

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)

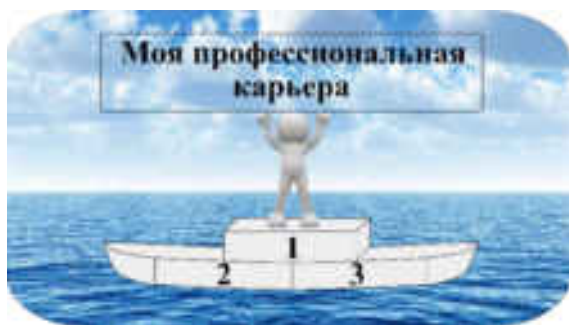


Google
Scholar



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): Saryyev. N.

*Lecturer, Institute of telecommunications and
Informatics of Turkmenistan*

Allanazarov. M.

*Student, Institute of telecommunications and
Informatics of Turkmenistan*

Almazov. S.

*Student, Institute of telecommunications and
Informatics of Turkmenistan*

Название публикации: «DATA PRIVACY AND CYBERSECURITY
CHALLENGES ACROSS MODERN TELECOMMUNICATIONS SERVICE
PROVIDERS»

Abstract

Modern telecommunications service providers operate complex digital ecosystems that process large volumes of personal, operational, and transactional data. This study examines the principal data privacy and cybersecurity challenges affecting telecommunications providers and evaluates the organizational and technical factors that intensify these risks. A qualitative methodology based on structured literature analysis, thematic classification, and comparative assessment was employed. The findings identify unauthorized data access, identity compromise, cloud misconfiguration, insecure application interfaces, insider threats, supply-chain vulnerabilities, legacy infrastructure, and regulatory fragmentation as major concerns. The analysis further indicates that privacy protection and cybersecurity are increasingly interdependent because failures in access control, network security, and data governance can directly expose sensitive information. The study concludes that telecommunications providers require integrated privacy-by-design and security-by-design strategies supported by zero-trust principles, encryption, continuous monitoring, strong identity management, data minimization, and coordinated regulatory governance.

Introduction

Telecommunications service providers form a central component of modern digital infrastructure. Mobile network operators, Internet service providers, cloud-integrated communication companies, satellite communication firms, broadband providers, and digital platform operators enable the exchange of information across individuals, businesses, governments, and critical infrastructure sectors. Their operational role requires the collection, processing, transmission, and storage of extensive quantities of information, including subscriber identities, billing records, communication metadata, location information, authentication credentials, network activity, and service usage data.

The growing dependence on telecommunications infrastructure has substantially increased the importance of both cybersecurity and data privacy. Telecommunications providers are attractive targets for cybercriminals, state-sponsored actors, insiders, and organized threat groups because compromise of these systems may provide access to highly sensitive information and strategically important network infrastructure. Unlike organizations that primarily store commercial data, telecommunications companies often maintain continuous visibility into communication patterns, device identifiers, subscriber relationships, and network behavior.

Technological modernization has further complicated this risk environment. Contemporary telecommunications networks increasingly incorporate cloud computing, software-defined networking, network function virtualization, fifth-generation mobile architecture, edge computing, Internet of Things connectivity, artificial intelligence, and application programming interfaces. These technologies improve scalability, automation, and service flexibility, but they also expand the number of systems through which sensitive data may be accessed or exposed.

Data privacy and cybersecurity are frequently treated as separate organizational concerns. Privacy focuses on lawful and appropriate collection, processing, use, retention, and disclosure of information, whereas cybersecurity emphasizes protection against unauthorized access, disruption, manipulation, and destruction. In practice, however, these areas are closely connected. A cybersecurity failure can result in a

privacy breach, while weak data governance can increase the consequences of a successful attack.

The purpose of this study is to examine the principal data privacy and cybersecurity challenges affecting modern telecommunications service providers. The study investigates technological, organizational, operational, and regulatory factors and evaluates defensive approaches capable of reducing risk. Particular attention is given to identity compromise, cloud environments, application interfaces, insider threats, legacy infrastructure, third-party dependencies, data governance, and regulatory compliance.

The significance of the study lies in the essential role telecommunications providers play in the digital economy. Failure to protect sensitive data can damage consumer trust, expose individuals to fraud or surveillance, interrupt services, generate regulatory penalties, and create risks for other sectors dependent on communications infrastructure.

Literature Review

Existing research demonstrates that telecommunications cybersecurity has evolved from a predominantly network-centered concern into a broader challenge involving data governance, cloud architecture, identity management, third-party dependencies, and privacy regulation. Traditional telecommunications security strategies concentrated on physical infrastructure, signaling systems, perimeter defenses, and controlled network boundaries. Modern service providers, however, operate increasingly distributed environments in which data travel across cloud services, mobile devices, external platforms, and virtualized systems.

Keller and Romano (2023) argue that the growing use of cloud-based telecommunications services has transformed data privacy risk. Cloud platforms permit rapid scaling and flexible deployment but distribute responsibility across telecommunications operators, cloud providers, developers, and administrators. Misconfigured storage, excessive permissions, exposed interfaces, and weak credential management can create conditions in which sensitive subscriber information becomes accessible to unauthorized parties.

