Policy Control Function (SPCF). **Functions:** Organisation of control plane interfaces; Organisation of RRC signaling traffic exchange, encryption and protection of its data integrity; Organisation of NAS signaling traffic exchange, encryption and protection of its data integrity; Management of user equipment registration in the network and control of possible registration states; Management of user equipment connection to the network and control of possible states; Management of user equipment availability in the network in CM-IDLE state; Management of user equipment mobility in the network; Management of user equipment mobility
6	**SEPP (Security Protection Function Proxy)** - Security Edge Protection Proxy is a new NF introduced in 5GS by the 3GPP SA3 protocol to secure signalling traffic between networks of different operators. The N32 interface between SEPPs is designed to protect sensitive data passing through it and to provide secure authentication between SEPPs. **Security measures:** Deep Packet Inspection (DPI); advanced ML and AI based threat detection mechanisms can be integrated for real-time threat analysis. **Features: Traffic filtering:** SEPP can filter and inspect inbound and outbound traffic to detect and prevent malicious activities; Proxy authentication: Can handle authentication requests and enforce access policies; Encryption/decryption: SEPP can participate in encrypting and decrypting traffic, ensuring secure communications.
7	**SMF (Session Management Function)** - Session Management Function. **Functions**: Communication session management, i.e. session creation, modification and release, including tunnel support between access network and UPF; Allocation and management of IP addresses of user equipment; Selection of UPF gateway to be used; Organization of interaction with PCF; Management of QoS policy enforcement; Dynamic configuration of user equipment using DHCPv4 and DHCPv6 protocols; Control of tariff data collection and organization of interaction with billing system; Seamless service provisioning; Interaction with guest networks within the framework of Roaming
8	**PCF (Policy Control Function)** - The Policy Control Function allows decisions to be routed up to management level functions. **Functions**: Generating and assigning service policies to users, including QoS parameters and charging rules; Enforcing policies related to QoS, access control and charging; Ensuring proper allocation of network resources based on established policies; Dynamic rule processing; User context awareness.
9	**AF (App function)** is a functional unit in the 5G core (5GC) architecture responsible for handling specific aspects of application-related services and policies. **Functions**: Service provisioning, Policy control; Session management, Payment and billing, Interfacing with network functions, Service orchestration.
10	**NSSF (Network Slice Selection Function)** - Network Slice Selection Function for selecting and managing network slices. **Security measures:** Advanced encryption algorithms and authentication procedures. **Functions**: AMF, SMF, UPF, Network Slice Selection; Slice Instance Identification; Policy and Context Awareness

No	Description
11	**N3IWF (Non-3GPP Interworking Function)** is a component which provides seamless connectivity between 5G Core networks and non-3GPP networks such as Wi-Fi, Ethernet, DSL and cable networks. **Security measures:** provides authentication and security features for network users, ensuring that only authorised users are allowed to access the network and that all data transmitted is secure. **Functions**: Interoperability, mobility support, authentication and security, session management; payment
12	**AUSF (Authentication Server Function)** - Authentication Server Function that completes the EPC Home Subscriber Server (HSS) functions together with the UDM. **Stores and/or processes data:** stores the key received after authentication. **Functions**: Authentication server; Authentication; Security key management; Interfaces with other services to ensure uninterrupted authentication and security operations.
13	**UDM (Unified Data Management)** is a unified database representing significant HSS (Home Subscription Server) features from the EPC (Evolved Packet Core). It has the following subsystems: • ARPF (Authentication credential Repository and Processing Function) - A repository of credential authentication and processing functions. Stores authentication keys • SIDF (Subscription Concealed Identifier) - Subscription Concealed Identifier for Subscription Permanent Identifier (SUPI). Decrypts the Subscription Concealed Identifier (SUCI) to obtain its long-term identification, namely the SUPI. **Stores and/or processes data:** Authentication data, including user IDs, authentication vectors, and security keys; Subscription profiles, which contain details of the user's subscribed services, QoS (quality of service) parameters and other relevant subscription information; Policy Rules. **Security measures:** Encryption and secure authentication. Compliance with data privacy regulations is ensured. **Functions**: User profile data management, including storing and modifying the list of services available to users and their corresponding parameters; SUPI management; Generation of 3GPP AKA authentication credentials; Authorisation of access based on profile data (e.g. roaming restriction); User registration management, i.e. storing the serving AMF; Supporting service and session seamlessness, i.e. storing the SMF assigned to the current session; SMS delivery management;
14	**CHF (control plane function / Charging function)** - serves as a critical control plane function responsible for session management, policy enforcement and control of user plane resources. It is part of the Service Based Architecture (SBA) introduced in 5G, which aims to separate functions, making the network more modular and scalable. **Functions:** session management; control of policies and user plane resources; charging.
15	**NEF (Network Exposure Function)** is a feature in the 5G system that provides third-party applications with controlled access to network capabilities and services. **Stores and/or processes data:** ensures secure communication between third-party applications and the network by applying strong security mechanisms such as authentication, authorisation and encryption; authenticates and authorises external applications before granting them access to network services. **Functions:** Authorisation and authentication; Policy enforcement; Network service disclosure; Security and privacy; Authentication and authorisation; Service discovery;

Fig. 1 shows that the data exchange between the Internet environment and the user is carried out with the help of two elements of the architecture i.e. NR/gNB and UPF. Other elements are involved in the process of traffic management. A brief description of the network elements, their functions, stored and processed data in the 5G network is given in Table 1 based on sources [9; 10; 11; 13; 14; 15; 16].

