

Моя профессиональная
карьера

ISSN

INTERNATIONAL
STANDARD
SERIAL
NUMBER

ISSN

2782-4365

Проверить
номер:



Научно-образовательный электронный журнал

ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ

Выпуск №78-3 (том 2)
(сентябрь), 2026)

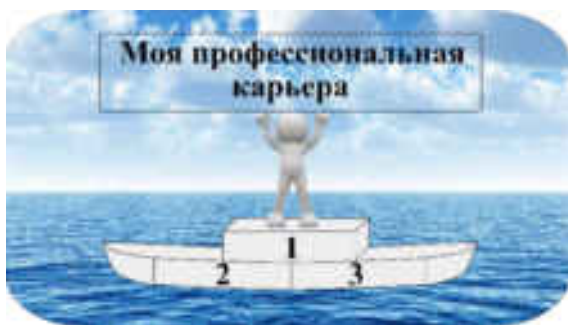


Google
Scholar



Периодичность выпуска: 1 раз в неделю

Сайт: mpcareer.ru/oinv21veke. Почта: obrmppcareer@mail.ru



Международный научно-образовательный
электронный журнал
«ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ»

ISSN 2782-4365

УДК 37

ББК 94

**Международный научно-образовательный электронный журнал
«ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ». Выпуск №78-3 (том 2) (сентябрь,
2026). Дата выхода в свет: 21.09.2026.**

Журнал объединяет авторов на территории стран СНГ и помогает обмениваться передовыми научно-образовательными исследованиями.

Содержит научные работы отечественных и зарубежных авторов по экономическим, техническим, философским, юридическим и другим наукам.

Миссия научно-образовательного электронного журнала «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ» состоит в поддержке интереса читателей к оригинальным исследованиям и инновационным подходам в различных тематических направлениях, которые способствуют распространению лучшей отечественной и зарубежной практики в интернет пространстве.

Целевая аудитория журнала охватывает работников сферы науки и образования (педагоги, учителя, ученые, преподаватели, научные сотрудники, бакалавры, магистранты, аспиранты).

Материалы публикуются в авторской редакции. За соблюдение законов об интеллектуальной собственности и за содержание работ ответственность несут авторы работ. Мнение редакции может не совпадать с мнением авторов научных работ. При использовании и заимствовании материалов ссылка на издание обязательна.

© ООО «МОЯ ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА»

