SCIENCE HUB REVIEW
2026
Volume 1
Issue 5
www.sciencehubreview.uz
ILMIY ELEKTRON JURNAL

TELEGRAM XABARLARIDA FIRIBGARLIK ALOMATLARINI AVTOMATIK ANIQLASH

Yusupov Samandar Anvarovich

OXUS Universiteti katta o‘qituvchisi, Toshkent 100208, O‘zbekiston

Samandar75781111@gmail.com

Qodirov Bahromjon Botirovich

OXUS University kompyuter ilimlari 501-26 guruh talabasi, Toshkent 100208, O‘zbekiston

godirovbahrom128@gmail.com

Annotatsiya

Ushbu maqolada Telegram xabarlarida uchraydigan firibgarlik alomatlarini avtomatik aniqlashga mo‘ljallangan intellektual tizim konsepsiyasi ko‘rib chiqiladi. Muammoning dolzarbligi, matnni tabiiy tilni qayta ishlash (NLP) usullari bilan tahlil qilish, shubhali havolalarni baholash va xabar kontekstidan foydalanish masalalari yoritiladi. Taklif etilayotgan yondashuv qoidaviy tekshiruv, an’anaviy mashinaviy o‘rganish modeli va ko‘p tilli transformer modelini birlashtirishga asoslanadi. O‘zbek tilining lotin va kirill yozuvlari, imlo variantlari, qisqartmalar hamda emoji ishlatilishi alohida hisobga olinadi. Maqolada tizim arxitekturasi, belgilar to‘plami, xavf darajasini hisoblash, baholash mezonlari va ma’lumotlar maxfiyligini ta’minlash choralari taklif etiladi. Ish konseptual-metodik xarakterga ega: tajribaviy sinov o‘tkazilmaganligi sababli maqolada yangi modelning o‘lchangan aniqlik ko‘rsatkichlari sifatida natijalar keltirilmaydi.

Kalit so‘zlar

Telegram, firibgarlikni aniqlash, fishing, tabiiy tilni qayta ishlash, mashinaviy o‘rganish, transformer, XLM-RoBERTa, kiberxavfsizlik, o‘zbek tili.

Abstract

This article presents a conceptual framework for automatically detecting signs of fraud in Telegram messages. It discusses natural language processing, suspicious-link analysis, contextual features, and the challenges posed by Uzbek written in Latin and Cyrillic scripts. The proposed approach combines rule-based indicators, a

conventional machine-learning classifier, and a multilingual transformer model. The article outlines a system architecture, risk-scoring strategy, evaluation metrics, and privacy safeguards. Since no empirical experiment was conducted for this paper, no performance figures are claimed for the proposed system.
Keywords
Telegram, fraud detection, phishing, natural language processing, machine learning, transformer, cybersecurity.

Kirish.

Raqamli muloqot vositalari kundalik hayot, ta’lim, savdo va xizmat ko‘rsatish jarayonlarining muhim qismiga aylandi. Telegram orqali foydalanuvchilar xabar almashish, guruhlarda muloqot qilish, e’lonlarni ko‘rish va turli xizmatlardan foydalanish imkoniga ega. Shu bilan birga, platformalarda soxta sovrinlar, soxta ish takliflari, akkauntni qo‘lga kiritishga qaratilgan fishing xabarlari, soxta investitsiya takliflari va pul o‘tkazishni so‘rovchi murojaatlar ham uchrashi mumkin. Bunday xabarlarning matni tez o‘zgarishi, havolalar almashtirilishi va foydalanuvchida shoshilinch qaror qabul qilish bosimi yaratilishi ularni faqat qo‘lda aniqlashni qiyinlashtiradi.

Firibgarlikni avtomatik aniqlash vazifasi xabarning alohida so‘zini topish bilan cheklanmaydi. Masalan, “sovrin”, “bank” yoki “tasdiqlash” kabi so‘zlar qonuniy xabarlarda ham ishlatiladi. Shuning uchun tizim so‘zlar va iboralar bilan birga gap mazmuni, havola xususiyatlari, maxfiy ma’lumotni so‘rash, haddan tashqari shoshiltirish va boshqa kontekst belgilarini birgalikda tahlil qilishi zarur. Telegramdagi soxta kanallarni aniqlash bo‘yicha tadqiqotlar platformaga xos xususiyatlar va mashinaviy o‘rganish usullaridan foydalanish mumkinligini ko‘rsatadi.