Let's reflect in Fig. 2 the description of Table 1, where SEC - presence of primary security measures, SSEC - presence of the secondary security measures (management of rules, policies, functions, etc.), DB - presence of DB in the element, $ - has/is responsible for financial functions.

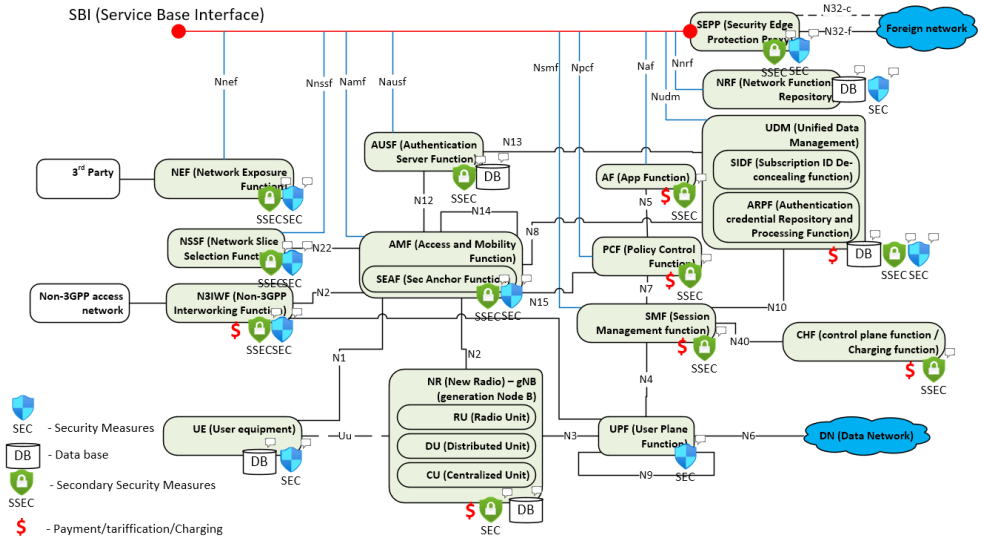

Figure 2. 5G/IMT-2020 architecture with the functions (created by the authors)

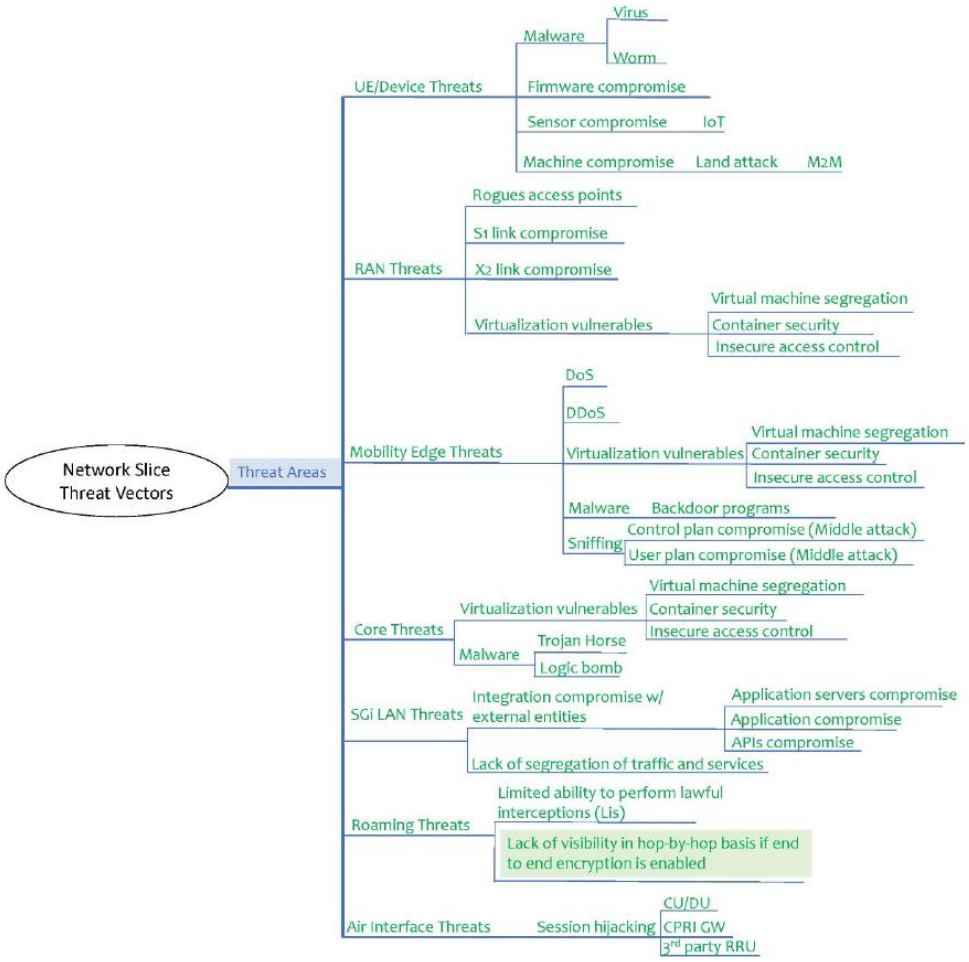

Figure 3. 5G Threat surface overview [17]

With this understanding of the 5G architecture and the purpose of its elements, it is possible to understand where the main attacks of attackers will be directed to the services responsible for billing and database, policy management and access provisioning. Note that the elements interacting with external networks - NR/gNB, NEF, N3IWF, SEPP, UPF, AMF - are critical and will be subject to the attackers' attacks first of all.