© Коллектив авторов

Saryyev. N., Allanazarov. M., Almazov. S. DATA PRIVACY AND CYBERSECURITY CHALLENGES ACROSS MODERN TELECOMMUNICATIONS SERVICE PROVIDERS	858
Atamyradova. E., Abdyev. A., Allanazarov. E. CLOUD COMPUTING SECURITY CHALLENGES WITHIN MODERN TELECOMMUNICATIONS NETWORKS AND SERVICES	868
Раззаков Батырхан, Хемраев Акрамджан, Сапаров Улугбек СОВРЕМЕННЫЕ МЕТОДЫ ХИМИЧЕСКОГО АНАЛИЗА И ИХ ПРИМЕНЕНИЕ В ПРОМЫШЛЕННОСТИ	878
Раззаков Батырхан, Рахманкулова Тазегуль, Ергешов Рустем ЗЕЛЁНАЯ ХИМИЯ КАК ОСНОВА ЭКОЛОГИЧЕСКИ БЕЗОПАСНОГО ПРОМЫШЛЕННОГО ПРОИЗВОДСТВА	888
Suvhanov. D., Yamadova. S., Abayev Yakub QUANTUM COMPUTING IMPLICATIONS FOR TELECOMMUNICATIONS CYBERSECURITY AND DATA PROTECTION STRATEGIES	898
Годжаева Огульсона, Ялкапова Кякилик МАРКЕТИНГ НАЦИОНАЛЬНОГО ИСКУССТВА И КУЛЬТУРНОГО НАСЛЕДИЯ	908
Марал Реджепмырадовна Ходжакулиева, Аннабердиева Айсолтан Гуванджовна РОЛЬ НАЦИОНАЛЬНОГО НАСЛЕДИЯ В ВОСПИТАНИИ ПОДРАСТАЮЩЕГО ПОКОЛЕНИЯ	916
Моллаева Ширин, Пыгамова Серви, Таджова Оразгуль ХОРЕОГРАФИЧЕСКОЕ ИСКУССТВО В СИСТЕМЕ ХУДОЖЕСТВЕННОГО ОБРАЗОВАНИЯ: ПЕДАГОГИЧЕСКИЙ ПОТЕНЦИАЛ ТАНЦЕВАЛЬНОГО ИСКУССТВА	927
Жураева Умида СОПОСТАВИТЕЛЬНЫЙ АНАЛИЗ ОБРАЗОВ МАРТИНА ИДЕНА И ЕВГЕНИЯ БАЗАРОВА В КОНТЕКСТЕ ЭВОЛЮЦИИ ГЕРОЯ-РЕАЛИСТА	937
Аллабердиева Ширин, Аннамухаммедова Язгюл ТРАНСФОРМАЦИЯ ФИНАНСОВОГО ПОВЕДЕНИЯ МОЛОДЕЖИ И СОВРЕМЕННОГО ОБЩЕСТВА В ЭПОХУ МОБИЛЬНОГО БАНКИНГА, БЕСКОНТАКТНЫХ ПЛАТЕЖЕЙ И БЛОКЧЕЙН-ТЕХНОЛОГИЙ	942
Тойлыева Айсона ХРОМАТОГРАФИЧЕСКИЕ МЕТОДЫ АНАЛИЗА В КОНТРОЛЕ КАЧЕСТВА ЛЕКАРСТВЕННЫХ СРЕДСТВ ПРОБЛЕМЫ, СОВРЕМЕННЫЕ ТЕНДЕНЦИИ И ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ	951

ФИО автора(-ов): *Atamyradova. E.*

*Lecturer, Institute of telecommunications and
Informatics of Turkmenistan*

Abdyev. A.

*Student, Institute of telecommunications and
Informatics of Turkmenistan*

Allanazarov. E.

*Student, Institute of telecommunications and
Informatics of Turkmenistan*

Название публикации: «CLOUD COMPUTING SECURITY CHALLENGES
WITHIN MODERN TELECOMMUNICATIONS NETWORKS AND SERVICES»

Abstract

Cloud computing has become an essential component of modern telecommunications networks, enabling scalable service delivery, virtualization, distributed processing, and rapid deployment of digital applications. However, the integration of cloud infrastructure into telecommunications environments introduces significant cybersecurity challenges related to data protection, identity management, misconfiguration, virtualization, application interfaces, multi-tenancy, and third-party dependence. This study examines the principal cloud security risks affecting telecommunications networks and services through a qualitative methodology based on structured literature analysis, thematic classification, and comparative assessment. The findings indicate that cloud-related security failures often emerge from complex interactions between technical vulnerabilities and organizational weaknesses rather than from isolated system defects. The study concludes that telecommunications providers require integrated security architectures incorporating zero-trust principles, strong identity management, encryption, continuous monitoring, secure configuration, workload isolation, supply-chain governance, and resilient incident-response capabilities to protect cloud-based infrastructure effectively.

Introduction

Cloud computing has transformed the architecture and operation of modern telecommunications networks. Telecommunications providers increasingly rely on cloud platforms to support network functions, data processing, customer services, billing systems, storage, analytics, artificial intelligence applications, and digital service delivery. The migration from traditional hardware-centric infrastructure toward virtualized and cloud-native environments has enabled greater scalability, flexibility, automation, and operational efficiency.

The development of fifth-generation mobile networks has accelerated this transformation. Modern telecommunications systems increasingly employ network function virtualization, software-defined networking, containerized applications, edge computing, and distributed cloud architectures. Functions that were previously implemented through dedicated physical equipment can now operate as software workloads within virtual machines or containers. This architectural evolution allows service providers to deploy and modify network functions rapidly, but it also creates new security dependencies.

