ZAMONAVIY TELEKOMMUNIKATSIYA TARMOQLARIDA KIBERXAVFSIZLIKNI TA'MINLASH: GLOBAL TAHDIDLAR VA KOMPLEKS HIMOYA MEXANIZMLARI

Jo'rayev Nurmaxamad Mamatovich
Farg'ona davlat texnika universiteti, Telekommunikatsiya muhandisligi kafedrasi dotsenti
E-mail: nmjuraev61@gmail.com
Aliqosimova Muhabbat Akbarjon qizi
Farg'ona davlat texnika universiteti, Telekommunikatsiya va kiberxavfsizlik fakulteti, Pochta aloqasi texnologiyalari yo'nalishi
E-mail: muhabbataliqosimova144@gmail.com
https://doi.org/10.5281/zenodo.23982774

Annotatsiya

Ushbu maqolada zamonaviy telekommunikatsiya tarmoqlarida kiberxavfsizlikni ta'minlash masalalari, xalqaro miqyosdagi tahdidlar va ularga qarshi himoya yondashuvlari tahlil qilinadi. Mobil aloqa, 5G tarmoqlari va raqamli xizmatlarning kengayishi axborot almashinuvini jadallashtirish bilan birga, tarmoq infratuzilmasi va foydalanuvchi ma'lumotlariga nisbatan xavflarni ham oshirmoqda. Tadqiqotda fishing, zararli dasturlar, xizmat ko'rsatishni rad etish hujumlari, deepfake va ovoz klonlash bilan bog'liq tahdidlar ko'rib chiqiladi. Xalqaro standartlar hamda mualliflarning avvalgi ilmiy ishlari asosida ko'p qatlamli va adaptiv himoya yondashuvi asoslanadi.

Kalit so'zlar: telekommunikatsiya tarmoqlari, kiberxavfsizlik, axborot xavfsizligi, 5G, sun'iy intellekt, deepfake, kiberhujum, adaptiv himoya, autentifikatsiya.

Аннотация

В статье анализируются вопросы обеспечения кибербезопасности современных телекоммуникационных сетей, глобальные угрозы и подходы к защите от них. Расширение мобильной связи, сетей 5G и цифровых услуг ускоряет обмен информацией, но одновременно повышает риски для сетевой инфраструктуры и пользовательских данных. Рассматриваются фишинг, вредоносное программное обеспечение, атаки типа «отказ в обслуживании», дипфейки и клонирование голоса. На основе международных стандартов и предыдущих научных работ авторов обосновывается многоуровневый адаптивный подход к защите.

Ключевые слова: телекоммуникационные сети, кибербезопасность, информационная безопасность, 5G, искусственный интеллект, дипфейк, кибератака, адаптивная защита, аутентификация.

Abstract

This article analyses cybersecurity in modern telecommunications networks, global threats and approaches to protection. The expansion of mobile communications, 5G networks and digital services accelerates information exchange while increasing risks to network infrastructure and user data. The study considers phishing, malware, denial-of-service attacks, deepfakes and voice cloning. Drawing on

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

international standards and the authors' previous research, it substantiates a multilayered and adaptive approach to telecommunications security.

Keywords: telecommunications networks, cybersecurity, information security, 5G, artificial intelligence, deepfake, cyberattack, adaptive protection, authentication.

1. KIRISH (INTRODUCTION)

Telekommunikatsiya tarmoqlari zamonaviy jamiyatda davlat xizmatlari, bank operatsiyalari, elektron savdo, ta'lim va kundalik muloqotning asosiy infratuzilmalaridan biriga aylandi. Mobil aloqa, yuqori tezlikdagi internet, bulutli xizmatlar va 5G texnologiyalarining rivojlanishi katta hajmdagi ma'lumotlarni uzatish imkonini bermoqda. Shu bilan birga, tarmoq elementlari va raqamli xizmatlar o'zaro bog'liqligining ortishi kiberhujumlarning ta'sir doirasini ham kengaytirmoqda.

Telekommunikatsiya xavfsizligi faqat aloqa qurilmalarini himoyalash bilan cheklanmaydi. Tarmoq orqali uzatiladigan shaxsiy ma'lumotlar, foydalanuvchi hisoblari, moliyaviy axborot va xizmatlarning uzluksizligi ham himoyani talab qiladi. Xalqaro kiberxavfsizlik hisobotlarida fishing, zararli dasturlar va ijtimoiy muhandislik keng tarqalgan tahdidlar sifatida qayd etiladi (European Union Agency for Cybersecurity [ENISA], 2025).

Generativ sun'iy intellektning rivojlanishi yuz tasviri va ovozni sun'iy yaratish yoki o'zgartirish imkoniyatlarini kengaytirdi. Natijada masofaviy identifikatsiya va biometrik tekshiruv tizimlari deepfake, ovoz klonlash hamda soxta media oqimini kiritish kabi tahdidlarga duch kelmoqda (Mirsky & Lee, 2021). Ushbu tadqiqotning maqsadi telekommunikatsiya tarmoqlaridagi asosiy kiberxavflarni tizimlashtirish va ularni kamaytirishga qaratilgan kompleks himoya yondashuvini asoslashdan iborat.

