

UDC 004.056:621.39

**Kozhabai Bereke**

Bachelor Student

**Scientific supervisor:** Mamilov Bakhytzhan

Associate Professor

Department of Telecommunication Engineering

Muhammadjan Tynyshbayev ALT University

(Almaty, Kazakhstan)

## SECURITY CHALLENGES IN IOT-BASED TELECOMMUNICATION NETWORKS

**Abstract:** The rapid expansion of the Internet of Things (IoT) has significantly transformed modern telecommunication networks, enabling the interconnection of billions of devices and supporting a wide range of applications, including smart cities, healthcare, and industrial automation. However, this massive integration introduces critical security challenges due to the heterogeneous nature of IoT devices, limited computational resources, and the complexity of network architectures. This paper analyzes the key security threats in IoT-based telecommunication networks, including device vulnerabilities, network-level attacks, data privacy issues, and software weaknesses. Particular attention is given to challenges such as unauthorized access, data interception, distributed denial-of-service (DDoS) attacks, and insecure communication protocols. Furthermore, the study reviews existing security mechanisms, including lightweight cryptography, secure communication protocols, and emerging solutions based on artificial intelligence and blockchain technologies. The paper also highlights future research directions aimed at enhancing the resilience and trustworthiness of IoT ecosystems. The findings emphasize the need for comprehensive, scalable, and adaptive security frameworks to ensure the safe deployment of IoT in next-generation telecommunication networks.

**Keywords:** Internet of Things (IoT); Telecommunication Networks; Cybersecurity; Network Security; Data Privacy; DDoS Attacks; Lightweight Cryptography; Edge Computing; Artificial Intelligence; Blockchain.

**Introduction.** The rapid development of the Internet of Things (IoT) has significantly reshaped modern telecommunication networks, transforming them into highly interconnected and intelligent systems. IoT refers to a network of physical devices embedded with sensors, software, and communication capabilities that enable them to collect, exchange, and process data over the Internet. In contemporary telecommunication environments, IoT technologies are widely applied across various domains, including smart cities, healthcare systems, industrial automation, transportation, and environmental monitoring. These applications rely on seamless connectivity, real-time data exchange, and efficient network performance, making IoT an essential component of next-generation communication infrastructures.

The number of IoT devices has been growing exponentially over the past decade, driven by advancements in wireless communication technologies such as 5G, low-power wide-area networks (LPWAN), and edge computing. Billions of connected devices—including sensors,

smart meters, wearable devices, and industrial machines—are now integrated into telecommunication networks, generating vast amounts of data. This rapid expansion has led to increased network complexity, heterogeneity, and scalability challenges. As IoT devices become more deeply embedded in telecom infrastructure, they not only enhance operational efficiency and service delivery but also introduce new risks and vulnerabilities.

Security has become a critical concern in IoT-based telecommunication systems due to the inherent limitations of many IoT devices, such as constrained processing power, limited memory, and energy efficiency requirements. These constraints often prevent the implementation of robust security mechanisms, making devices susceptible to various cyber threats. Additionally, the distributed nature of IoT networks, combined with diverse communication protocols and platforms, creates a broad attack surface for malicious actors. Security breaches in such systems can lead to severe consequences, including data leakage, unauthorized access, disruption of services, and even risks to human safety in critical applications like healthcare and smart infrastructure.

The research problem addressed in this article is the identification and analysis of key security challenges associated with IoT-based telecommunication networks, as well as the evaluation of existing and emerging solutions to mitigate these risks. Despite significant advancements in cybersecurity technologies, ensuring end-to-end security in IoT ecosystems remains a complex and unresolved issue. Therefore, this study aims to provide a comprehensive overview of current threats, analyze their impact on telecommunication networks, and explore effective strategies for enhancing security.

The main objectives of this article are: (1) to examine the architecture and characteristics of IoT-based telecommunication networks; (2) to identify major security vulnerabilities and attack vectors at different layers of the system; (3) to review existing security mechanisms and technologies; and (4) to outline future research directions for improving the reliability, scalability, and security of IoT-enabled communication systems.

**Architecture of IOT-based telecommunication networks.** IoT-based telecommunication networks are designed as complex, multi-layered architectures that enable seamless interaction between physical devices, communication infrastructures, and intelligent applications. These architectures support large-scale connectivity, real-time data exchange, and distributed processing, which are essential for modern digital services. Typically, IoT systems are organized into three fundamental layers—perception, network, and application—supplemented by advanced computing paradigms such as Edge Computing and cloud computing. This layered approach ensures scalability, flexibility, and interoperability across heterogeneous environments.