Maqolaning maqsadi — Telegram xabarlaridagi ehtimoliy firibgarlik belgilarini avtomatik baholovchi tizimning metodik modelini taklif etish. Ushbu maqsadga erishish uchun firibgarlik alomatlarini tasniflash, xabarlarni oldindan qayta ishlash usullarini belgilash, model arxitekturasini ishlab chiqish, natijalarni baholash mezonlarini asoslash hamda maxfiylik va xatolik xavflarini ko‘rib chiqish vazifalari qo‘yiladi.

Mavzuga oid taqdiqotlar tahlili.

Matnli xabarlardagi zararli yoki keraksiz mazmunni aniqlashda dastlab kalit so‘zlar va qoidalar asosidagi filtrlar ishlatilgan. Bunday yechimlar tezkor bo‘lsa-da, firibgarlar matnni o‘zgartirganda yoki belgilar orasiga qo‘shimcha simvollar kiritganda

samaradorlik pasayishi mumkin. SMS-fishingni aniqlashga oid adabiyotlar tahlili tabiiy tilni qayta ishlash va mashinaviy o‘rganish usullarini birlashtirish istiqbolli ekanini ko‘rsatadi; shu bilan birga, model sifati ma’lumotlar to‘plami, belgilar tanlovi va baholash protokoliga bog‘liq.

Chuqur o‘rganishdagi transformer arxitekturasi matn kontekstini hisobga olish imkonini beradi. BERT modeli so‘zning ma’nosini uning ikki tomonidagi kontekst bilan birgalikda o‘rganish yondashuvini ommalashtirgan. Ko‘p tilli modellar o‘zbekcha matnlarni tahlil qilishda ham foydali bo‘lishi mumkin, ammo natija modelning tilni qamrab olishi, o‘quv ma’lumotlari va yozuv variantlariga bog‘liq.

O‘zbekcha Telegram xabarlarini xavf darajasi bo‘yicha tasniflashga bag‘ishlangan 2026-yilgi tadqiqotda 10 000 ta xabar qo‘llanib, TF-IDF va Logistic Regression, FastText, mBERT hamda XLM-RoBERTa yondashuvlari solishtirilgan. Mualliflar xavfsiz va xavfli mazmunni tasniflash vazifasida XLM-RoBERTa eng yuqori ko‘rsatkichlarga erishganini bildiradi. Biroq ushbu ishning sinflari umumiy xavfli mazmunga taalluqli bo‘lib, uni barcha turdagi moliyaviy firibgarliklarni aniqlash natijasi sifatida talqin qilish to‘g‘ri emas.

Telegramdagi fishingni aniqlash bo‘yicha 2026-yilda chop etilgan tadqiqot esa umumiy maqsadli katta til modellarining natijasi har doim ham barqaror bo‘lmasligini, ayrim sinovlarda xususiyatlarga asoslangan maxsus modellar aniqroq muvozanat ko‘rsatganini qayd etadi. Demak, amaliy tizimni faqat bitta modelga bog‘lamasdan, qoidaviy belgilar, matn klassifikatori va havola tahlilini uyg‘unlashtirish maqsadga muvofiq.

Taqdiqot metodologiyasi va firibgarlik belgilari.

Taklif etilayotgan tizim xabarni uchta asosiy sinfdan biriga ajratadi: “xavfi past”, “shubhali” va “yuqori xavf”. Bu sinflar jinoyat sodir etilganini qat’iy tasdiqlamaydi; ular foydalanuvchiga ehtiyotkorlik darajasini ko‘rsatadigan ogohlantirish sifatida ishlatiladi. Xabar klassifikatsiyasi quyidagi belgilar guruhlariga tayanadi:

Belgi guruhi	Tahlil qilinadigan xususiyatlar	Ehtimoliy signal
Til va mazmun	Shoshiltirish, qo‘rqitish, kafolatlangan foyda yoki noodatiy sovrin va’dasi	“Darhol bajaring”, “kafolatlangan daromad”

