DEEPFAKE TEXNOLOGIYASINING KIBERXAVFSIZLIK TIZIMLARIGA TA'SIRI

Latipov J.T.
Muhammad al-Xorazmiy nomidagi TATU "Sun'iy intellekt kafedrasi" assistenti
Abdurahimov D.R.
Muhammad al-Xorazmiy nomidagi TATU "Sun'iy intellekt kafedrasi" assistenti

Annotatsiya: Mazkur maqolada Deepfake texnologiyasining kiberxavfsizlik tizimlariga ta'siri tahlil qilingan. Unda deepfakeni yaratish usullari, xususan GAN va boshqa sun'iy intellekt modellari asosida ishlash prinsiplari yoritilgan. Shuningdek, ijtimoiy muhandislik hujumlari, biometrik autentifikatsiya tizimlariga tahdidlar va yolg'on axborot tarqatish kabi xavflar misollar asosida ko'rib chiqilgan. Maqolada ushbu tahdidlarga qarshi kurashish usullari, jumladan, aniqlash algoritmlari, ko'p faktorli autentifikatsiya va huquqiy-etik yondashuvlar bayon etilgan. Tadqiqot natijalari deepfake texnologiyalarining kiberxavfsizlikka ta'siri murakkab va ko'p qirrali ekanligini ko'rsatadi.

Kalit so'zlar: deepfake, sun'iy intellekt, kiberxavfsizlik, GAN, biometrik autentifikatsiya, yolg'on axborot, ijtimoiy muhandislik, axborot xavfsizligi

Аннотация: В данной статье анализируется влияние технологии Deepfake на системы кибербезопасности. Рассматриваются методы создания deepfake, включая использование GAN и других моделей искусственного интеллекта. Особое внимание уделяется таким угрозам, как социальная инженерия, уязвимость биометрической аутентификации и распространение дезинформации. В статье приведены практические примеры использования deepfake в киберпреступлениях. Также рассматриваются методы противодействия, включая технологии обнаружения, многофакторную аутентификацию и правовые и этические меры. Результаты исследования показывают, что deepfake представляет собой сложную и многогранную угрозу для кибербезопасности.

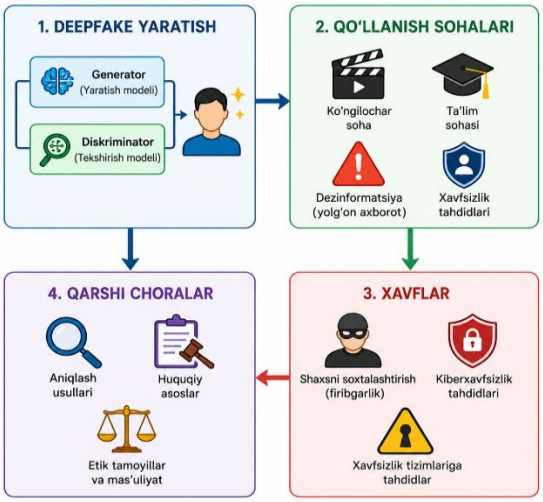
Ключевые слова: deepfake, искусственный интеллект, кибербезопасность, GAN, биометрическая аутентификация, дезинформация, социальная инженерия, информационная безопасность

Abstract: This article analyzes the impact of Deepfake technology on cybersecurity systems. It discusses the methods of deepfake generation, particularly those based on Generative Adversarial Networks and other artificial intelligence models. The study highlights major threats such as social engineering attacks, vulnerabilities in biometric authentication, and the spread of misinformation. Practical examples of deepfake usage in cybercrime are also examined. Furthermore, the paper outlines countermeasures including detection techniques, multi-factor authentication, and legal and ethical frameworks. The findings indicate that deepfake technology poses a complex and multifaceted challenge to cybersecurity.

Keywords: deepfake, artificial intelligence, cybersecurity, GAN, biometric authentication, misinformation, social engineering, information security

Barchamizga ma'lumki, so'nggi yillarda sun'iy intellekt asosidagi texnologiyalar jadallik bilan rivojlanib, inson hayotining deyarli barcha sohalarida keng qo'llanilmoqda. Xususan, kiberxavfsizlik sohasida sun'iy intellekt integratsiyasi bugungi kunda eng dolzarb yo'nalishlardan biri bo'lib, u hujumlarni real vaqt rejimida kuzatish, shubhali xatti-harakatlarni tahlil qilish, avtomatik ravishda tahdidlarni aniqlash va ularga qarshi choralar ko'rish imkonini yaratadi.