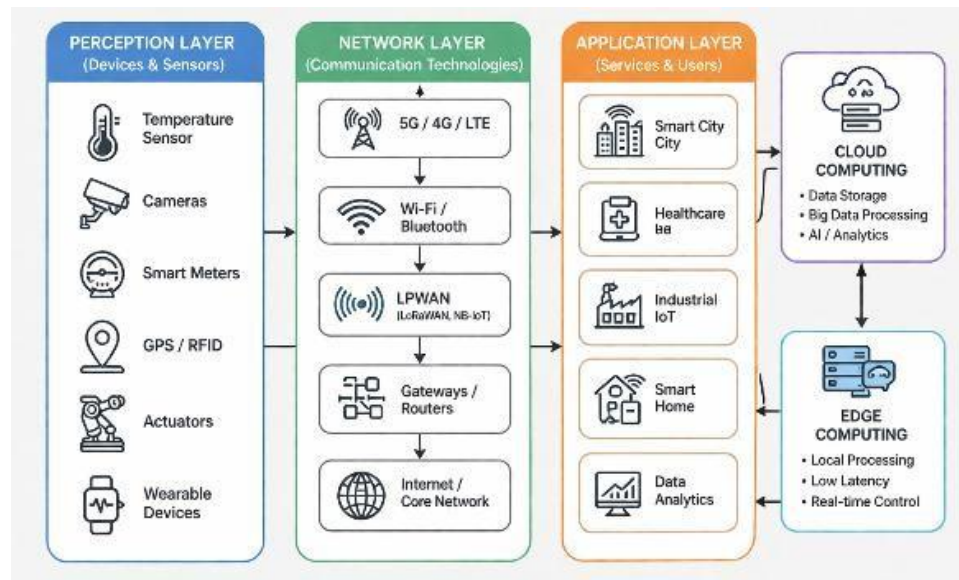


Fig 1. Architecture of IoT-based telecommunication networks

The perception layer represents the physical interface between the digital system and the real world. It consists of sensors, actuators, RFID tags, embedded systems, and smart devices that collect data from the environment. These devices monitor various parameters such as temperature, humidity, motion, pressure, location, and physiological signals.

This layer incorporates multiple communication technologies, including:

1. 5G networks, which support high bandwidth, ultra-low latency, and massive device connectivity

2. LPWAN technologies (e.g., LoRaWAN, NB-IoT), designed for long-range, low-power communication

3. Wi-Fi and Bluetooth, used for short-range communication in local networks

4. Wired technologies such as Ethernet and fiber optics, providing high reliability and stability

The network layer must address key challenges such as interoperability, routing efficiency, congestion management, and quality of service (QoS). At the same time, it is a critical point of vulnerability where data can be intercepted, modified, or disrupted by cyberattacks.

The application layer is responsible for delivering IoT services to end-users and enabling interaction with the system. It processes the data received from lower layers and converts it into meaningful insights, supporting decision-making and automation.

This layer includes a wide range of applications, such as:

- Smart home systems and automation
- Healthcare monitoring and telemedicine
- Industrial IoT (IIoT) and process control
- Smart city solutions (traffic, energy, environment)
- Agricultural monitoring systems

In addition, the application layer incorporates user interfaces, mobile applications, dashboards, and APIs, allowing users to interact with IoT systems efficiently. Advanced technologies such as data analytics, artificial intelligence, and machine learning are often integrated at this level to enhance system intelligence and performance.

The integration of edge and cloud computing plays a crucial role in modern IoT-based telecommunication networks.

Cloud computing provides centralized data storage, large-scale processing capabilities, and advanced analytics. It supports long-term data analysis, system optimization, and machine learning model development. However, reliance on cloud infrastructure can introduce latency and increase bandwidth usage.

To overcome these limitations, edge computing has emerged as a complementary approach. By processing data closer to the source, edge computing reduces latency, improves real-time responsiveness, and minimizes network congestion. This is particularly important for time-sensitive applications such as autonomous systems, industrial control, and healthcare monitoring.

The combination of edge and cloud computing forms a hybrid architecture that balances performance, scalability, and efficiency.

Data flow in IoT-based telecommunication networks typically follows a multi-stage process: data is generated at the perception layer, transmitted through the network layer, processed at edge or cloud nodes, and delivered to the application layer.

Several communication models are commonly used:

- Device-to-Device (D2D): direct communication between devices
- Device-to-Cloud (D2C): devices send data directly to cloud platforms
- Device-to-Edge (D2E): local processing at edge nodes before cloud transmission
- Publish/Subscribe model: data is distributed via brokers (e.g., MQTT)
- Request/Response model: traditional client-server interaction (e.g., HTTP, CoAP)

These models provide flexibility and adaptability for different application scenarios but also introduce challenges related to latency, scalability, interoperability, and security.