3 5G/IMT-2020 Security Threats

As seen from the description in Table 1, each element of the architecture plays an important role in both the provisioning of any of the services and the implementation of IS. The threats that are applicable to 5G are shown in Figure 3 [17].

Knowing the 5G architecture, it is possible to understand the threats and risks that could be faced with. Let's take a look at some of them.

3.1 Security Threats on UEs

UE can be infected in absolutely any way and thus the UE data and user data can be compromised to launch an attack on the 5G infrastructure. There is also a risk of the zero-day attack application vulnerabilities that could be discovered months later. Multiple infected devices are often networked into botnets used to launch the DDoS attacks.

The second important factor is the high data rate in 5G which allows attackers access and rights to the infrastructure to steal the network and user information faster than in previous technologies.

Mitigation measures: 1) provide mechanisms for analysing UE by the provider for the presence of malware on the device and tracking requests and traffic by UE. 2) apply flexible measures to tighten the IS compliance requirements, audit norms and control over their implementation and finalise mechanisms and regulations for a prompt remediation of identified new vulnerabilities.

3.2 Security Threats over the Wireless Interface (Air Interface)

Air-Interface attacks are one of the most popular attacks, making the task of securing IS over this interface quite challenging. Man-in-the-Middle (hereafter MitM)

attack [11] is one of the frequently encountered attacks that result in covert interception and/or decryption of data. Interception of the IMSI identifier [18] poses a serious threat to the subscriber, since the identifier is responsible for registering the subscriber's card in the network. By intercepting the IMSI and successfully selecting the encryption key (Ki), an attacker is able to clone the victim's card, resulting in access to almost any user resource. However, the 5G standard has strengthened the privacy protection against such attacks by frequently updating and encrypting the SUCI user ID and dynamically setting paging timings. But still, this type of the attack remains relevant for several reasons:

- interoperability with previous generations of networks where this problem is not solved and 5G can redirect the subscriber to the 4G segment if necessary;
- connecting UE to a fake radio station rather than a real gNB,

The next type of the attack is jamming the physical channel using a powerful signal source of the same frequency. This suppresses the UE signal and causes the link to break down.

Mitigation measures: Based on the above, the question arises about the continuity of previous G-technologies, the organization of their security level, and the prohibition of redirecting UEs to a previous G-technology. Refining the security measures of previous technologies (2G - 4G) may require significant investments. Cancellation of previous technologies may threaten to overload a new equipment, unavailability of subscribers due to the presence of outdated equipment and supported protocols, which will entail at least reputational and financial risks for the service provider. Therefore, it is necessary to analyze in which regions it is advisable to replace the outdated architecture, in which regions it is necessary to make the necessary improvements to meet the IS requirements, and in which regions it is acceptable to leave the existing architecture in place.

3.3 Security Threats on CN (Core Network)

The 5G packet core, which deploys and manages large-scale virtual machines (hereafter VMs) for network function virtualization and fragment management, is prone to information leakage through covert channels between different VM instances and is vulnerable to attacks attempting to access the system-level information of the entire infrastructure.

A tunnel with a strong encryption between UE and N3IWF is vulnerable to cyber threats if a weak encryption cannot resist brute-force attacks that Virtual Private Network (VPN) or Secure Shell (SSH) tunnels often face in an insecure Internet.

The Signaling System 7 (SS7) and Diameter protocols used for signaling in call processing, value-added services, traffic routing and information exchange are known to have vulnerabilities. Prior to 3G there was no encryption in SS7. 4G uses an advanced IP-based signaling protocol, Diameter, where encryption is mandatory but often not practiced by service providers in the network. The 5GS specifications propose an improved procedure for accepting resource reservation requests using the HTTP/XML interface from other services [11; 19]. However, PCF retains the traditional Diameter protocol for exchanging information with AFs, which retains a vulnerability in 5GS.

Mitigating measures: Service providers and developers need to find/develop an alternative to the Diameter protocol or make modifications to it, which will improve the IS level. At the moment in the Russian Federation within the framework of import substitution of foreign software, the Nexign Diameter Routing Agent (DRA) is used [20, 21]. Besides the technological advantages it helps operators to reduce the labour intensity of the maintenance and increase the security of the signaling network, as well as to implement complex monetization scenarios in the 3G, 4G networks, including 5G NSA (Non-Standalone).

