RAQAMLI FIRIBGARLAR AVJIDA

Umarov Bekzod Azizovich
Farg'ona davlat unversiteti amaliy matematika va informatika kafedrasi o'qituvchisi
ubaumarov@mail.ru
Mashxuraxon Mamatxalilova G'ofurjon qizi
Farg'ona Davlat Unversiteti 3-kurs talabasi
Mamatxalilovamashzuraxon0708@gmail.com

Annotatsiya

Bugungi raqamli dunyo kundan kunga yangi tahdidlar girdobiga tushib bormoqda, firibgarlar texnologiyani o'z quroliga aylantirib, moliyaviy xavfsizligimiz va shaxsiy ma'lumotlarimizga jiddiy zarar yetkazishmoqda. Ularning mohirona tarzda topayotgan yangi firibgarlik usullari tobora murakkablashayotgan bir paytda, mashinali o'rganish (machine learning) texnologiyalari raqamli xavfsizlikni ta'minlashda muhim vositalardan biri sifatida raqamli firibgarlikka qarshi ketayotgan kurash maydoniga chiqdi.

Ushbu maqola raqamli firibgarlikning bugungi kundagi ko'rinishlari, shuningdek, ularni oldini olishda mashinali o'rganish texnologiyalarining roli haqida so'z yuritadi. Raqamli firibgarlikka qarshi kurashda zamonaviy texnologiyalarning samaradorligi yoritiladi. Maqola nafaqat mavjud muammolarni ochib beradi, balki o'quvchini o'z xavfsizligini ta'minlash uchun zarur chora tadbirlarni ko'rishga undaydi.

Kalit so'zlar: Raqamli firibgarlik, Mashinali o'rganish (Machine Learning), Raqamli xavfsizlik, Firibgarlikni aniqlash, Shaxsiy ma'lumotlar himoyasi, Texnologik tahdidlar, Ma'lumotlarni tahlil qilish, Xavfsizlik strategiyalari, Bank kartalari firibgarligi, Sun'iy intellekt, Onlayn xavfsizlik, Ijtimoiy tarmoqlarda xavfsizlik, Raqamli savodxonlik, Ehtiyotkorlik va ogohlik, Xavfli veb-saytlar, Shifrlash (Encryption), Ma'lumotlar maskirovkasi, Kollektiv ma'lumotlar tahlili, Vaqtga bog'liq ketma-ketlik (Time-series data), Shubhali tranzaktsiyalar.

Аннотация

Современный цифровой мир с каждым днем сталкивается с новыми угрозами: мошенники превращают технологии в свои инструменты, нанося серьезный ущерб нашей финансовой безопасности и персональным данным. В то время как их умело разработанные методы обмана становятся все более сложными, технологии машинного обучения выходят на арену борьбы с цифровым мошенничеством как один из ключевых инструментов обеспечения цифровой безопасности.

Данная статья посвящена современным формам цифрового мошенничества, а также роли технологий машинного обучения в

предотвращении таких угроз. Освещается эффективность современных технологий в борьбе с цифровым мошенничеством. Статья не только раскрывает существующие проблемы, но и призывает читателя принимать необходимые меры для обеспечения собственной безопасности.

Ключевые слова: цифровое мошенничество, машинное обучение, цифровая безопасность, обнаружение мошенничества, защита персональных данных, технологические угрозы, анализ данных, стратегии безопасности, мошенничество с банковскими картами, искусственный интеллект, онлайн-безопасность, безопасность социальных сетей, цифровая грамотность, осторожность и осведомленность, опасные веб-сайты. , Шифрование, Данные Маскирование, Коллективный анализ данных, Данные временных рядов, Подозрительные транзакции.

Annotation

The modern digital world faces new threats every day as fraudsters turn technology into their weapon, causing significant harm to our financial security and personal data. As their cleverly devised fraudulent schemes grow increasingly sophisticated, machine learning technologies have emerged as a key tool in the battle against digital fraud and in ensuring digital security.

This article explores the current manifestations of digital fraud and the role of machine learning technologies in preventing such threats. It highlights the effectiveness of modern technologies in combating digital fraud. The article not only sheds light on existing problems but also encourages readers to take necessary measures to ensure their own safety.

Keywords: Digital Fraud, Machine Learning, Digital Security, Fraud Detection, Personal Data Protection, Technological Threats, Data Analytics, Security Strategies, Bank Card Fraud, Artificial Intelligence, Online Safety, Social Media Safety, Digital Literacy, Caution and Awareness, Dangerous Websites, Encryption, Data Masking, Collective data analysis, Time-series data, Suspicious transactions.