**Key security challenges.** The integration of the Internet of Things (IoT) into modern telecommunication networks has introduced a wide range of complex security challenges that stem from the scale, heterogeneity, and distributed nature of these systems. Unlike traditional networks, IoT-based infrastructures consist of billions of interconnected devices operating under diverse conditions and using different communication protocols. This significantly expands the attack surface and creates numerous entry points for malicious actors. As a result, ensuring comprehensive security across all layers of IoT-based telecommunication networks has become one of the most critical issues in contemporary cybersecurity research.

One of the primary challenges arises from the inherent limitations of IoT devices themselves. Many devices are designed with minimal computational resources, limited memory, and strict energy constraints, which restrict the implementation of advanced security mechanisms. Consequently, such devices often rely on weak authentication methods, lack proper encryption, and are frequently deployed with default or hardcoded credentials. These vulnerabilities make IoT devices easy targets for attackers, who can gain unauthorized access and use compromised devices as entry points into larger telecommunication networks.

In addition to device-level weaknesses, the communication infrastructure of IoT systems presents significant security risks. Data transmitted across networks is often exposed to threats such as interception, manipulation, and disruption. Wireless communication technologies, including Wi-Fi, LPWAN, and cellular networks, are particularly susceptible to eavesdropping and man-in-the-middle attacks. Furthermore, large-scale distributed denial-of-service (DDoS) attacks, often orchestrated through compromised IoT devices, can overwhelm network resources and disrupt critical telecommunication services. These threats highlight the

vulnerability of the network layer, which plays a central role in maintaining connectivity and data exchange.

Another major concern is the security and privacy of data generated by IoT systems. IoT devices continuously collect vast amounts of sensitive information, including personal data, industrial metrics, and environmental parameters. In many cases, this data is transmitted and stored without adequate protection, increasing the risk of data breaches and unauthorized access. The lack of end-to-end encryption and insufficient access control mechanisms further exacerbate these issues. In sensitive applications such as healthcare and smart cities, data security failures can lead not only to privacy violations but also to serious consequences affecting human safety and public trust.

Software and firmware vulnerabilities also contribute significantly to the overall security challenges in IoT-based telecommunication networks. Many IoT devices operate on outdated or poorly maintained software, and secure update mechanisms are often отсутствуют или реализованы ненадежно. This allows attackers to exploit known vulnerabilities, inject malicious code, and establish persistent control over devices. The widespread use of insecure firmware has facilitated the emergence of large-scale IoT botnets, which can be used to launch coordinated cyberattacks against critical infrastructure.

Moreover, the heterogeneity and масштабируемость IoT ecosystems complicate the implementation of consistent security strategies. Devices from different manufacturers often use incompatible protocols and security mechanisms, making it difficult to enforce unified standards across the network. Managing identities, authentication, and encryption keys in such a large and diverse environment becomes increasingly complex. The absence of standardized security frameworks and regulatory requirements further aggravates the situation, leading to inconsistent security practices and increased vulnerability.

In summary, the key security challenges in IoT-based telecommunication networks are multifaceted and interconnected, encompassing device vulnerabilities, network threats, data privacy risks, software weaknesses, and systemic issues related to scalability and standardization. Addressing these challenges requires a holistic approach that integrates secure design principles, advanced technologies, and coordinated efforts across industry, academia, and regulatory bodies to ensure the resilience and trustworthiness of next-generation telecommunication systems.

**Security requirements for IOT networks.** Ensuring security in Internet of Things (IoT)-based telecommunication networks requires the implementation of fundamental security principles adapted to the specific characteristics of IoT environments. Unlike traditional systems, IoT networks operate under conditions of large-scale device deployment, heterogeneity, and resource constraints, which necessitate lightweight, scalable, and flexible security solutions. Therefore, defining clear security requirements is essential for protecting data, maintaining system integrity, and ensuring reliable communication across all layers of the network.

One of the primary requirements is confidentiality, which ensures that sensitive data transmitted and processed within IoT systems remains protected from unauthorized access. Given the continuous exchange of data between devices, edge nodes, and cloud platforms, encryption mechanisms must be employed to safeguard information. However, due to the limited computational capabilities of many IoT devices, traditional encryption algorithms may not always be suitable, leading to the need for lightweight cryptographic techniques that balance security and performance.

Another critical requirement is data integrity, which guarantees that information is not altered or tampered with during transmission or storage. In IoT-based telecommunication networks, data often passes through multiple intermediate nodes, increasing the risk of manipulation. Mechanisms such as hashing, digital signatures, and message authentication codes are essential to ensure that any unauthorized modification can be detected. Maintaining integrity is particularly important in applications such as industrial control systems and healthcare, where incorrect data may lead to serious consequences.