Texnologiyalarning rivojlanishi bilan birga kiberhujumlarning soni va ularning murakkabligi oshib bormoqda [1]. O‘z navbatida bu jarayon yangi imkoniyatlar bilan bir qatorda jiddiy muammolarni ham keltirib chiqarmoqda. Deep Learning asosidagi “deepfake” texnologiyasi yuqori realistik darajadagi audio va video yaratish imkonini beradi. Deepfake dastlab ko‘ngilochar va kreativ sohalarda qo‘llangan bo‘lsa-da, hozirda u xavfsizlik tzimlari uchun jiddiy muammolarini keltirib chiqarmoqda (1- rasm).



1-rasm. Deepfake texnologiyasining grafik ko‘rinishdagi umumiy tavsifi

Deepfake texnologiyasi yordamida video, audio va tasvirlarni sun’iy ravishda o‘zgartirish yoki mutlaqo yangi kontent yaratish imkoniyati paydo bo‘ldi. Deepfeyklar (deepfakes) o‘ta realistik sintetik tasvirlar, videolar va audiolar yaratish imkonini beruvchi eng kuchli va bahsli texnologiyalardan biri hisoblanadi [2]. GAN (generativ-yovuz tarmoqlar), avtoenkoderlar va diffuziya modellari kabi arxitekturalardan foydalangan holda, deepfeyk tizimlari inson yuzlari, ovozlari, yuz ifodalari va harakatlarini hayratlanarli aniqlik bilan takrorlay oladi. Ushbu sun’iy intellekt texnologiyasidan foydalanib, kiberjinoyatchilar ham murakkab hujumlar uyushtirish yo‘llarini o‘rganmoqda.

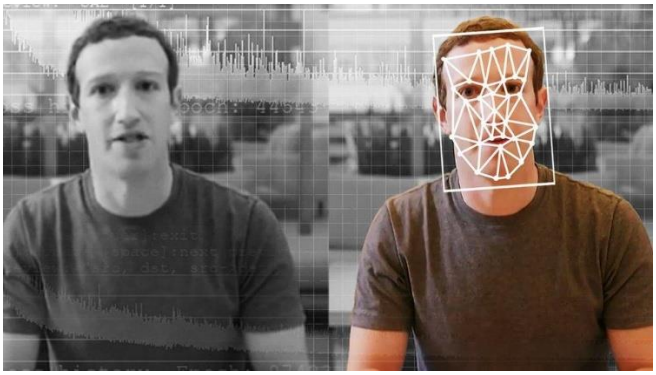
Deepfake texnologiyalari yordamida amalga oshiriladigan eng katta tahdidlardan biri ijtimoiy muhandislik hujumlarining murakkablashuvidir. Masalan, hujumchi kompaniya rahbarining ovozini sun’iy ravishda yaratib, xodimga moliyaviy operatsiyani bajarishni buyurishi mumkin. Bunday holatlarda xodim ovozning haqiqiy ekanligiga ishonib, firibgarlik qurboniga aylanadi.

Yana bir muhim xavf — bu biometrik autentifikatsiya tizimlarining zaiflashuvidir. Deepfake yordamida yaratilgan soxta video yoki audio orqali biometrik autentifikatsiya tizimlari aldab o‘tilishi mumkin [3]. Masalan, yuzni aniqlash tizimiga soxta video orqali kirish holatlari amaliyotda kuzatilgan.

Shuningdek, deepfake texnologiyasi g‘araz niyatli shaxslar tomonidan yolg‘on axborot tarqatishda ham keng qo‘llanilmoqda. Soxta video yoki nutq orqali jamoatchilik fikrini manipulyatsiya qilish, siyosiy yoki ijtimoiy beqarorlik keltirib chiqarish holatlari tez-tez uchrab turibdi. Bu esa axborot xavfsizligi uchun katta tahdid hisoblanadi. Bunga misol sifatida 2019-yilda ijtimoiy tarmoqlarda tarqalgan Mark Zuckerberg aks ettirilgan deepfake videoni keltirish mumkin. Videoda u go‘yoki “foydalanuvchilar ma’lumotlarini nazorat qilayotgani” haqida maqtanayotgandek tasvirlangan (2-rasm). Ushbu keng tarqalgan media namunasi deepfake texnologiyasining etik chegaralari hamda uning raqamli boshqaruv va jamoatchilik ishonchiga ta’siri bo‘yicha global muhokaralarni yanada kuchaytirdi.