3.4 Security Threats to the Application Server

Application servers external to 5GS remain vulnerable to a full range of cyber threats, from domain name server tunnelling to DDoS attacks such as Transmission Control Protocol Synchronize (SYN) flood attacks. 5G subscribers will experience slow application response rates or no service at all if the application server is subjected to such an attack, regardless of which ultrafast 5G connection they subscribe to.

The use of open source tools has contributed to a wide range of cybersecurity threats to 5G. To mitigate the threats to 5GS, 3GPP has published recommendations [22] on security and privacy procedures. But not all operators follow these recommendations due to which there are security holes. These are mainly problems with unreliable traffic encryption between UEs and gNBs, separation of trust zones between operators and many others.

Mitigating measures: Providers and service providers need to implement in their 5G infrastructure the requirements of IS, local regulators and 3GPP:

- to UE: 1) provide the capability to exchange encrypted messages with the gNB using NEA0, 128-NEA1 and 128-NEA2 encryption algorithms as presented in R-15; 2) provide support for 5G-GUTI, an 80-bit unique identifier assigned to AMF UE when registering with the network to preserve the subscriber's IMSI;
- to gNB: 1) provide similar encryption algorithms as UEs; 2) commissioning should be done through secure O&M systems;
- to core: 1) network operators should divide the network into several trust zones so that subnets of different operators are in different trust zones; 2) messaging between SBA NFs should

be confidential and only after a successful authentication; 3) activate the E2E core network interconnection security solution.

3.5 Open Source Softwarization

In 2018 at the OCP Summit conference, Arpit Joshipura, Linux Foundation's general manager of networking, stated that Open Source technologies will underpin the development of 5G and IoT and will automate functions to support a high speed and low latency in the 5G networks as well as the huge number of endpoints in IoT [23]. Obviously, the advantage of using open source software is the low cost of its implementation and anyone can find a vulnerability and report it to the developer, and also the Open Source code does not have software bookmarks, backdoors and other hidden functionality.

On the other hand, the National Vulnerability Database publishes reports that can be a potential red rag for hackers. Another risk is slow development practices and slow security patching process. 5G uses the Open Air Interface, which is an open source software [8].

Mitigating measures: At the organizational and legal level in companies: 1) fix procedures and regulations on a secure development; 2) mandatory pen-test and eliminate identified vulnerabilities before implementing and launching software into the product environment; 3) modernize the security patching process; 4) for developers: define a list of trusted sources and develop an internal code repository; mandatory regular courses on secure development.

3.6 Security Threats in AI

5GS uses a huge number of third-party services, network management and orchestration systems, and IPS/IDS systems that expose ML capabilities, which in themselves are not secure. Recently, ML using adversary attacks has gained popularity. In the context of 5G, AI and its subfields such as ML and deep learning are being used for various tasks including resource management, carrier sensing, cross-channel learning, user-needs profiling, and anomalous traffic detection for the cyber defense.

Hackers are also using ML techniques to perform smarter, faster and less expensive attacks. For example, the PfssGAN neural network can guess passwords better than brute force password mining tools. Spammers use AI tools to generate unwanted emails a with spam content that can bypass spam filters and get into a user's inbox. Fuzzying vulnerability detection tool have become more effective and sought after by hackers after AI was introduced.

Mitigating measures: develop a unified international standard regulating the basic requirements and recommendations for a safe implementation and use of AI systems in wireless networks, taking as a basis documents that impose such requirements, e.g.: 1) EU AI Law [24]; 2) ‘Interim Measures for the Management of Generative Artificial Intelligence Services’ [20], developed by PRC regulators; 3) National Strategy for Artificial Intelligence Development until 2030 [21], Approved by Presidential Decree N 490 dated 10 October 2019; 4) Responsible Artificial Intelligence Strategy and Implementation Pathways [14], developed by the US Pentagon in June 2022; 5) UAE National Artificial Intelligence Strategy by 2031.

3.7 Security threats at the physical level

Securing a noisy physical channel in the presence of an active listening device is a difficult task, since an eavesdropping device can disrupt the pilot signal and corrupt the channel measurement which is extremely important for the operation of mass MIMO and beamforming technologies. Also, non-orthogonal multiple access methods are difficult to implement safely, since users need to exchange unsecured messages.!

Mitigation measures: Regardless of the network segment, all data flows and all traffic must be encrypted. This may seem like a "double-edged sword" due to the fact that: 1) encrypting traffic creates an illusion of the security because we encrypt the traffic, but we should not forget about encrypting the data in the database. In many cases of information leakage, the attackers steel valuable data exactly in the process of its storage, not transmission; 2) traffic encryption requires a lot of productive equipment resources that could be used for "useful" business purposes. It is worth taking into account the fact that modern equipment has a sufficient capacity to process the encrypted traffic.

3.8 State Requirements

A lawful interception of the user data is often a requirement in scenarios where law enforcement agencies want to trace individuals for criminal offences they have committed. Consequently, it is necessary not to completely remove a support for a zero encryption or unencrypted communication mode in 3GPP specifications. This government requirement leaves a vulnerability that could potentially lead to rare instances of security threats to networks.

Mitigation measures: monitoring and analytics systems with inbuilt ML and AI mechanisms should be implemented to detect anomalies between network functions, on the basis of which it will be possible to compile certain statistics and further develop the strategy with regulators to manage the problem, as there is a fine line between legitimate interception and invasion of privacy, which is respected by regulations and strict implementation of regulated procedures.