Fig.2. Figure X – Security Requirements in IoT-Based Telecommunication Networks

Availability is also a fundamental requirement, as IoT systems must ensure continuous operation and accessibility of services. Telecommunication networks supporting IoT applications are expected to function in real time, and any disruption can affect critical services such as emergency response, smart infrastructure, and medical monitoring. Therefore, systems must be designed to withstand attacks such as distributed denial-of-service (DDoS) and ensure resilience through redundancy, load balancing, and fault-tolerant architectures.

Authentication and authorization mechanisms play a vital role in verifying the identity of devices and controlling access to network resources. In large-scale IoT environments, where billions of devices interact dynamically, it is essential to establish secure identity management systems. Authentication ensures that only legitimate devices and users can access the network, while authorization defines the level of access granted to each entity. Implementing efficient and scalable authentication protocols remains a significant challenge due to the diversity and constraints of IoT devices.

In addition, secure key management is a crucial requirement for maintaining cryptographic security in IoT networks. The distribution, storage, and renewal of cryptographic keys must be handled securely, especially in dynamic environments where devices frequently join or leave the network. Poor key management practices can lead to compromised encryption and unauthorized access, undermining the overall security of the system.

Another important requirement is privacy protection, particularly in applications involving personal or sensitive data. IoT systems often collect detailed information about users and environments, making them susceptible to privacy violations. Ensuring data minimization, anonymization, and secure data handling practices is essential to protect user privacy and comply with regulatory requirements.

Finally, IoT networks require scalable and adaptive security mechanisms that can operate efficiently in highly dynamic environments. As the number of connected devices continues to grow, security solutions must be capable of handling increasing complexity without compromising performance. Emerging approaches such as AI-based threat detection and Zero Trust architectures are being explored to enhance the adaptability and robustness of IoT security frameworks.

In conclusion, the security requirements for IoT-based telecommunication networks extend beyond traditional cybersecurity principles, requiring specialized approaches tailored to the unique characteristics of IoT systems. Achieving confidentiality, integrity, availability, authentication, and privacy in such environments demands the integration of lightweight cryptography, efficient key management, and scalable security architectures to ensure the safe and reliable operation of next-generation networks.

**Existing security solutions.** The rapid expansion of the Internet of Things (IoT) in telecommunication networks has led to the development of a wide range of security solutions aimed at mitigating the diverse threats associated with these systems. Given the unique characteristics of IoT environments, including resource-constrained devices, heterogeneous architectures, and large-scale deployment, traditional cybersecurity mechanisms alone are insufficient. As a result, researchers and industry practitioners have proposed specialized approaches that combine lightweight cryptography, secure communication protocols, intelligent monitoring systems, and emerging technologies to enhance overall network security.

One of the most fundamental approaches to securing IoT systems is the use of cryptographic techniques. Encryption plays a crucial role in ensuring data confidentiality and integrity during transmission and storage. Symmetric encryption algorithms, such as the Advanced Encryption Standard (AES), are widely used due to their efficiency and relatively low computational overhead, making them suitable for constrained IoT devices. In addition, asymmetric cryptographic methods, including RSA and elliptic curve cryptography (ECC), are employed for secure key exchange and authentication processes. ECC, in particular, is considered more suitable for IoT environments because it provides strong security with smaller key sizes, thereby reducing computational and energy requirements.

Secure communication protocols also form a critical component of IoT security solutions. Protocols such as Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) are widely used to provide end-to-end encryption and secure data transmission over networks. For lightweight IoT applications, specialized protocols such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) are often enhanced with security extensions to ensure safe communication between devices, gateways, and cloud platforms. These protocols help protect against common network threats, including eavesdropping and man-in-the-middle attacks.

Another important class of security solutions involves intrusion detection and prevention systems (IDS/IPS), which are designed to monitor network traffic and detect abnormal or malicious activities. Traditional signature-based detection methods are increasingly being complemented by anomaly-based approaches that leverage machine learning techniques to identify previously unknown threats. Artificial intelligence (AI) and deep learning models are being actively integrated into IoT security frameworks to enable real-time threat detection, predictive analysis, and automated response mechanisms. These intelligent systems enhance the ability to detect complex and evolving cyberattacks in large-scale IoT environments.

In recent years, blockchain technology has emerged as a promising solution for addressing security and trust issues in IoT networks. By providing a decentralized and tamper-resistant ledger, blockchain can be used to secure data transactions, manage device identities, and ensure transparency in communication processes. This approach eliminates the need for centralized authorities and reduces the risk of single points of failure. However, challenges related to scalability, latency, and energy consumption still limit the widespread adoption of blockchain in IoT systems.