2. TADQIQOT METODOLOGIYASI (METHODS)

Tadqiqotda ilmiy adabiyotlarni tizimli o'rganish, qiyosiy tahlil va konseptual umumlashtirish usullaridan foydalanildi. Xalqaro standartlar, raqamli identifikatsiya bo'yicha tavsiyalar hamda kiberxavfsizlikka oid ilmiy ishlar ko'rib chiqildi. Xususan, NIST SP 800-63-4 raqamli identifikatsiya bo'yicha ko'rsatmalari va ISO/IEC 30107-3:2023 biometrik taqdimot hujumlarini sinash hamda hisobot berish talablariga oid standart sifatida tahlil qilindi (International Organization for Standardization & International Electrotechnical Commission, 2023; Temoshok et al., 2025).

Tahlil doirasida tahdidlar to'rt guruhga ajratildi: (1) tarmoq infratuzilmasiga qaratilgan hujumlar, jumladan DDoS va qurilmalarga ruxsatsiz kirish; (2) ma'lumotlarni ushlab qolish, o'g'irlash yoki o'zgartirish; (3) fishing va boshqa ijtimoiy muhandislik usullari; (4) deepfake, ovoz klonlash va biometrik tekshiruvga soxta oqim kiritish kabi sun'iy intellektga asoslangan hujumlar. Ushbu tasnif tahdidlarning kirish nuqtasi va himoya talablarini taqqoslash imkonini berdi.

3. TADQIQOT NATIJALARI (RESULTS)

Tahlil natijalari telekommunikatsiya tarmoqlarida xavfsizlikni ta'minlash bir-birini to'ldiruvchi himoya qatlamlarini talab qilishini ko'rsatdi. Birinchi qatlam — tarmoq infratuzilmasini himoyalash. Serverlar, marshrutizatorlar, baza stansiyalari va ma'lumotlar markazlari muntazam yangilanishi, kirish huquqlari cheklanishi hamda tarmoq faoliyati doimiy kuzatilishi lozim. DDoS hujumlari va ruxsatsiz kirish urinishlarini aniqlash uchun trafikdagi noodatiy o'zgarishlarni monitoring qilish muhim.

Ikkinchi qatlam — uzatilayotgan ma'lumotlarning maxfiyligi va yaxlitligini ta'minlash. Shifrlash, xavfsiz aloqa protokollari, zaxira nusxalash va kirish huquqlarini boshqarish ma'lumotlarning noqonuniy qo'lga kiritilishi yoki o'zgartirilishi xavfini kamaytiradi. Uchinchi qatlam foydalanuvchini ishonchli

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

aniqlash bilan bog'liq. Ko'p omilli autentifikatsiya va yuqori xavfli operatsiyalarda qo'shimcha tasdiqlashdan foydalanish faqat parolga tayanish bilan bog'liq zaifliklarni kamaytirishi mumkin.

To'rtinchi qatlam sun'iy intellekt yordamida amalga oshiriladigan hujumlarga qarshi kurashni qamrab oladi. Juraev va Aliqosimova (2026a) tomonidan chop etilgan tadqiqotda deepfake, ovoz klonlash va kamera oqimiga soxta ma'lumot kiritish hujumlarini birgalikda baholash uchun besh turdagi signalga asoslangan adaptiv model taklif etilgan. Unda aloqa kanali yaxlitligi, yuz tasviri, ovoz, hujjat va ma'lumotlar muvofiqligi hamda xatti-harakat belgilari yagona xavf ko'rsatkichiga birlashtiriladi. Bunday yondashuv telekommunikatsiya xizmatlarida ham ahamiyatli, chunki masofaviy identifikatsiya ko'pincha audio, video va raqamli kanallarga tayanadi.

Juraev va Aliqosimova (2026b) tomonidan AI va IoT texnologiyalarini pochta-logistika tizimiga integratsiyalash bo'yicha olib borilgan tadqiqotda turli manbalardan keladigan ma'lumotlarni yagona platformada birlashtirish masalasi ko'rib chiqilgan. Ushbu ish yangi maqolada tarmoq va raqamli xizmatlar o'rtasidagi ma'lumot almashinuvi xavfsizligi, ma'lumotlar sifati hamda tizimlararo muvofiqlikning ahamiyatini tushuntirish uchun qo'llanildi.