Belgi guruhi	Tahlil qilinadigan xususiyatlar	Ehtimoliy signal
		kabi iboralar kontekstda kelishi
Maxfiy ma’lumot so‘rovi	SMS/Telegram tasdiqlash kodi, parol, bank karta ma’lumoti yoki hujjat nusxasini so‘rash	Sir tutilishi kerak bo‘lgan ma’lumotni yuborishga undash
Havola xususiyatlari	Qisqartirilgan URL, imlo jihatdan o‘xshash domen, kutilmagan yo‘naltirish yoki noma’lum manzil	Xabardagi matn bilan havola domeni o‘rtasidagi nomuvofiqlik
Muloqot konteksti	Kutilmagan pul talabi, o‘zini tanish yoki rasmiy tashkilot vakili sifatida ko‘rsatish	Tasdiqlash uchun mustaqil kanal orqali tekshirish zarurati
Texnik/format belgilari	Harflarni o‘xshash belgilar bilan almashtirish, noodatiy imlo, takroriy shablonlar	Filtrni chetlab o‘tishga o‘xshash yozilish variantlari

Keltirilgan belgilar alohida olinganda firibgarlikni isbotlamaydi. Masalan, qonuniy tashkilot ham foydalanuvchiga havola yuborishi mumkin. Shu sababli tizimning qarori bir nechta mustaqil belgi uyg‘unligiga va xabarning umumiy mazmuniga asoslanishi kerak. Ayniqsa, tasdiqlash kodini so‘rash yoki foydalanuvchini shaxsiy ma’lumot yuborishga undash kuchli ogohlantiruvchi belgi sifatida qaraladi.

Taklif etilayotgan tiizim arxitekturasi.

Tizim quyidagi ketma-ket bosqichlarda ishlashi taklif etiladi:

1-bosqich — ma’lumotni qabul qilish. Tahlil qilinadigan xabar foydalanuvchi tomonidan tekshiruvga yuboriladi yoki foydalanuvchi roziligi va tegishli ruxsatlar mavjud bo‘lgan guruhdagi botga keladi. Tizim foydalanuvchining barcha shaxsiy suhbatlarini avtomatik ko‘ra oladi, degan noto‘g‘ri taxmin qilinmasligi lozim.

2-bosqich — matnni me’yorlashtirish. Lotin va kirill yozuvlari aniqlanadi, Unicode belgilar normallashtiriladi, takroriy bo‘shliqlar va shovqinli formatlar tozalanadi. Emoji va URL kabi mazmun uchun muhim elementlar butunlay o‘chirib yuborilmaydi; ular alohida belgilar sifatida saqlanadi.

3-bosqich — belgilarni ajratish. Matndan shoshiltirish, sovrin va’dasi, hisobni bloklash bilan qo‘rqitish, tasdiqlash kodi yoki pul so‘rashga oid semantik belgilar olinadi.

Havolalar bo‘lsa, domen yozilishi, URL qisqartiruvchisi va manzilning ishonchlilik signallari alohida baholanadi.

4-bosqich — modellar yordamida tasniflash. Boshlang‘ich model sifatida TF-IDF bilan Logistic Regression yoki SVM qo‘llanadi. Keyingi bosqichda ko‘p tilli transformer modeli kontekstni chuqurroq tahlil qiladi. Qoidalar juda aniq belgilarni, mashinaviy o‘rganish esa turli belgilar kombinatsiyasini aniqlashga yordam beradi.

5-bosqich — natijani birlashtirish va ogohlantirish. Matn klassifikatori, URL bahosi va qoidaviy indikatorlar natijalari yagona xavf balliga birlashtiriladi. Foydalanuvchiga xavf darajasi, qarorga ta’sir qilgan asosiy sabablar va xavfsiz keyingi harakatlar ko‘rsatiladi.

6-bosqich — fikr-mulohaza va yangilash. Foydalanuvchi xabarni noto‘g‘ri belgilangan deb baholashi mumkin. Bunday fikrlar shaxsni aniqlovchi ma’lumotlardan tozalangach, yangi modelni qayta o‘qitish va xatolarni tahlil qilish uchun ishlatiladi.

Xavf ballini soddalashtirilgan ko‘rinishda quyidagicha ifodalash mumkin:

$$R(x) = w_1T(x) + w_2U(x) + w_3P(x) + w_4C(x)$$

Bu yerda R(x) — xabar uchun umumiy xavf balli; T(x) — matnning semantik belgilari; U(x) — URL va domen belgilari; P(x) — maxfiy ma’lumot yoki pul so‘rashga oid belgilar; C(x) — muloqot konteksti; $w_1 \ldots w_4$ — o‘quv ma’lumotlari asosida sozlanadigan vaznlar. Belgilar 0 dan 1 gacha normallashtirilishi mumkin. Vaznlar va xavf chegaralari oldindan taxmin bilan emas, belgilangan ma’lumotlar to‘plamida validatsiya orqali tanlanishi kerak.