Edge computing has also been increasingly utilized as a security-enhancing mechanism in IoT-based telecommunication networks. By processing data closer to the source, edge computing reduces the need to transmit sensitive information over long distances, thereby minimizing exposure to network-based attacks. Additionally, edge nodes can perform local security functions such as data filtering, anomaly detection, and access control, improving both security and system responsiveness.

Furthermore, modern IoT security solutions incorporate identity and access management (IAM) frameworks to ensure that only authorized devices and users can interact with the network. These frameworks include authentication mechanisms, role-based access control, and secure credential management systems. In large-scale IoT deployments, automated identity management and scalable authentication protocols are essential for maintaining system integrity.

### References:

1. L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014. <https://doi.org/10.1109/TII.2014.2300753>
2. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015. <https://doi.org/10.1109/COMST.2015.2444095>
3. D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco White Paper, 2011. [https://www.cisco.com/c/dam/en\\_us/about/ac79/docs/innov/IoT\\_IBSG\\_0411FINAL.pdf](https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf)
4. M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A Survey on the Security of IoT Frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018. <https://doi.org/10.1016/j.jisa.2017.11.002>
5. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015. <https://doi.org/10.1016/j.comnet.2014.11.008>
6. K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in *Proceedings of the 9th International Conference on Computational Intelligence and Security*, 2013. <https://doi.org/10.1109/CIS.2013.145>
7. J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015. <https://doi.org/10.1109/COMST.2015.2388550>
8. M. Abomhara and G. M. Køien, "Security and Privacy in the Internet of Things: Current Status and Open Issues," in *International Conference on Privacy and Security in Mobile Systems*, 2014. <https://doi.org/10.1109/PRISMS.2014.6970594>



9. E. Bertino and N. Islam, “Botnets and Internet of Things Security,” *Computer*, vol. 50, no. 2, pp. 76–79, 2017. <https://doi.org/10.1109/MC.2017.62>
10. Butun, P. Österberg, and H. Song, “Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2020. <https://doi.org/10.1109/COMST.2019.2953364>

## МАЗМҰНЫ – СОДЕРЖАНИЕ – CONTENT

### ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖӘНЕ ҚҰҚЫҚ ҒЫЛЫМДАРЫ - СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ И ЮРИДИЧЕСКИЕ НАУКИ - SOCIO-ECONOMIC AND LEGAL SCIENCES

Төлегенов Тимур Сейфуллаулы

**ДИНАМИКА ТУРИСТСКИХ ПОТОКОВ И ЭФФЕКТИВНОСТЬ ИНФРАСТРУКТУРЫ  
ТУРКЕСТАНА: ОТ ЭКСТЕНСИВНОГО РОСТА К СМАРТ-УПРАВЛЕНИЮ ..... 10**

Alexander Gorevoy

**WHICH INEQUALITY STATISTICS SURVIVE AN ADMINISTRATIVE BOUNDARY CHANGE?  
EVIDENCE FROM KAZAKHSTAN, 2010–2023 ..... 14**

Rakhimov Djalil

**DOES THE SHIFT TO CASHLESS PAYMENTS GO TOGETHER WITH FASTER GROWTH IN  
HOUSEHOLD CREDIT? EVIDENCE FROM THE REGIONS OF KAZAKHSTAN, 2023-2025 ..... 26**

Kazhgerey Asan

**HOW MANY FOOD BASKETS DOES AN AVERAGE WAGE BUY? WAGES AND FOOD PRICES IN  
THE 20 REGIONS OF KAZAKHSTAN, 2024-2026 ..... 37**

Tagimova Alua

**WHO WAS LEFT BEHIND? EDUCATION AND FINANCIAL INCLUSION IN KAZAKHSTAN AND  
THREE CENTRAL ASIAN NEIGHBOURS, 2021-2024 ..... 44**

Wei Wei, Mynzhanova Gulzhakan, Niyetalina Gaukhar

**DIGITAL–PHYSICAL INTEGRATION AND ECONOMIC PERFORMANCE IN INDUSTRIAL  
INTEGRATED ENERGY SYSTEMS: A SCENARIO-BASED ANALYSIS OF SMART GRID  
CONTROL, BATTERY ENERGY STORAGE, AND DIGITAL TWINS ..... 51**

Xu Fumin, Wei Wei, Ruziyeva Elvira, Moldabekova A.