3.9 Threats of interoperability with a vulnerable LTE network

The 5G network will initially coexist with an LTE analogue where there is a number of known vulnerabilities, including RNTI tracking and Layer 2 DNS traffic hijacking, that have not been adequately addressed in the current security proposals. Thus, the existing LTE loopholes could be a potential weakness for new 5G networks, and no countermeasures are recommended by 3GPP. Also applicable in this case are issues related to: 1) data protection and privacy (e.g. MITM attack); 2) re-routing capabilities of sensitive data (e.g. DDoS attack and network hijacking); 3) collision of policies and technologies; 4) Network Slicing and cyber-attacks; 5) IoT vulnerabilities [18; 25].

Mitigation measures: This point also raises the issue we raised above in p.3.2 about the interaction between the old and new technologies.

3.10 Security Threats of SDN (Software-defined Networking)

Recent attacks, such as SSH over secure hidden cache channels in the cloud, expose weaknesses inherent in cloud computing on which most SDN solutions depend. For example, in 2023, researchers from the Ruhr University Bochum developed a Terrapin attack, which 'exploits weaknesses in the SSH transport protocol combined with new cryptographic algorithms and encryption modes introduced in OpenSSH more than ten years ago,' the researchers write, adding that those have been adopted by a wide range of the SSH implementations and affect the most current implementations [26; 27]. In addition, there are the following attacks on SDN: D-DOS, DOS, Hijacked Controllers, MITM, Back Hole, Eavesdropping.

Mitigating measures: for a secure and rapid 5G deployment, a scalable, certified security monitoring tool is needed to ensure the security of microservices running in the public cloud. There is also a need to improve the existing authentication mechanisms and use a role-based authorization encryption of data streams.

4 RESULT

Assessment of the IS risks and measures to mitigate them

A risk is an unfavourable event which is ubiquitous to losses and has three characteristics: probability of occurrence, amount of losses, and time horizon. To make it convenient to assess the magnitude of risks visually, matrices are used in which the most significant threshold values of probabilities of the risks occurrence of risks and threshold values of their consequences of these risks are entered. We use the CASE (Consequence, Assets, Source, Event) technology as a basis for determining the risk degree [28].

Table 2 shows a risk assessment of a threat realization before and after application of mitigation measures, where the probability of the threat occurrence (hereinafter Probability) is estimated as Low (0-20%), Medium (21-40%), High (41-60%), Very high (61-80%), Critical (81-99%). And the Risk Level (hereinafter R.Lev) is assessed according to the risk matrix in Fig.5.

Impact	Low	Medium	High	Very high	Critical
Critical	4	5	5	5	5
Very high	3	4	4	4	5
High	2	3	3	4	5
Medium	1	2	2	3	4
Low	1	1	2	2	3

Probability

Where:

Critical	5
Very high	4
High	3
Medium	2
Low	1

Figure 4. Risk assessment matrix (created by the authors)

Table 2. Risk assessment of a threat realization before and after application of measures

Threat (Th)	**BEFORE**			**AFTER**		
	Impact	**Prob**	**R.Lev**	**Impact**	**Prob**	**R.Lev**
Th1: Security threats on UEs	*High*	Med	3	*Med*	Med	2
Th2: Security threats over the wireless interface	*Med*	Med	2	*Low*	Low	1
Th3: Security threats on CN	*High*	Med	3	*Med*	Med	2
Th4: Security threats to the application server	*High*	High	3	*Med*	Med	2
Th5: Open-source softwarization	*High*	High	3	*Med*	Low	1
Th6: Security threats in AI	*High*	Med	3	*Med*	Low	1
Th7: Security threats at the physical level	*Med*	High	2	*Med*	Med	2
Th8: State requirements	*Med*	Med	2	*Med*	Med	2
Th9: Threats of interoperability with a vulnerable LTE network	*High*	High	3	*Med*	Med	2
Th10: Security threats of SDN	*High*	High	3	*Med*	Med	2

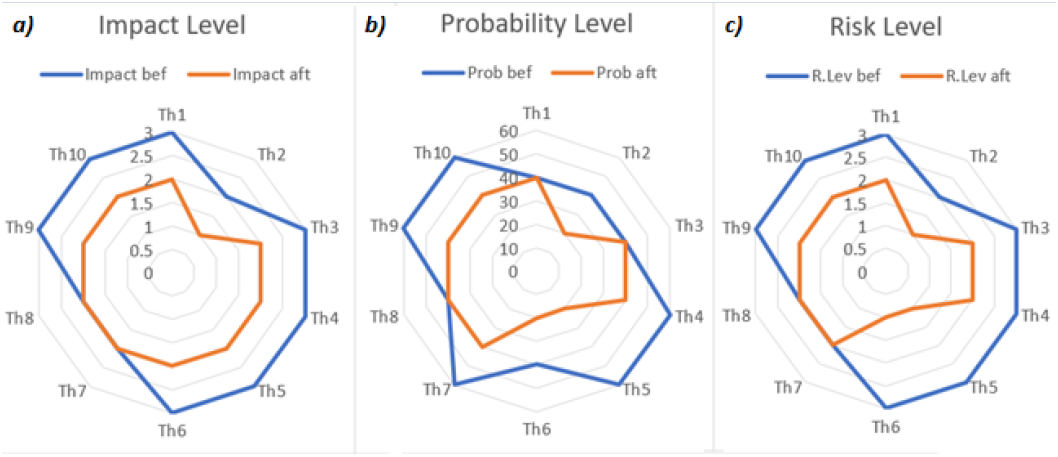

Figure 5. Results of assessing *(a)* the level of exposure, *(b)* the level of probability *(c)* the level of risk of threat realization BEFORE and AFTER mitigation measures are implemented (created by the authors)