Tizim natijani “xavfi past”, “shubhali” yoki “yuqori xavf” ko‘rinishida chiqarishi mumkin. “Yuqori xavf” holatida xabarni darhol o‘chirish yoki yuboruvchini avtomatik jazolash o‘rniga, avval foydalanuvchini ogohlantirish, havolani ochmaslikni tavsiya etish, yuboruvchini boshqa aloqa kanali orqali tekshirish hamda zarur bo‘lsa platformaga shikoyat qilish yo‘lini ko‘rsatish xavfsizroq hisoblanadi.

Ma’lumotlar to‘plami va baholar mezonlari.

Model sifatini xolis baholash uchun o‘zbek tilidagi haqiqiy va firibgarlikka o‘xshash xabarlar to‘plami zarur. To‘plamga shaxsiy ma’lumotlar olib tashlangan, ruxsat bilan olingan yoki ochiq manbalardan qonuniy foydalanish shartlari asosida yig‘ilgan xabarlar

kiritilishi lozim. Xabarlar mutaxassislar tomonidan “xavfsiz”, “shubhali” va “firibgarlik ehtimoli yuqori” sinflariga ajratiladi. Chegaraviy holatlarda bir nechta annotator bahosi va kelishmovchiliklarni ko‘rib chiqish tartibi bo‘lishi kerak.

Ma’lumotlarni trening, validatsiya va test qismlariga ajratishda bir xil kanal yoki bir xil matn shablonining nusxalari turli qismlarga tushib qolmasligiga e’tibor beriladi. Aks holda model yangi firibgarlik usulini o‘rganish o‘rniga ilgari ko‘rgan matnni yodlab, sun’iy ravishda yuqori natija ko‘rsatishi mumkin. Vaqt bo‘yicha ajratilgan test ham foydali: u firibgarlik matnlari vaqt o‘tishi bilan o‘zgarganda model qanday ishlashini tekshiradi.

Asosiy baholash ko‘rsatkichlari quyidagilar bo‘lishi maqsadga muvofiq:

1. Precision (aniqlik ulushi) — firibgar deb belgilangan xabarlarning qanchasi haqiqatan ham xavfli ekanini ko‘rsatadi; u yolg‘on ogohlantirishlarni kamaytirishda muhim.

2. Recall (qamrov) — mavjud firibgar xabarlarning qanchasi aniqlanganini ifodalaydi; past recall ko‘plab xavfli xabarlarning o‘tib ketishini anglatadi.

3. F1-score — precision va recall orasidagi muvozanatni umumlashtiradi.

4. PR-AUC — xavfli xabarlar kam uchraydigan va sinflar nomutanosib bo‘lgan sharoitda modelni baholashga yordam beradi.

5. Kechikish va resurs sarfi — xabarni tekshirish uchun sarflanadigan vaqt, xotira va hisoblash quvvatini ko‘rsatadi.

Sinovda faqat umumiy aniqlikni ko‘rsatish yetarli emas. Masalan, firibgar xabarlar to‘plamning kichik qismini tashkil etsa, tizim barcha xabarlarni xavfsiz deb belgilab ham yuqori umumiy aniqlikka erishishi mumkin. Shu sababli sinflar kesimidagi precision, recall va F1 ko‘rsatkichlari hamda yolg‘on ijobiy holatlar alohida hisobot qilinadi. Mazkur maqolada ishlab chiqilgan konsepsiya uchun bunday tajriba hali o‘tkazilmagan; shuning uchun aniq foizli ko‘rsatkichlar natija sifatida da’vo qilinmaydi.

Amaliy qo‘llash , maxfiylik va cheklovlar.

Tizimning amaliy qiymati faqat xavfli xabarni topish bilangina belgilanmaydi. U foydalanuvchiga qaror sababini tushunarli qilib ko‘rsatishi, masalan, “xabar tasdiqlash kodini so‘rayapti”, “havola matndagi tashkilot nomiga mos kelmaydi” yoki “tezkor pul

o‘tkazish talab qilinmoqda” kabi izohlar berishi kerak. Bunda tizim noaniq holatlarni firibgarlik deb qat’iy hukm qilmasligi, “shubhali” darajasida ko‘rsatishi mumkin.