Schneider and Bellini (2024) emphasize the privacy implications of metadata collection. Telecommunications providers may collect information concerning call duration, service usage, geographic movement, device identifiers, and network connections. Even where communication content remains encrypted, metadata can reveal behavioral patterns and social relationships. The authors argue that privacy protection therefore requires attention not only to message content but also to the broader information generated through telecommunications activity.

Application programming interfaces constitute another major concern. Modern telecommunications systems rely heavily on interfaces that connect network functions, customer platforms, mobile applications, billing systems, cloud services, and external providers. Insecure authentication, excessive authorization, exposed tokens, insufficient validation, and weak monitoring can allow attackers to access sensitive systems or retrieve personal information.

Baumann and Moretti (2024) identify insider threats as an important but frequently underestimated issue. Telecommunications employees, contractors, and administrators may possess extensive access to network and customer systems. Malicious insiders can deliberately misuse privileges, while accidental actions can expose data through configuration mistakes, weak security practices, or unauthorized sharing. Privileged-access management and behavioral monitoring are therefore important components of both privacy and cybersecurity protection.

Supply-chain risk has also become increasingly significant. Telecommunications service providers depend on software vendors, hardware manufacturers, cloud providers, managed security services, contractors, and open-source technologies. Fischer and Whitmore (2025) observe that vulnerabilities introduced through external suppliers may bypass conventional security boundaries because third-party systems often possess trusted access.

Legacy infrastructure presents a further challenge. Telecommunications equipment may remain operational for many years because replacement is expensive and operationally complex. Older systems may lack modern encryption, access control,

logging, and update capabilities. When integrated with cloud-based or software-defined networks, these systems can expose new pathways to sensitive information.

The literature also highlights regulatory complexity. Telecommunications providers may operate across multiple jurisdictions with different privacy requirements, data retention rules, breach notification obligations, and cross-border transfer restrictions. Existing studies often analyze cybersecurity controls or privacy compliance independently. A significant gap therefore remains in understanding how technical security and privacy governance interact across modern telecommunications environments. This study addresses that gap through an integrated analysis.

Materials and Methods

This research adopted a qualitative methodology based on structured literature analysis, thematic classification, and comparative cybersecurity assessment. The approach was selected because the objective was to identify recurring privacy and security challenges across different telecommunications service environments rather than measure the performance of a specific network operator.

The research material consisted of academic studies addressing telecommunications cybersecurity, data privacy, cloud computing, identity security, application programming interfaces, insider threats, third-party risk, regulatory governance, and critical digital infrastructure. Sources were examined according to their relevance to telecommunications service providers and their contribution to understanding the interaction between security controls and privacy obligations.

The analytical framework classified risks into several broad categories. These included unauthorized access to personal data, identity and credential compromise, cloud and infrastructure misconfiguration, application interface vulnerabilities, insider activity, legacy infrastructure exposure, supply-chain risk, excessive data collection, inadequate data retention practices, and regulatory inconsistency.

Each category was examined according to its potential impact on confidentiality, integrity, availability, and privacy. The analysis also considered the extent to which a single security incident could affect multiple data systems or services simultaneously.

This approach was particularly important because modern telecommunications infrastructure is highly interconnected.

A comparative assessment was conducted between conventional security practices and integrated privacy-security approaches. Traditional perimeter defenses were examined alongside zero-trust architecture, encryption, data minimization, privacy-by-design, multifactor authentication, privileged-access management, behavioral monitoring, secure application development, continuous vulnerability assessment, and incident-response planning.

The methodology also incorporated a lifecycle perspective. Privacy and security requirements were considered during system design, data collection, procurement, deployment, operation, maintenance, sharing, retention, and deletion. This enabled the study to assess risk as a continuous governance issue rather than a problem limited to the moment of cyberattack.

Results

The analysis identified identity compromise as one of the most significant cross-cutting risks affecting telecommunications providers. Administrative credentials, subscriber accounts, service identities, and application credentials may provide attackers with access to sensitive data and critical systems. Strong authentication and controlled privilege therefore emerged as essential defensive requirements.

Cloud environments were found to create substantial operational advantages but also introduce configuration and governance risks. Inadequately protected storage, excessive permissions, weak logging, and unclear responsibility between providers and customers may expose sensitive telecommunications data.

Application programming interfaces were also identified as a significant attack surface. Because modern telecommunications services depend on extensive machine-to-machine communication, insecure interfaces can provide direct access to customer records, billing systems, identity platforms, or network-management functions.

Insider threats remain particularly relevant because telecommunications personnel may possess broad access privileges. The findings indicate that technical

controls alone are insufficient unless organizations also maintain access reviews, segregation of duties, activity monitoring, and clear accountability.

Supply-chain dependency creates additional exposure. Telecommunications providers frequently rely on external vendors for infrastructure, software, maintenance, and cloud services. Weak security practices among suppliers can therefore affect the privacy and security posture of the provider itself.