Cloud adoption changes the traditional security model of telecommunications infrastructure. Conventional network security frequently relied on clearly defined boundaries between internal and external systems. Cloud environments are more dynamic and distributed. Data, applications, workloads, and users may operate across multiple regions, platforms, devices, and administrative domains. Consequently, security cannot depend exclusively on network location or perimeter controls.

Modern telecommunications providers also operate in complex ecosystems involving public cloud companies, private cloud infrastructure, software vendors, managed service providers, equipment manufacturers, contractors, and application developers. This interdependence expands the number of entities that influence cybersecurity outcomes. A vulnerability within an external service provider or software dependency may indirectly expose telecommunications systems even when the operator's internal controls are otherwise effective.

The purpose of this study is to examine the principal cloud computing security challenges affecting modern telecommunications networks and services. The research

considers identity compromise, cloud misconfiguration, virtualization risks, application programming interfaces, multi-tenancy, data security, supply-chain vulnerabilities, distributed denial-of-service attacks, and operational governance. The study also evaluates defensive strategies appropriate for highly distributed cloud-based telecommunications environments.

The importance of this topic derives from the critical role of telecommunications services in contemporary society. Cloud-related failures within telecommunications networks can affect financial systems, healthcare, transportation, emergency communications, public administration, and commercial activity. Therefore, protecting cloud-integrated telecommunications infrastructure is essential for both organizational cybersecurity and broader digital resilience.

Literature Review

Existing research indicates that cloud computing introduces both security advantages and new categories of risk within telecommunications environments. Cloud platforms can provide advanced security services, centralized monitoring, rapid patching, redundancy, and automated management. However, these benefits depend heavily on correct configuration, identity governance, and clearly defined responsibility between cloud providers and telecommunications operators.

Keller and Romano (2023) identify cloud misconfiguration as one of the most persistent security concerns in telecommunications environments. Inadequately configured storage resources, open administrative interfaces, excessive privileges, exposed management ports, and improper network policies can unintentionally make sensitive systems accessible. Their research emphasizes that many cloud security incidents result not from sophisticated exploitation but from administrative error.

Identity and access management represents another central concern. Schneider and Bellini (2024) argue that cloud environments shift security toward identity-based control because users, workloads, services, and machines frequently communicate across distributed infrastructure. Compromised administrative credentials can provide extensive access to cloud resources, particularly when accounts possess excessive

privileges. Traditional assumptions that internal users or workloads can be automatically trusted are therefore increasingly unsuitable.

Virtualization creates additional risks. Telecommunications providers rely on virtual machines, containers, orchestration platforms, and virtualized network functions to increase flexibility and resource utilization. Baumann and Moretti (2024) note that vulnerabilities in hypervisors, container runtimes, orchestration systems, or management interfaces may affect multiple workloads simultaneously. Shared infrastructure can consequently create concentrated points of failure.

Application programming interfaces have also become fundamental to cloud-based telecommunications. Interfaces enable automated communication between cloud services, billing systems, network functions, applications, and management platforms. Weak authentication, exposed credentials, insufficient input validation, and excessive API permissions may allow attackers to interact directly with sensitive services.

Multi-tenancy is another important issue. Cloud providers may host resources belonging to multiple customers on shared infrastructure. Strong logical separation is therefore essential. Fischer and Whitmore (2025) argue that isolation failures, insecure virtualization, or configuration errors can undermine separation between tenants and create risks to confidentiality and integrity.

Data protection remains a persistent challenge. Telecommunications providers process personal data, billing information, metadata, customer records, authentication information, and operational telemetry. When such information is stored or processed in cloud environments, organizations must manage encryption, access control, backup security, retention practices, and data location requirements.

The existing literature nevertheless shows a recurring limitation. Many studies focus narrowly on particular technical risks, such as virtualization vulnerabilities or identity compromise, without examining how these problems interact within operational telecommunications ecosystems. This study addresses that gap by evaluating cloud security as an integrated technical and organizational challenge.