Natijalarni umumlashtirish asosida quyidagi kompleks yondashuv shakllantirildi: tarmoq infratuzilmasini monitoring qilish; ma'lumotlarni shifrlash; ko'p omilli autentifikatsiya; shubhali faoliyatni aniqlash; xavflarni muntazam baholash; hodisalarga javob berish rejasini ishlab chiqish; foydalanuvchilarning kiberxavfsizlik savodxonligini oshirish. Bu yondashuv alohida vositalarni emas, ularning yagona xavfsizlik siyosati doirasida ishlashini nazarda tutadi.

4. MUHOKAMA (DISCUSSION)

O'rganilgan manbalar an'anaviy himoya vositalari yangi turdagi sun'iy intellektga asoslangan tahdidlar sharoitida doimiy takomillashtirilishi zarurligini ko'rsatadi. Deepfake aniqlash bo'yicha tadqiqotlarda laboratoriya sharoitida olingan natijalar real muhitdagi materiallarga har doim ham to'liq mos kelmasligi qayd etilgan (Chandra et al., 2025; Mirsky & Lee, 2021). Shu sababli telekommunikatsiya xizmatlarida faqat bitta aniqlash algoritmiga tayanish maqsadga muvofiq emas.

Bir nechta mustaqil xavfsizlik signallarini birlashtirish, shubhali holatlarda qo'shimcha tekshiruv o'tkazish va yuqori xavfli operatsiyalarda inson nazoratini saqlash ishonchlilikni oshirishga yordam beradi. Biroq monitoring jarayonida ortiqcha shaxsiy ma'lumot yig'ish yoki ularni uzoq muddat saqlash yangi xavflarni yuzaga keltirishi mumkin. Shuning uchun ma'lumotlarni minimallashtirish, saqlash muddatini cheklash va ulardan foydalanish huquqlarini aniq belgilash zarur.

Tadqiqotning cheklovi shundaki, real telekommunikatsiya operatori tarmog'ida tajriba yoki simulyatsiya o'tkazilmadi. Natijalar ilmiy manbalar va konseptual tahlilga asoslangan. Taklif etilgan yondashuvning amaliy samaradorligini keyingi bosqichda ochiq ma'lumotlar yoki operator bilan hamkorlikda olingan ma'lumotlar asosida baholash talab etiladi.

5. XULOSA

Tadqiqotda zamonaviy telekommunikatsiya tarmoqlarida uchraydigan asosiy kiberxavfsizlik tahdidlari tizimlashtirildi va ularni kamaytirish yo'nalishlari tahlil qilindi. Tarmoq infratuzilmasiga hujumlar, ma'lumotlarni noqonuniy qo'lga kiritish, ijtimoiy muhandislik hamda deepfake va ovoz klonlash kabi sun'iy intellektga asoslangan tahdidlar raqamli aloqa xizmatlari uchun muhim xavf omillari hisoblanadi.

Tahlil asosida ko'p qatlamli va adaptiv himoya yondashuvini qo'llash, tarmoq monitoringini kuchaytirish, ma'lumotlarni shifrlash, ko'p omilli autentifikatsiyani joriy etish va xavfsizlik hodisalariga

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

tezkor javob berish tavsiya etiladi. Kelgusidagi tadqiqotlarda ushbu yondashuvni 5G va boshqa zamonaviy telekommunikatsiya tarmoqlarida amaliy sinovdan o'tkazish maqsadga muvofiq.

FOYDALANILGAN ADABIYOTLAR

1. Chandra, N. A., Murtfeldt, R., Qiu, L., Karmakar, A., Lee, H., Tanumihardja, E., Farhat, K., Caffee, B., Paik, S., Lee, C., Choi, J., Kim, A., & Etzioni, O. (2025). Deepfake-Eval-2024: A multi-modal in-the-wild benchmark of deepfakes circulated in 2024. arXiv. https://doi.org/10.48550/arXiv.2503.02857
2. European Union Agency for Cybersecurity. (2025). ENISA threat landscape 2025. ENISA.
3. International Organization for Standardization, & International Electrotechnical Commission. (2023). Information technology—Biometric presentation attack detection—Part 3: Testing and reporting (ISO/IEC 30107-3:2023). https://www.iso.org/standard/79520.html
4. Juraev, N., & Aliqosimova, M. (2026a). Adaptive defence model of remote identity verification systems against deepfake and voice cloning attacks: The case of government and financial digital services. Bulletin of Contemporary Researches: Multidisciplinary, 2(3), 56–65.
5. Juraev, N. M., & Aliqosimova, M. A. (2026b). Model for improving shipment management efficiency by integrating artificial intelligence and IoT technologies in the postal-logistics system. Descendants of Al-Farghani Electronic Scientific Journal, 1(3), 524–531.
6. Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. ACM Computing Surveys, 54(1), Article 7. https://doi.org/10.1145/3425780
7. Temoshok, D., Proud-Madruga, D., Choong, Y.-Y., Galluzzo, R., Gupta, S., LaSalle, C., Lefkovitz, N., & Regenscheid, A. (2025). Digital identity guidelines (NIST Special Publication 800-63-4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-4

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.