Maxfiylik masalasi alohida ahamiyatga ega. Telegramning amaldagi maxfiylik siyosatida spam va fishingga qarshi ayrim avtomatik tahlil mexanizmlari hamda foydalanuvchilar yuborgan shikoyatlarni ko‘rib chiqish tartibi bayon etilgan. Biroq mustaqil ishlab chiqilgan bot yoki ilovaning imkoniyatlari Telegramning o‘z tizimlari bilan bir xil emas. Botning guruh xabarlarini ko‘rish imkoniyati uning sozlamalari va ruxsatlariga bog‘liq; shuning uchun tizim faqat qonuniy ravishda ruxsat etilgan va foydalanuvchi tushungan ma’lumotlarni tahlil qilishi lozim.

Asosiy cheklovlar qatoriga firibgarlarning usullarini tez-tez o‘zgartirishi, o‘zbek tilidagi belgilangan ma’lumotlar hajmining yetarli bo‘lmasligi, sheva va aralash tilli matnlar, rasm ichiga joylangan matn, yashirin URL yo‘naltirishlari hamda noto‘g‘ri ijobiy ogohlantirishlar kiradi. Kelgusida rasmlardan matn ajratish (OCR), URL obro‘sini tekshirish, foydalanuvchi fikr-mulohazasi asosida qayta o‘qitish va yangi hujum usullariga moslashish mexanizmlarini sinash mumkin. Biroq har bir qo‘shimcha manba maxfiylik va xavfsizlik talablariga muvofiq ishlatilishi zarur.

Xulosa

Telegram xabarlarida firibgarlik alomatlarini avtomatik aniqlash tabiiy tilni qayta ishlash, havolalarni tahlil qilish va kontekstga asoslangan xavf bahosini birlashtirishni talab qiladi. Faqat kalit so‘zlarga tayangan filtrlar sodda va tezkor bo‘lsa-da, matnning ma’nosi va belgilar uyg‘unligini hisobga olish imkoniyati cheklangan. Shu sababli qoidaviy tekshiruv, an’anaviy mashinaviy o‘rganish va ko‘p tilli transformer modelini birgalikda qo‘llash istiqbolli yondashuv sifatida taklif etildi.

Taklif etilgan tizim lotin va kirill yozuvlarini me’yorlashtirish, shoshiltirish va maxfiy ma’lumot so‘rash belgilarini ajratish, URL xususiyatlarini baholash hamda foydalanuvchiga izohli ogohlantirish berish bosqichlaridan iborat. Uning samaradorligini tasdiqlash uchun ruxsat bilan to‘plangan va ekspertlar tomonidan belgilangan ma’lumotlar, xolis test ajratilishi hamda precision, recall, F1 va PR-AUC kabi ko‘rsatkichlar zarur. Kelgusi ish sifatida o‘zbekcha Telegram xabarlari uchun

ma’lumotlar to‘plamini yaratish, bazaviy modellarni solishtirish va amaliy prototipni foydalanuvchi roziligi asosida sinash tavsiya qilinadi.

Foydalanilgan adabiyotlar

1. Al Saidat, M. R., Yerima, S. Y., Shaalan, K. Advancements of SMS Spam Detection: A Comprehensive Survey of NLP and ML Techniques. Procedia Computer Science, 244, 2024, 248–259-b. DOI: https://doi.org/10.1016/j.procs.2024.10.198.

2. Devlin, J., Chang, M.-W., Lee, K., Toutanova, K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. Proceedings of NAACL-HLT 2019, 2019, 4171–4186-b. DOI: https://doi.org/10.18653/v1/N19-1423.

3. La Morgia, M., Mei, A., Mongardini, A. M., Wu, J. It’s a Trap! Detection and Analysis of Fake Channels on Telegram. 2023 IEEE International Conference on Web Services (ICWS), 2023. DOI: https://doi.org/10.1109/ICWS60048.2023.00026.

4. Qoyliyeva, F. A., Babomuradov, O. J., Savurbayev, A. A. Comparative Evaluation of Traditional and Transformer-Based Models for Risk-Level Classification of Uzbek Telegram Messages. International Journal of Advanced Computer Science and Applications, 17(6), 2026. DOI: https://doi.org/10.14569/IJACSA.2026.0170651.

5. Erfan, M., Branco, P., Jourdan, G.-V. Can LLMs Keep Up? Evaluating Phishing Detection on Telegram. Digital Threats: Research and Practice, 2026. DOI: https://doi.org/10.1145/3829369.