Materials and Methods

This research employed a qualitative methodology based on structured literature analysis, thematic categorization, and comparative assessment. The approach was selected because the objective was to identify recurring cloud security challenges across telecommunications environments rather than evaluate a single provider or technological platform.

The research material consisted of academic studies addressing cloud computing, telecommunications cybersecurity, virtualization, identity management, application programming interfaces, distributed infrastructure, data protection, and cyber resilience. Sources were examined according to their relevance to cloud-based telecommunications networks and services.

The analytical procedure categorized security challenges into several domains. These included cloud misconfiguration, identity and credential compromise, insecure application interfaces, virtualization vulnerabilities, multi-tenancy risks, data exposure, third-party dependency, distributed denial-of-service threats, and governance weaknesses. Each category was evaluated according to its potential effect on confidentiality, integrity, availability, and service continuity.

A comparative assessment was also conducted between traditional perimeter-oriented security and cloud-adapted approaches. Conventional security controls were examined in relation to static boundaries and centralized infrastructure. Modern approaches were evaluated according to zero-trust principles, continuous authentication, least-privilege access, workload segmentation, encryption, automated monitoring, and adaptive incident response.

The study additionally incorporated a lifecycle perspective. Security controls were considered during architecture design, procurement, configuration, deployment, operation, updating, monitoring, incident response, and retirement. This framework was used because cloud security weaknesses frequently originate from design or configuration decisions made long before an actual attack occurs.

The methodology did not attempt to rank specific cloud providers or security products. Instead, it focused on recurring structural and operational risks applicable

across different telecommunications environments. This approach allowed the research to emphasize general security principles rather than vendor-specific characteristics.

Results

The analysis identified cloud misconfiguration as one of the most significant security risks affecting telecommunications providers. Incorrect access policies, exposed storage resources, open interfaces, and unnecessary services can create direct pathways into sensitive infrastructure. Because cloud environments are highly dynamic, configuration errors may also propagate quickly across multiple workloads.

Identity compromise emerged as another major concern. Administrative accounts, service accounts, application credentials, and cryptographic keys can provide extensive control over cloud resources. Attackers who obtain legitimate credentials may bypass several traditional defenses and perform actions that appear to originate from authorized users.

Application programming interfaces were found to represent a substantial attack surface. Telecommunications systems rely heavily on automated service interaction, and insecure interfaces can expose network functions, customer information, and administrative operations. Strong authentication, authorization, input validation, and monitoring are therefore essential.

Virtualization and containerization introduce additional challenges. Shared physical infrastructure can host many virtualized telecommunications functions. Vulnerabilities within hypervisors, orchestration platforms, or container environments may therefore affect multiple services simultaneously. Effective isolation is particularly important where workloads have different sensitivity levels.

The analysis also found that multi-cloud and hybrid-cloud strategies increase operational complexity. Telecommunications providers may distribute workloads across private infrastructure, public cloud platforms, and edge locations. This can create inconsistent security policies, fragmented monitoring, and differences in access controls.

Data security remains a central concern. Encryption can reduce confidentiality risks, but poor key management can undermine otherwise strong protection. Excessive data retention can also increase the consequences of compromise.

Supply-chain dependency was identified as another systemic challenge. Telecommunications providers frequently depend on external software, cloud platforms, open-source libraries, and managed services. A compromised dependency can introduce vulnerabilities through trusted channels.

Finally, the results indicate that conventional perimeter-based security is insufficient for distributed cloud environments. Continuous verification, segmentation, identity-centered security, monitoring, and automated response provide stronger alignment with the operational characteristics of cloud-based telecommunications networks.

Discussion

The findings reinforce the argument that cloud security within telecommunications infrastructure is primarily a problem of distributed trust and complexity. Keller and Romano's (2023) emphasis on misconfiguration is consistent with the present study, which identifies administrative error as a major source of cloud exposure. Security controls may be technically strong while still failing when resources are incorrectly configured.

The findings concerning identity management also support Schneider and Bellini's (2024) position that identity has become a primary security boundary in cloud environments. Telecommunications providers should therefore limit administrative privileges, implement multifactor authentication, rotate credentials, monitor privileged activity, and avoid excessive access rights.