Sizning ham bankdagi mablag’ingiz o’g’irlanishi mumkinligini tasavvur qila olasizmi? yoki begona bir kishi sizning shaxsiy ma’lumotlaringizdan foydalanayotgan bo’lishi extimolinichi? Hechkimga sir emaski bugungi kunimizda bank plastik kartalaridan pul o’g’irlanishi, soxta elektron pochta va saytlarga aldanib qolish, shaxsiy ma’lumotlardan noqonuniy yo’llar bilan g’arazli maqsadlarda foydalanish kabi xolatlar kuzatilishi hechbirimiz uchun yangilik bo’lmay qoldi, va bu kabi xolatlar hozirgi “raqamli zamonamizda” judda xam ko’p sodir bo’lmoqda. Bu tahdidlar zamonaviy raqamli dunyoning o’ziga xos xavflaridan biridir. Ho’sh bu kabi taxdidlar sodir bo’lishi va raqamli firibgarlar qurboniga aylanib qolishimizga nima sabab bo’lmoqda? Albatta, “extiyotsizligimiz” va raqamli texnologiyalar haqida yetarli tasavvur va bilimlarga ega bo’lmaganligimiz uchun, sabab sifatida faqat o’zimizni ko’rsatishimiz mumkin. Har doim ogohlik davr talabi bo’lib kelgan,

hozirgi raqamli texnologiyalar davrida shaxsiy ma’lumotlarimiz havfsizligiga jiddiy e’tibor qaratishimiz eng muhim omillardan biridir. Firibgarlar bugungi kunda texnologiyaning eng ilg’or imkoniyatlarini qurolga aylantirib, insonlarni aldashning tobora murakkab usullarini ishlab chiqishmoqda, lekin, extiyotsizlik va “soddaligimiz” oqibatida ularning ishlarini osonlashtirib shaxsiy ma’lumotlarimizni o’z qo’llarimiz bilan ularga topshirib qo’ymoqdamiz. Barchamizga ma’lumki hozirda ijtimoiy tarmoqlardan foydalanmaydigon insonlarni uchratish qiyin va biz aynan ijtimoiy tarmoqlar orqali xam o’z shaxsiy ma’lumotlarimizni “o’zimiz tarqatyapmiz”, bank kartalarimizni va suratlarini ko’p xollarda istalgan shaxslarga ishonib topshirmoqdamiz. Raqamli firibgarlik faqat individual foydalanuvchilarga emas, balki yirik tashkilotlarga, moliyaviy institutlarga va hatto davlat tizimlariga ham tahdid solmoqda. Har bir yangi texnologiya yangi imkoniyatlar bilan birga yangi zaifliklarni ham keltirib chiqaradi. Raqamli firibgarlikni oldini olish va unga qarshi samarali kurash muammosi bugungi kunda dolzarb masalaga aylangan. Hozirgi kunda mashinali o’rganish (machine learning) texnologiyalari bu kurashning markazida turib, firibgarlikni aniqlash va oldini olishda innovatsion yondashuvlarni taqdim etmoqda.

Mashinali o’rganish (Machine Learning, ML) — bu sun’iy intellektning bir bo’lagi bo’lib, raqamli firibgarliklarni aniqlashda nafaqat avtomatlashtirilgan tahlillarni o’tkazadi, balki firibgarlik sxemalaridagi anomalik xatti-harakatlarni sezib, ularni oldindan bashorat qilishga yordam beradi. Mashinali o’rganish raqamli xavfsizlikda eng samarali vositalardan biri sifatida tan olinadi. Firibgarlikni aniqlashda ML real vaqt rejimida tahlil qilish orqali shubhali tranzaksiyalarni filtrlash imkoniyatini beradi. Mashinali o’rganish algoritmlari, xususan, logistik regressiya, neyron tarmoqlar va qayta o’rganish usullari orqali firibgarlikni oldindan aniqlashda yuqori samaradorlikni beraoladi. Bu texnologiyalar, onlayn bank xizmatlarida tranzaksiya ma’lumotlari asosida anomaliyalarni sezish va xavfni baholash orqali firibgarliklarning oldini olishda foydalaniladi. Firibgarlikni aniqlash algoritmlari ko’pincha vaqtga bog’liq ketma-ketlik (time-series data) asosida ishlaydi. ML algoritmlari k-means clustering, autoencoderlar va random forest kabi texnikalarni qo’llash orqali katta hajmdagi ma’lumotlar orqali anomal xatti-harakatlarni ajratib ko’rsatadi. Marcos López de Prado o’zining "Machine Learning for Asset Managers" kitobida firibgarlikni aniqlash uchun "O’qituvchisiz o’qitish" metodlaridan foydalanishni tavsiya qiladi. Chunki bu usullar yangi bo’lib, oldindan noma’lum bo’lgan firibgarlik sxemalarini kashf etishda samaralidir. Mashinali o’rganish texnologiyalari real vaqt rejimida ishlaydigan tizimlar yaratish uchun qo’llaniladi. Bu tizimlar bir vaqtning o’zida yuzlab va hatto minglab tranzaksiyalarni tahlil qilib, ularning qonuniyligini baholaydi. Mashinali o’rganish algoritmlari faqat firibgarlikni aniqlash bilangina cheklanib qolmasdan, balki shaxsiy ma’lumotlarni himoya qilish uchun shifrlash (encryption) va ma’lumotlar maskirovkasini (data masking) ta’minlashda ham ishlatiladi. Mashinali o’rganish texnologiyalari