2-rasm. 2019-yilda tarmoqqa sizdirilgan Mark Zuckerberg aks ettirilgan deepfake videodan lavha.

Texnik jihatdan deepfake ko‘pincha Generative Adversarial Networks orqali yaratiladi, bunda ikki neyron tarmoq bir-biri bilan raqobatlashib, juda realistik natija hosil qiladi. Shu sababli oddiy foydalanuvchi bunday soxtalikni aniqlay olmaydi. Yuqorida sanab o’tilgan tahdidlarga qarshi kurashish uchun bir qator samarali usullar mavjud. Birinchidan, sun’iy intellekt asosida deepfake aniqlovchi tizimlar ishlab chiqilmoqda, ular yuz mimikasi, yorug‘lik va ovozdagi nomuvofiqliklarni aniqlaydi. Masalan, video ichidagi lab harakati bilan ovoz sinxron emasligi aniqlanishi mumkin (3-rasm).



3- rasm. Asl va soxta videoni yuz mimikalari va lab harakatlari orqali aniqlash jarayoni

Ikkinchidan, ko‘p faktorli autentifikatsiya (MFA) joriy etilishi axborot xavfsizligida muhim ahamiyatga ega. Bu usulda foydalanuvchi faqat biometrik ma’lumot bilan emas, balki qo‘shimcha tasdiqlash bosqichlari orqali tekshiriladi [4]. Bundan tashqari, raqamli watermarking va elektron imzo texnologiyalari orqali media fayllarning haqiqiyligini tekshirish mumkin. Bu usul ayniqsa rasmiy video va hujjatlarni himoya qilishda samarali hisoblanadi.

Eng asosiy kurash choralaridan biri sifatida foydalanuvchilarni yangi texnologiyalardan xabardor qilish ham muhim ahamiyat kasb etadi. Tashkilotlarda xodimlarga deepfake tahdidlari haqida treninglar o‘tkazish orqali ijtimoiy muhandislik hujumlarining oldini olish mumkin. Kelajakda esa sun’iy intellekt asosidagi himoya tizimlari yanada rivojlanib, tahdidlarni oldindan aniqlash imkoniyatini beradi. Shu bilan birga, deepfake texnologiyasining o‘zi ham takomillashib boradi, bu esa “texnologiyalar kurashi”ni yuzaga keltiradi.

Xulosa qilib aytganda, sun’iy intellekt asosidagi deepfake texnologiyalari kiberxavfsizlik tizimlari uchun yangi va murakkab tahdidlarni yuzaga keltirmoqda. Ular biometrik autentifikatsiya, axborot ishonchliligi va foydalanuvchi xavfsizligiga bevosita ta’sir ko‘rsatadi. Shu bilan birga, zamonaviy himoya usullari ushbu tahdidlarga qarshi samarali kurashish imkonini yaratadi. Kelajakda kiberxavfsizlik tizimlari yangi algoritmlar, yanada murakkab va samarali

metodlar orqali deepfake xavfini hisobga olgan holda yanada takomillashtirilishi zarur. Qo‘shimcha ravishda, kelajakda sun’iy intellektni kiberxavfsizlik tizimlarida yanada samarali va xavfsiz qo‘llash uchun turli xil xavfsizlik standartlari va me’yorlar ishlab chiqilishi, shuningdek, sun’iy intellekt texnologiyalarining yanada rivojlanishi uchun ilmiy izlanishlar davom ettirilishi zarur bo‘ladi. Faqat kompleks yondashuv orqali deepfake tahdidlarini kamaytirish va xavfsiz raqamli muhitni ta’minlash mumkin.

Foydalanilgan adabiyotlar:

1. Brooks, T., Princess, G., Heatley, J., Jeremy, J., & Scott, K. (2019). Increasing threats of deepfake identities. US Department of Homeland Security [online].
2. Popa, C., Pallath, R., Cunningham, L., Tahiri, H., Kesavarajah, A., & Wu, T. (2025). Deepfake technology unveiled: The commoditization of AI and its impact on digital trust. preprint arxiv:2506.07363.
3. Romero-Moreno, F. (2025). Deepfake detection in generative AI: A legal framework proposal to protect human rights. Computer Law & Security Review, 58, 106162.
4. Kaushik, P., Garg, V., Priya, A., & Kant, S. (2025). Financial fraud and manipulation: The malicious use of deepfakes in business. In Deepfakes and Their Impact on Business (pp. 173-196). IGI Global Scientific Publishing.