Zero-trust architecture provides a useful response to this problem. Rather than assuming that users or workloads are trustworthy because of network location, access should be verified continuously. Least-privilege permissions and segmentation can reduce the impact of compromised identities.

The virtualization findings correspond with Baumann and Moretti's (2024) research. Virtualization improves efficiency, but concentration of multiple services on

common infrastructure can amplify the effects of compromise. Telecommunications providers should therefore strengthen hypervisor security, container isolation, orchestration controls, and vulnerability management.

Multi-tenancy presents similar concerns. Fischer and Whitmore (2025) emphasize that shared infrastructure requires dependable isolation mechanisms. Logical separation must be supported by strong configuration, monitoring, and access control to prevent unauthorized interaction between workloads.

The study also demonstrates that cloud security is inseparable from supply-chain governance. Telecommunications providers cannot fully protect their infrastructure if external vendors, software dependencies, or cloud platforms introduce vulnerabilities. Vendor assessment, secure procurement, software-component visibility, and vulnerability disclosure processes are therefore essential.

Data governance should also be integrated into cloud security strategy. Encryption, retention limits, access control, and secure deletion reduce the consequences of compromise. Telecommunications organizations should avoid unnecessary data accumulation because larger datasets create greater exposure during breaches.

Continuous monitoring is equally important. Cloud infrastructure changes rapidly, and static security reviews may become outdated soon after deployment. Automated configuration assessment, threat detection, and behavioral monitoring can help identify vulnerabilities and suspicious activity more quickly.

The broader implication is that cloud computing security requires organizational transformation as well as technical controls. Network engineering, cloud operations, cybersecurity, software development, privacy, procurement, and management teams must coordinate security responsibilities. Fragmented governance can create gaps between cloud architecture and operational security.

Conclusion

Cloud computing has become integral to modern telecommunications networks and services, but its benefits are accompanied by substantial cybersecurity challenges. This study identified cloud misconfiguration, identity compromise, insecure

application programming interfaces, virtualization vulnerabilities, multi-tenancy risks, data exposure, third-party dependency, and distributed infrastructure complexity as major areas of concern.

The analysis demonstrates that traditional perimeter-based security is insufficient for cloud-integrated telecommunications environments. Effective protection requires zero-trust principles, strong identity management, least-privilege access, encryption, segmentation, continuous monitoring, secure configuration, resilient incident response, and coordinated supply-chain governance.

The principal contribution of this study is its integrated treatment of cloud security as both a technical and organizational challenge. Security must be embedded throughout the cloud infrastructure lifecycle rather than introduced only after deployment. Telecommunications providers should treat cloud cybersecurity as a continuous process involving architecture, configuration, monitoring, governance, and recovery.

Future research should examine cloud security in sixth-generation telecommunications, edge-cloud integration, artificial intelligence-driven network management, confidential computing, privacy-preserving analytics, post-quantum security, and automated cloud defense. As telecommunications infrastructure becomes increasingly cloud-native, the ability to manage distributed trust, shared responsibility, and rapidly changing digital environments will remain fundamental to maintaining secure, resilient, and dependable communication services.

References

Baumann, L. H., & Moretti, A. R. (2024). Virtualization security and cloud-native network functions in modern telecommunications infrastructure. *International Journal of Cloud and Network Security*, 16(2), 119–138.

Fischer, M. J., & Whitmore, E. P. (2025). Multi-tenancy, distributed trust, and resilience in telecommunications cloud environments. *Journal of Critical Digital Infrastructure Security*, 13(1), 51–70.

Keller, T. M., & Romano, F. G. (2023). Cloud misconfiguration and operational cybersecurity risk in telecommunications networks. *International Review of Telecommunications Security*, 18(4), 281–299.

Schneider, K. L., & Bellini, C. A. (2024). Identity-centric cybersecurity and zero-trust architectures for cloud-based communication services. *Journal of Network Security and Cloud Systems*, 11(3), 197–216.