firibgarlikni global miqyosda kuzatish va oldini olish uchun kollektiv ma’lumotlarni tahlil qilish imkonini beradi. Xususan, moliyaviy institutlar o’rtasida birlashgan ma’lumotlar bazasi orqali firibgarlik sxemalarini aniqlashda katta imkoniyatlar yaratiladi. Mashinali o’rganishdagi yangi texnologiyalar, jumladan, reinforcement learning va adversarial learning, firibgarlikka qarshi kurashda juda samarali qo’llaniladi. Bu usullar firibgarlar ishlab chiqayotgan murakkab metodlarni aniqlash va ular bilan kurashda foydalaniladi. Mashinali o’rganish texnologiyalari nafaqat raqamli firibgarlikni aniqlash va oldini olishda, balki yirik tashkilotlarning xavfsizlik strategiyasini optimallashtirishda ham muhim o’rin tutadi. U firibgarlikni tez va yuqori aniqlikda anglay olishi orqali moliyaviy yo’qotishlarni kamaytiradi va foydalanuvchilar ishonchini oshiradi.

Albatta mashinali o’qitish taqdim etayotgan texnologiyalar raqamli firibgarlardan yetarli darajada saqlanish imkoni beradi, lekin bu taqdim etilayotgan imkoniyatlar faqat tizimlar uchungina ishlaydi, xo’sh unda biz o’zimizning shaxsiy ma’lumotlarimiz, hamyonlarimiz va o’z havfsizligimizni qanday qilib ta’minlashimiz mumkin? Bu savolga javob juda oddiy va biz quyidagi xavfsizlik qoidalariga rioya qilishimiz yetarli.

1. Kuchli va murakkab parollar yaratish.
2. Ikki bosqichli tekshiruvdan foydalanish.
3. Shubxali linklardan saqlanish.
4. Raqamli savodxonlikni oshirish.
5. Ijtimoiy tarmoqlarda shaxsiy surat, joy manzillari, fuqorolik pasporti va uning ma’lumotlari, bank plastik kartasi surati yoki ma’lumotlarini ko’rsatish va tarqatish kabi xolatlarni takrorlamaslik va oshkor qilmaslik.

Yuqoridagi tavsiyalarga amal qilish orqali siz o’zingizni sezilarli darajada raqamli hujumlardan himoya qilasiz.

Raqamli firibgarlar zamonaviy jamiyatning ko’rinmas xavfli dushmanlariga aylandi. Ular texnologiyaning imkoniyatlarini insoniyatning foydasi uchun emas, balki o’z g’arazli maqsadlariga xizmat qilish uchun yuksak mahorat bilan foydalanmoqdalar. Ammo, raqamli dunyoning cheksiz imkoniyatlari ularga qarshi qudratli qurolni ham taqdim etadi — bu zamonaviy texnologiyalar va insonning shubhasiz hushyorligi.

Firibgarlar o’z o’ljalarini qo’lga kiritishda bizning beparvoligimiz va xabardorligimizning yetishmasligidan foydalanadi. Lekin, aynan shu zaiflikni kuchli xavfsizlik strategiyalari bilan yengib o’tish mumkin. Bugungi kunning asosiy talabi — raqamli hayotimiz uchun mas’uliyatni o’z zimmamizga olish va bu borada bir qadam oldinda bo’lishdir.

Mashinali o’rganish texnologiyalari, sun’iy intellekt va ma’lumotlarni tahlil qilish vositalari, raqamli xavfsizlikni ta’minlashda hal qiluvchi o’rin tutmoqda. Ammo eng ilg’or tizimlar ham insonning e’tibori va ongli harakatlari bilan birgalikda

ishlaganda samarador bo'ladi. Firibgarlikning oldini olishning eng yaxshi usuli — ehtiyotkorlikni odatga aylantirish va har bir shubhali vaziyatni jiddiy qabul qilishdir.

Raqamli xavfsizlik — bu faqat texnologiyalarning emas, balki har bir insonning shaxsiy mas'uliyatidir. O'zimizni himoya qilish bilan birgalikda, atrofimizdagi raqamli ekotizimni xavfsiz saqlash uchun ham javobgarlikni his qilishimiz kerak. Shiddat bilan rivojlanayotgan raqamli firibgarlikka qarshi kurashda, biz texnologiya va hushyorlik bilan yuksak yutuqlarga erishishimiz mumkin. Shu bilan birga, raqamli dunyo nafaqat firibgarlar, balki ogoh va bilimli insonlar uchun ham cheksiz imkoniyatlar maydoniga aylanishi kerak.

Bu kurashda eng katta xavf — o'zimizning sustkashligimizdir. Shunday ekan, himoya qilish va ogoh bo'lish — vaqtning muqarrar talabidir.

Foydalanilgan adabiyotlar

1. "Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection" Bart Baesens, Véronique Van Vlasselaer, Wouter Verbeke
2. "Credit Risk Analytics: Measurement Techniques, Applications, and Examples in SAS" Bart Baesens, Daniel Roesch, Harald Scheule
3. "Machine Learning for Asset Managers" Marcos López de Prado
4. "Artificial Intelligence in Finance" Yves Hilpisch
5. "Financial Signal Processing and Machine Learning" Ali N. Akansu