Let's make calculations based on the data from Table 2.

$$Probability_{lev}=AVG(Th1_{aft}-Th1_{bef},\ldots,Th10_{aft}-Th10_{bef})=AVG(0,20,0,20,40,20,20,0,20,20)=16\% \quad (1)$$

$$Impact_{lev}=AVG(Th1_{aft}-Th1_{bef},\ldots,Th10_{aft}-Th10_{bef})=AVG(20,20,20,20,20,20,0,0,20,20)=16\% \quad (2)$$

where $Th[i]_{aft}$ is a threat **After,** and $Th[i]_{bef}$ is a threat **Before**.

These calculations show that the proposed measures will significantly improve the security of the fifth-generation networks. The risk probability of the threat realization is reduced by 16% on average. The aim applies to level of the impact. Fig. 6 graphically presents the results of the calculations, which applies this.

5 Discussion

There are many risk assessment methodologies. Each has its advantages and disadvantages. We use the CASE methodology because, this method considers these key elements of the risk statement, e.g. the likely impact (consequence) of the risk on a specific asset, the source of the risk, and the event that can trigger a risk. By being specific and thorough in one's risk statements, all the stakeholders should be on the same page to effectively manage the risk. Some other available methodologies are:

- DREAD (damage potential, reproducibility, exploitability, affected users, discoverability) identifies the most dangerous variants of attacks to rationally plan the budget of the project for the implementation (testing) of security measures and protection of the software product. By calculating a combined DREAD score, security professionals can prioritize threats based on their potential business impact. A high DREAD score indicates a threat that requires an immediate attention due to its high potential to cause a significant damage.
- STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) is more about finding and categorizing threats. The model is one of the most commonly used threat modeling methodologies as it provides an important insights to be proactive in recognizing and defending important system infrastructure, devices, and networks that are susceptible to attacks. Moreover, The STRIDE threat model ensures that software products maintain the CIA (confidentiality, integrity, availability) triad.
- CVSS (Common Vulnerability Score System) is a standardized quantitative scoring system designed specifically for a vulnerability assessment alternative to CVSS. It assigns a score from 0.0 to 10.0 based on the key metrics: base score, temporal score, environmental score. A high CVSS score indicates a serious vulnerability that requires quick patches or mitigation strategies. It is important to note that CVSS focuses on the technical severity of the vulnerability.
- PASTA (Process for Attack Simulation and Threat Analysis) is a seven-step methodology used to identify, analyze and prioritize threats and attacks in software applications. The PASTA framework is comprehensive and focuses on a risk-based approach to threat modeling.

Each of the above methodologies is effective in its own field and is designed for its own tasks. But for an effective IS risk management, a comprehensive approach

should be applied. This is why CASE is a more universal approach. Our findings provide an opportunity for companies to analyze and review their IS level in relation to the wireless network technologies they use and, if necessary, to take measures we propose to mitigate the risks in relation to their infrastructure. For a risk assessment, the method described in the "Security Risk Assessment for 5G Networks can be used: National Perspective" [4; 29; 30] or in "Power 5G hybrid networking and Security Risk Analysis" [5], however, in practice, the CASE or DREAD methods are more applicable. their effectiveness in conducting the risk assessment [31, 32, 33, 34]. A fairly detailed description of threats with security enhancement measures is presented in "5G Security Threat Assessment in Real Networks" [35, 36, 37, 38, 39], but an assessment is mode of the level of risks and of the effectiveness of the proposed measures. In our paper, we review other current threats, assess their level of risk of their realization and propose and evaluate the mitigation measures.

6 CONCLUSION

In the fifth generation wireless networks, the security is a critical aspect due to the increased complexity and variety of services it supports. The important security concepts in 5G include:

- Security Edge Protection Proxy (SEPP);
- User Plane Function (UPF): In 5G, UPF is responsible for handling user data as it passes through the network. It can incorporate security features such as encryption and integrity protection, to ensure the confidentiality and integrity of user data;
- Network slicing security: 5G networks introduce a concept of network slicing, where different logical networks (slices) are created on a common physical infrastructure to support different services with different requirements. Security mechanisms must ensure the isolation and integrity of these slices;
- Authentication and Key Management: 5G networks use advanced authentication mechanisms and key management procedures to secure communications between network elements and user devices. This includes the use of a mutual authentication and creation of a secure key material;
- Radio Interface Security: The 5G radio interface, known as a New Radio (NR), employs security measures to protect wireless communications. These include encryption of the user data and signals, and the use of secure key exchange protocols;
- Security Gateways: 5G networks can use security gateways that provide a barrier between the core network and external networks, ensuring the security and integrity of the core network.