**FROM CULTURAL RESOURCES TO GLOBAL CONSUMER VALUE: THE BRIDGE–IMC MODEL  
AND THE INTERNATIONALIZATION OF BLACK MYTH: WUKONG UNDER THE BELT AND  
ROAD INITIATIVE ..... 64**

Ibraimkhan Alikhan

**WHICH CRIMES CAN A 14-YEAR-OLD BE TRIED FOR? THE LIST IN ARTICLE 15 OF  
KAZAKHSTAN'S CRIMINAL CODE COMPARED WITH 30 OTHER JURISDICTIONS ..... 80**

Yerboluly Madi

**DID IMPORTED CARS REALLY GET CHEAPER? CHINESE CARS AND THE AVERAGE  
CUSTOMS VALUE OF PASSENGER CARS IMPORTED INTO KAZAKHSTAN, 2015-2025 ..... 91**

Салимбаев Ербол Аманжолович

**АНАЛИЗ ИНВЕСТИЦИОННОЙ АКТИВНОСТИ КАК ИНДИКАТОР ИЗМЕНЕНИЙ  
ПОТЕНЦИАЛЬНОГО СПРОСА НА КОНСАЛТИНГОВЫЕ УСЛУГИ ..... 99**

Rambergenov Ramil

**REGIONAL NEW-FIRM FORMATION IN UZBEKISTAN AFTER THE 2017 REFORMS:  
PERSISTENCE IN SCALE, CONVERGENCE IN INTENSITY, AND RECOMPOSITION TOWARD  
TRADE ..... 107**

Abdesh Dinara

**FROM A WOMEN'S LEAD TO A MEN'S LEAD: THE GENDER GAP IN DIGITAL PAYMENTS IN  
KAZAKHSTAN AND THREE CENTRAL ASIAN NEIGHBOURS, 2021-2024 ..... 116**

Amangeldi Aidana

**DID SMALL BUSINESS IN KAZAKHSTAN REALLY SHRINK IN 2026? THE NEW TAX CODE,  
REGIONAL TAX RATES AND THE FALL IN THE NUMBER OF INDIVIDUAL ENTREPRENEURS ..... 124**

|                                                                                                                                                      |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| Cheng Che                                                                                                                                            |            |
| <b>BUILD, BUY, OR PARTNER? ENTRY MODE SELECTION AND RISK GOVERNANCE FOR WIND POWER INVESTMENT IN KAZAKHSTAN .....</b>                                | <b>133</b> |
| Wang Liang                                                                                                                                           |            |
| <b>FROM CAPACITY EXPANSION TO SYSTEM VALUE: COORDINATED DEVELOPMENT OF RENEWABLE ENERGY, GRID FLEXIBILITY AND ENERGY STORAGE IN KAZAKHSTAN .....</b> | <b>146</b> |
| Chen Jun                                                                                                                                             |            |
| <b>CONSTRUCTION-PERIOD CREDIT RISK MANAGEMENT FOR LARGE INFRASTRUCTURE PROJECT FINANCE IN KAZAKHSTAN .....</b>                                       | <b>159</b> |
| Alniyaz Danial                                                                                                                                       |            |
| <b>HOW MUCH FUEL DOES A HYBRID REALLY SAVE? A SAME-MODEL COMPARISON OF HYBRID AND GASOLINE CARS IN US FUEL ECONOMY .....</b>                         | <b>173</b> |