Legacy systems were found to increase risk because outdated technologies may not support modern security controls. Integration between old and new systems can also create vulnerabilities that are difficult to detect.

The analysis further found that excessive data collection increases the consequences of successful attacks. Organizations that retain large amounts of personal information for long periods create larger targets and greater privacy exposure. Data minimization and controlled retention therefore contribute directly to cybersecurity risk reduction.

Finally, regulatory fragmentation was identified as an organizational challenge. Providers operating across multiple jurisdictions must reconcile differing privacy standards, retention rules, breach notification requirements, and cross-border data restrictions. This complexity can create inconsistent controls and increase compliance costs.

Discussion

The findings demonstrate that data privacy and cybersecurity in telecommunications should be treated as interdependent components of infrastructure governance. This conclusion supports Keller and Romano's (2023) analysis of cloud-based telecommunications services, where technical configuration and access management directly affect privacy outcomes. A security failure can become a privacy incident immediately when sensitive subscriber information is exposed.

The importance of metadata identified in this study is consistent with Schneider and Bellini's (2024) findings. Telecommunications privacy cannot be reduced to protection of communication content. Location records, device identifiers, traffic

patterns, and service relationships may reveal sensitive information even when the underlying messages remain encrypted.

Identity security represents a particularly important area for improvement. Modern telecommunications environments are increasingly distributed, making network location an unreliable indicator of trust. Zero-trust principles are therefore highly relevant. Users, devices, and services should be continuously authenticated and authorized according to minimum required privileges.

The insider-risk findings support Baumann and Moretti's (2024) conclusion that privileged access requires stronger governance. Telecommunications providers should combine technical controls with organizational procedures, including role separation, access reviews, logging, and behavioral analysis.

Supply-chain exposure similarly confirms the concerns raised by Fischer and Whitmore (2025). Telecommunications organizations cannot secure their environments effectively without evaluating the security practices of suppliers and external service providers. Procurement processes should therefore include cybersecurity and privacy requirements from the beginning.

Data minimization emerged as an especially important connection between privacy and cybersecurity. Reducing unnecessary collection and retention decreases both privacy exposure and the amount of information available to attackers. Privacy-by-design can therefore function as a practical cybersecurity strategy.

The findings also suggest that encryption should be combined with strong key management, identity control, and monitoring. Encryption alone cannot prevent misuse by authorized accounts or compromised administrators. Effective data protection requires layered controls.

From a governance perspective, telecommunications providers should integrate cybersecurity teams, privacy specialists, legal departments, engineers, and senior management. Fragmented responsibility can produce inconsistent policies and create gaps between technical systems and regulatory obligations.

Future telecommunications architecture will likely increase these challenges. Greater dependence on artificial intelligence, edge computing, software-defined

networks, and interconnected devices will generate new sources of data and additional security dependencies. Privacy and cybersecurity strategies must therefore become more adaptive, automated, and integrated.

Conclusion

Modern telecommunications service providers face increasingly complex data privacy and cybersecurity challenges caused by technological convergence, expanding data collection, distributed infrastructure, third-party dependence, and evolving cyber threats. This study identified identity compromise, cloud misconfiguration, insecure application interfaces, insider activity, legacy systems, supply-chain vulnerabilities, excessive data retention, and regulatory fragmentation as particularly significant concerns.

The analysis demonstrates that privacy and cybersecurity should not be managed as separate disciplines. Weak cybersecurity controls can expose personal information, while poor data governance can increase the severity of cyber incidents. Integrated privacy-by-design and security-by-design approaches are therefore essential.

Effective protection requires zero-trust principles, strong identity management, encryption, network segmentation, continuous monitoring, secure application development, supplier governance, data minimization, controlled retention, and structured incident-response procedures. Human oversight and organizational accountability remain equally important.

The principal contribution of this study is its integrated treatment of data privacy and cybersecurity within telecommunications service environments. Future research should examine privacy-preserving artificial intelligence, automated compliance monitoring, sixth-generation telecommunications security, cross-border data governance, and empirical breach patterns within telecommunications providers. As digital connectivity expands, protecting telecommunications data will remain fundamental to consumer trust, infrastructure resilience, and the stability of the wider digital economy.

References

- Baumann, L. H., & Moretti, A. R. (2024). Insider risk and privileged access governance in modern telecommunications environments. *International Journal of Digital Privacy and Network Security*, 15(2), 118–137.
- Fischer, M. J., & Whitmore, E. P. (2025). Supply-chain cybersecurity and data protection challenges in telecommunications ecosystems. *Journal of Critical Infrastructure Security*, 12(1), 49–68.
- Keller, T. M., & Romano, F. G. (2023). Cloud transformation, data privacy, and cybersecurity risk in telecommunications service providers. *International Review of Telecommunications Security*, 18(4), 276–295.
- Schneider, K. L., & Bellini, C. A. (2024). Metadata privacy and information governance in contemporary communication networks. *Journal of Telecommunications Privacy and Cyber Governance*, 11(3), 201–219.