The analysis of the 5G/IMT-2020 network architecture gives an idea of the strengths and weaknesses of the solution to help identify the IS risks and how to avoid them. The measures taken to mitigate the IS risks of the considered threats will reduce the probability of realization of these threats and the level of their impact by 16%, thus avoiding in the future similar problems related to the implementation of the IS protection in the next generation wireless networks.

As part of our further research the list of the considered IS threats will be expanded to conduct an in-depth analysis of the risks in wireless networks, and to assess the effectiveness of the proposed measures to mitigate them.

REFERENCES

[1] Kaspersky (2020). *5G networks: pros and cons*. [Online]. Available: https://www.kaspersky.ru/resource-center/threats/5g-pros-and-cons

[2] Government of the Russian Federation (2019). *Decree of the President of the Russian Federation No. 490 of 10.10.2019.* Moscow, Russia.

[3] *ENISA threat landscape for DOS attacks.* (2023, December 6). ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks

[4] J. Batalla, E. Andrukiewicz, G. Gomez, P. Sapiecha, C. Mavromoustakis, G. Mastorakis, J. Zurek, and M. Imran, 'Security Risk Assessment for 5G Networks: National Perspective'. *IEEE Wireless Communications*, vol. 27, pp. 16-22, 2020. DOI: 10.1109/MWC.001.1900524.

[5] Y. Jiang, Y. Cong, and A. Hu, 'Power 5G hybrid networking and Security risk analysis'. *Frontiers in Energy Research*, vol. 9, 2022. https://doi.org/10.3389/fenrg.2021.796257

[6] I. Ahmad, J. Suomalainen, and J. Huusko, '5G-Core Network Security'. In book: *Wiley 5G Ref*, pp. 1-18, 2019. DOI: 10.1002/9781119471509.w5GRef151.

[7] X. Zhang, J. Fei, H. Jiang, and X. Huang, 'Research on Power 5G Business Security Architecture and Protection Technologies'. *6th International Conference on Power and Renewable Energy (ICPRE),* pp. 913-917, 2021. DOI: 10.1109/ICPRE52634.2021.9635437.

[8] 5G Americas (2020). *The Status of Open Source for 5G.* 5G Americas White Paper. [Online]. Available: https://www.5gamericas.org/the-status-of-open-source-for-5g/

[9] 3GPP TR 38.801 Technical Report (2017-03). 3rd Generation Partnership Project; Technical specification Group Radio Access Network; Study on New Radio Access Technology: Radio Access Architecture and Interfaces. [Online]. Available: https://panel.castle.cloud/view_spec/38801-e00/pdf/

[10] *Technical specification 5G; NG-RAN; Architecture description (3GPP TS 38.401 version 16.3.0 Release 16).* ETSI TS 138 401 V16.3.0 (2020-11) [Online]. Available: https://www.etsi.org/deliver/etsi_ts/138400_138499/138401/16.03.00_60/ts_138401v160300p.pdf

[11] R. Mitra, and M. Marina, '5G Mobile Networks Security Landscape and Major Risks'. *The Wiley 5G REF: Security, Wiley*, pp. 1-23, 2021. DOI: 10.1002/9781119471509.w5GRef145.

[12] S. Holtmanns, I. Oliver, L. Miche, A. Kalliola, G. Limonta, and Peinado, G. 'G Security – Complex Challenges'. In *The Wiley 5G REF*, pp. 1-15, 2021. DOI: 10.1002/9781119471509.w5GRef161.

[13] *5G Core Network.* (n.d.). 5G Non 3GPP Access-N3IWF - Programmer sought. [Online]. Available: https://programmersought.com/article/96376554983/

[14] *TELECOM TRAINER* (2023, December 25). nrf 5g. Telecom Trainer. [Online]. Available: https://www.telecomtrainer.com/nrf-5g/

[15] *5G Network Repository Function (NRF) | Oracle. (2024, April).* [Online]. Available: https://www.oracle.com/communications/service-providers-network/products/5g-network-repository-function/

[16] *Inseego*. (n.d.). What is a GNB (gNodeB)? Inseego. [Online]. Available: https://inseego.com/resources/5g-glossary/what-is-gnb/

[17] 5G Americas. (2020, April 27). *The evolution of security in 5G. A "Slice" of Mobile Threats.* 5G Americas White Paper. [Online]. Available: https://www.5gamericas.org/the-evolution-of-security-in-5g-2/

[18] A. Shalaginov, '*Vulnerabilities 2G GSM'.* Telecom & IT, 2023, February 26 [Online]. Available: https://shalaginov.com/2023/02/26/2g-gsm-network-vulnerabilities/

[19] Ali Hussein, Imad Elhajj, Ali Chehab, and Kayssi, Ayman. 'Securing Diameter: Comparing TLS, DTLS, and IPSec'. *2016 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET),* pp. 1-8, 2016. DOI: 10.1109/IMCET.2016.7777417

[20] TAdviser.ru. (n.d.). *Nexign Diameter Routing Agent (DRA).* [Online]. Available: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Nexign_Diameter_Routing_Agent_%28DRA%29