#### **ТЕХНИКАЛЫҚ ҒЫЛЫМДАР - ТЕХНИЧЕСКИЕ НАУКИ - TECHNICAL SCIENCE**

|                                                                                                                                                                                 |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| Nurmakhan Almira                                                                                                                                                                |            |
| <b>ADVANTAGES OF FIBER OPTIC COMMUNICATION OVER TRADITIONAL COPPER CABLES .....</b>                                                                                             | <b>180</b> |
| Kozhabai Bereke                                                                                                                                                                 |            |
| <b>SECURITY CHALLENGES IN IOT-BASED TELECOMMUNICATION NETWORKS .....</b>                                                                                                        | <b>188</b> |
| Azamatuly Yerassyl                                                                                                                                                              |            |
| <b>WHY AI-GENERATED CODE FAILS A BENCHMARK: A FAILURE ANALYSIS OF THREE OPEN LANGUAGE MODELS ON 30 HUMANEVAL+ TASKS .....</b>                                                   | <b>197</b> |
| Nurzhan Sanzhar                                                                                                                                                                 |            |
| <b>A FEW SHELLS, A FEW OPERATORS: WHERE LOW EARTH ORBIT IS CROWDED IN AN ALTITUDE-INCLINATION MAP OF 16,620 ACTIVE SATELLITES .....</b>                                         | <b>206</b> |
| Askarbek Nurislam                                                                                                                                                               |            |
| <b>CAN THE WEATHER TELL WHICH DAYS IN ASTANA WILL BE POLLUTED? CLASSIFYING PM2.5 EXCEEDANCE DAYS WITH MACHINE LEARNING AND CHECKING THE DATA AGAINST A GROUND MONITOR .....</b> | <b>212</b> |
| Iliyas Arman                                                                                                                                                                    |            |
| <b>SHOOTING ON THE MOVE: HOW MUCH AIM A ROBOT LOSES BY IGNORING ITS OWN VELOCITY, AND WHETHER A VIRTUAL-TARGET CORRECTION RECOVERS IT .....</b>                                 | <b>223</b> |
| Ануар Әлімжан Бахытжанұлы, Сексенбаева Айша Курманбековна                                                                                                                       |            |
| <b>СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТАНДАРТОВ И МЕТОДИК ОБУЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ: NICE FRAMEWORK, ECSF И ПРАКТИКО- ОРИЕНТИРОВАННЫЕ ТЕХНОЛОГИИ .....</b>                                  | <b>229</b> |
| Mukhamedzhan Yerganat                                                                                                                                                           |            |
| <b>GROWTH OF GITHUB DEVELOPER COMMUNITIES IN KAZAKHSTAN, UZBEKISTAN AND KYRGYZSTAN, 2020-2026: EVIDENCE FROM THE GITHUB INNOVATION GRAPH .....</b>                              | <b>239</b> |

#### **ПӘНДЕР АРАЛЫҚ ҒЫЛЫМДАР – МЕЖДИСЦИПЛИНАРНЫЕ НАУКИ – INTERDISCIPLINARY SCIENCES**

|                                                                                                                                       |            |
|---------------------------------------------------------------------------------------------------------------------------------------|------------|
| Albiyev Asser                                                                                                                         |            |
| <b>HOW MUCH OF AN ARTICLE COUNT IS HUMAN WORK? DECOMPOSING THE CREATION OF FIVE WIKIPEDIAS, 2010–2025 .....</b>                       | <b>251</b> |
| Amangeldy Nurbolat                                                                                                                    |            |
| <b>HOW MUCH OF KAZAKHSTAN'S URBAN BUILT STOCK PREDATES ITS SEISMIC CODES, AND WHERE DOES THAT STOCK SIT RELATIVE TO HAZARD? .....</b> | <b>261</b> |

Torekhan Sabrina

|                                                                                                             |            |
|-------------------------------------------------------------------------------------------------------------|------------|
| <b>WHERE ALMATY WALKS ITS OWN WAY: INFORMAL SHORTCUTS IN OPENSTREETMAP AND THE DETOURS THEY AVOID .....</b> | <b>267</b> |
|-------------------------------------------------------------------------------------------------------------|------------|

## **ӘЛЕУМЕТТІК ЖӘНЕ ГУМАНИТАРЛЫҚ ҒЫЛЫМДАР - СОЦИАЛЬНО-ГУМАНИТАРНЫЕ НАУКИ - SOCIAL SCIENCES AND HUMANITIES**

Мұқатаева Айзат Амантайқызы, Стамбекова Жанат Байғазықызы, Слямханова Гүлім Болатқызы, Қызырбек Аяулым Ерболқызы

|                                                                                                              |            |
|--------------------------------------------------------------------------------------------------------------|------------|
| <b>ЖАСАНДЫ ИНТЕЛЛЕКТ ДӘУІРІНДЕГІ ҒЫЛЫМИ ТАНЫМ: ПОППЕР, КУН ЖӘНЕ ЛАКАТОС ИДЕЯЛАРЫ ТҮРҒЫСЫНАН ТАЛДАУ .....</b> | <b>272</b> |
|--------------------------------------------------------------------------------------------------------------|------------|

Мұқатаева Айзат Амантайқызы, Сапарханова Мадина Төлегенқызы, Окенова Аружан Муратхановна, Тұрсынғазыева Ақерке Ерболатқызы

|                                                                               |            |
|-------------------------------------------------------------------------------|------------|
| <b>ШӘКӘРІМ ФИЛОСОФИЯСЫНДАҒЫ ЕРКІНДІК ЖӘНЕ МОРАЛЬДЫҚ ТАҢДАУ МӘСЕЛЕСІ .....</b> | <b>282</b> |
|-------------------------------------------------------------------------------|------------|

Komekova Saida

|                                                                                                                                 |            |
|---------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>DO UNHAPPY REVIEWERS MIX IN MORE RUSSIAN? STAR RATINGS AND KAZAKH-RUSSIAN CODE-SWITCHING IN 175,002 ONLINE REVIEWS .....</b> | <b>291</b> |
|---------------------------------------------------------------------------------------------------------------------------------|------------|