[21] *Nexign Diameter Routing Agent (DRA).* (n.d.). [Online]. Available: https://catalog.arppsoft.ru/product/6222144

[22] *5G; Security architecture and procedures for 5G System* (3GPP TS 33.501 version 16.17.0 Release 16) // ETSI TS 133 501 V16.17.0 (2024-01) [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.17.00_60/ts_133501v161700p.pdf

[23] Fgts_Ru. (2021, November 30). *The Future of 5G Mobile Networks: A Software-Defined Approach with OpenSource, Canonical's Experience*. [Online]. Available: https://habr.com/ru/companies/fgts/articles/568340

[24] *Network Repository Function (NRF).* (2021, August 3). YateBTS - LTE & GSM mobile network components for MNO & MVNO. [Online]. Available: https://yatebts.com/documentation/concepts/5g-core-network/network-repository-function-nrf/

[25] A. Shalaginov, '*Mobile Network Vulnerabilities (Overview)'.* Telecom & IT. 2023, March 30 [Online]. Available: https://shalaginov.com/2023/02/25/mobile-networks-vulnerabilities-overview/

[26] F. Bäumer, M. Brinkmann, and J. Schwenk. *Terrapin attack: Breaking SSH channel integrity by sequence number manipulation.* arXiv.org, (2023, December 19) [Online]. Available: https://arxiv.org/abs/2312.12422

[27] *Terrapin Attack*. (n.d.). Retrieved from: https://terrapin-attack.com/

[28] J. Talbot, '*What's right with risk matrices?'* 2023, October 4 [Online]. Available: https://www.juliantalbot.com/post/2018/07/31/whats-right-with-risk-matrices

[29] S. Sesia, I. Toufik, and M. Baker, LTE - The UMTS Long Term Evolution From Theory to Practice. Second Edition. *Wiley eBooks. IEEE Xplore,* 2011 [Online]. Available: https://ieeexplore.ieee.org/book/8039669

[30] A. K. Yerrapragada, T. Eisman and Kelley, B. 'Physical Layer Security for Beyond 5G: Ultra Secure Low Latency Communications'. *IEEE Open Journal of the Communications Society,* vol. 2, pp. 2232-2242, 2021. DOI: 10.1109/OJCOMS.2021.3105185.

[31] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, 'Overview of 5G Security Challenges and Solutions' *IEEE Communications Standards Magazine,* vol. 2, no. 1, pp. 36-43, 2018. DOI: 10.1109/MCOMSTD.2018.1700063.

[32] *CFI Team*. (2024, May 25). Inflection point. Corporate Finance Institute. [Online]. Available: https://corporatefinanceinstitute.com/resources/commercial-lending/inflection-point/

[33] I.A. Mihajlova, 'Architecture of HR and LBO roaming in 5G networks'. *Economics and quality of communication systems*, vol. 1, no. 23, pp. 26-36, 2022.

[34] M. J. Mohammed, et al. A Comparison of 4G LTE and 5G Network Cybersecurity Performance. *2024 35th Conference of Open Innovations Association (FRUCT), Tampere, Finland,* pp. 452-464, 2024. DOI: 10.23919/FRUCT61870.2024.10516378.

[35] Edgardo Montes de Oca. SDMN Security. In *The Wiley 5G REF: Security, Wiley,* pp. 25-42, 2021. DOI:10.1002/9781119471509.w5gref154.

[36] S. Park, D. Kim, Y. Park, H. Cho, D. Kim and S. Kwon, '5G Security Threat Assessment in real networks', *Sensors*, vol. 21, no. 16, pp. 5524, 2021. https://doi.org/10.3390/s21165524

[37] S. Qin, and C. Lao, 'Computer Network Security Defense System in 5G Era'. *2022 International Conference on Artificial Intelligence of Things and Crowdsensing (AIoTCs),* pp. 169-174, 2022. DOI: 10.1109/AIoTCs58181.2022.00032.

[38] W. You, M. Xu and D. Zhou, 'Research on security protection technology for 5G cloud network'. *2021 International Conference on Advanced Computing and Endogenous Security,* pp. 01-11, 2022. DOI: 10.1109/IEEECONF52377.2022.10013352.

[39] Z. Zou, T. Chen, J. Chen, Y. Hou and R. Yang, 'Research on Network Security Risk and Security Countermeasures of 5G Technology in Power System Application'. *2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC),* pp. 102-105, 2021. DOI: 10.1109/IAEAC50856.2021.9390826.

Ivan A. Smirnov is a PhD student, Moscow Institute of Electronics and Mathematics named after A.N. Tikhonov, National Research University Higher School of Economics, Department of Computer Engineering, Methods and Systems of Information Protection, Information Security. His research interests include Cyber security, Information protection, personal data protection, information security risks, Wireless networks 5G/6G. His work has been published in a range of scientific conferences journals.

Yevgeni Koucheryavy is a Full Professor and R&D Institute director at the A.N. Tikhonov Moscow Institute of Electronics and Mathematics, National Research University Higher School of Economics. His research interests include Radio resource management (RRM), digital twins, AI/ML, wireless networks and THz communications. He is the author and co-author of numerous scientific papers published in renowned international journals and conferences.