Zhumagali Yerbol

|                                                                                                                                                                       |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>DOES A BIGGER MODEL CLOSE THE GAP? KAZAKH-LANGUAGE ACCURACY ON KAZAKHSTAN-SPECIFIC VERSUS UNIVERSAL SCHOOL SUBJECTS IN SMALL OPEN-WEIGHT LANGUAGE MODELS .....</b> | <b>304</b> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|

Abdrakhmanova Madina

|                                                                                                                           |            |
|---------------------------------------------------------------------------------------------------------------------------|------------|
| <b>DOES A MEDAL BUY ATTENTION? WIKIPEDIA VIEWS OF KAZAKHSTAN'S ATHLETES BEFORE AND AFTER THE PARIS 2024 OLYMPIC .....</b> | <b>308</b> |
|---------------------------------------------------------------------------------------------------------------------------|------------|

## **ПЕДАГОГИКАЛЫҚ ЖӘНЕ ПСИХОЛОГИЯЛЫҚ ҒЫЛЫМДАР – ПЕДАГОГИЧЕСКИЕ И ПСИХОЛОГИЧЕСКИЕ НАУКИ – PEDAGOGICAL AND PSYCHOLOGICAL SCIENCES**

Kaldarbek Mergen

|                                                                                                                        |            |
|------------------------------------------------------------------------------------------------------------------------|------------|
| <b>FAMILY OR SCHOOL? SOCIOECONOMIC COMPOSITION AND MATHEMATICS ACHIEVEMENT IN KAZAKHSTAN, PISA 2022 AND 2025 .....</b> | <b>316</b> |
|------------------------------------------------------------------------------------------------------------------------|------------|

Zhenis Adilzhan

|                                                                                                                                                |            |
|------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>WHICH OLYMPIAD PROBLEMS DO STUDENTS TAKE TO THE BOARD? CHOICES AND DEFENCES IN THE 8TH-GRADE LEAGUE OF KARAGANDY MATHBATTLES 2026 .....</b> | <b>323</b> |
|------------------------------------------------------------------------------------------------------------------------------------------------|------------|

Базарбаева Айнура Бектуровна

|                                                                                                                                           |            |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>ДЕТСКИЙ ФОЛЬКЛОР И ПОДВИЖНЫЕ ИГРЫ КАК ИНСТРУМЕНТЫ ФОРМИРОВАНИЯ ОСНОВ ПРАВОВОЙ КУЛЬТУРЫ У ДЕТЕЙ СТАРШЕГО ДОШКОЛЬНОГО ВОЗРАСТА .....</b> | <b>330</b> |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------|

## **БИОЛОГИЯ ҒЫЛЫМДАР - БИОЛОГИЧЕСКИЕ НАУКИ - BIOLOGICAL SCIENCES**

Bazhenova Diana

|                                                                                                                     |            |
|---------------------------------------------------------------------------------------------------------------------|------------|
| <b>GROWTH DYNAMICS OF STERLET (<i>Acipenser ruthenus</i> L.) REARED IN A RECIRCULATING AQUACULTURE SYSTEM .....</b> | <b>333</b> |
|---------------------------------------------------------------------------------------------------------------------|------------|

## **ТУРИСТИЧЕСКИЕ И СПОРТИВНЫЕ НАУКИ - ТУРИСТІК ЖӘНЕ СПОРТ ҒЫЛЫМДАРЫ - TOURISM AND SPORTS SCIENCES**

Төлеп Жазира Маратқызы

|                                                                                                                        |            |
|------------------------------------------------------------------------------------------------------------------------|------------|
| <b>ГАСТРОНОМИЯЛЫҚ ФЕСТИВАЛЬДЕРДІҢ ТУРИСТІК ДЕСТИНАЦИЯ ТАРТЫМДЫЛЫҒЫН ҚАЛЫПТАСТЫРУДАҒЫ РӨЛІ МЕН ДАМУ ҮРДІСТЕРІ .....</b> | <b>340</b> |
|------------------------------------------------------------------------------------------------------------------------|------------|

**ЕСТЕСТВЕННЫЕ НАУКИ - ЖАРАТЫЛЫСТАНУ ҒЫЛЫМДАРЫ - NATURAL SCIENCES**

Нургельдина Асель Ермаковна, Серикбаева Жанерке Алимжановна

**ШЕКАРАСЫЗ ФИЗИКА: ӘР ЕЛДЕГІ ФИЗИКАЛЫҚ БІЛІМДІ САЛЫСТЫРУ ..... 347**