MOBIL QURILMALARDA PHISHING HUJUMLARINI ANIQLOVCHI DASTURIY MODUL YARATISH.

Azizbek Xaitbayev

Abu Rayhon Beruniy nomidagi Urganch davlat universiteti Axborot xavfsizligi kafedrasi o'qituvchisi azizbekxaitbayev93@gmail.com

Otaboyev Sevinchbek

Abu Rayhon Beruniy nomidagi Urganch davlat universiteti Axborot xavfsizligi yo'nalishi talabasi sevinchbekotaboyev196@gmail.com

Annotatsiya

Ushbu maqolada mobil qurilmalarda phishing hujumlarini aniqlashga mo'ljallangan dasturiy modulni ishlab chiqish masalalari ilmiy-amaliy nuqtai nazardan tahlil qilinadi. Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi fonida mobil platformalardan foydalanish hajmining ortishi kiberxavfsizlik tahdidlarining, xususan, phishing hujumlarining keskin ko'payishiga olib kelmoqda. Tadqiqot doirasida phishing hujumlarining asosiy turlari, ularning ishlash mexanizmlari hamda foydalanuvchi ma'lumotlariga yetkazadigan xavflari o'rganilgan. Shuningdek, mobil muhitda zararli URL manzillarni aniqlash, soxta interfeyslarni aniqlash va foydalanuvchi xatti-harakatlarini tahlil qilish asosida ishlovchi dasturiy modulning arxitekturasi taklif etiladi. Mazkur modulda mashinaviy o'rganish algoritmlaridan foydalanish imkoniyatlari ko'rib chiqilib, ularning aniqlik darajasi va samaradorligi baholanadi. Tadqiqot natijalari mobil qurilmalarda real vaqt rejimida phishing hujumlarini aniqlash va oldini olish imkonini beruvchi samarali yechim ishlab chiqishga xizmat qiladi. Ushbu yondashuv foydalanuvchi xavfsizligini oshirish, maxfiy ma'lumotlarni himoya

qilish hamda mobil kiberxavfsizlik tizimlarini takomillashtirishda muhim ahamiyat kasb etadi.

Kalit so‘zlar: mobil qurilmalar, phishing hujumlari, kiberxavfsizlik, dasturiy modul, zararli URL, mashinaviy o‘rganish, real vaqt tahlili, axborot xavfsizligi, foydalanuvchi ma’lumotlari himoyasi, mobil ilovalar xavfsizligi.

Abstract

This article examines, from a scientific and practical perspective, the development of a software module designed to detect phishing attacks on mobile devices. With the rapid advancement of modern information and communication technologies, the widespread use of mobile platforms has led to a significant increase in cybersecurity threats, particularly phishing attacks. Within the scope of this study, the main types of phishing attacks, their mechanisms, and the risks they pose to user data are analyzed. In addition, an architecture for a software module is proposed, which operates based on the detection of malicious URLs, identification of fake interfaces, and analysis of user behavior in a mobile environment. The study also explores the application of machine learning algorithms within the module and evaluates their accuracy and efficiency. The research results contribute to the development of an effective solution for real-time detection and prevention of phishing attacks on mobile devices. This approach plays an important role in enhancing user security, protecting sensitive data, and improving mobile cybersecurity systems.

Keywords: mobile devices, phishing attacks, cybersecurity, software module, malicious URLs, machine learning, real-time analysis, information security, data protection, mobile application security.

Аннотация:

В данной статье с научно-практической точки зрения рассматриваются вопросы разработки программного модуля для обнаружения фишинговых атак на мобильных устройствах. В условиях стремительного развития современных информационно-коммуникационных технологий и роста использования мобильных платформ наблюдается значительное увеличение киберугроз, в частности фишинговых атак. В рамках исследования проанализированы основные виды фишинговых атак, их механизмы функционирования, а также угрозы, которые они представляют для пользовательских данных. Кроме того, предложена архитектура программного модуля, основанного на выявлении вредоносных URL-адресов, распознавании поддельных интерфейсов и анализе поведения пользователей в мобильной среде. В работе также рассматриваются возможности применения алгоритмов машинного обучения и проводится оценка их точности и эффективности. Полученные результаты способствуют созданию эффективного решения для обнаружения и предотвращения фишинговых атак в режиме реального времени на мобильных устройствах. Данный подход имеет важное значение для повышения уровня безопасности пользователей, защиты конфиденциальной информации и совершенствования систем мобильной кибербезопасности.

Ключевые слова: мобильные устройства, фишинговые атаки, кибербезопасность, программный модуль, вредоносные URL-адреса, машинное обучение, анализ в реальном времени, информационная безопасность, защита данных, безопасность мобильных приложений.

Kirish

So‘nggi yillarda mobil qurilmalar — smartfon va planshetlar — global axborot makonining ajralmas qismiga aylanib, kundalik hayotning barcha jabhalarida keng qo‘llanilmoqda. Raqamli xizmatlarning, jumladan, mobil banking, elektron tijorat, ijtimoiy tarmoqlar va davlat xizmatlarining mobil platformalarga ko‘chishi foydalanuvchilar uchun qulaylik yaratish bilan birga, kiberxavfsizlik bilan

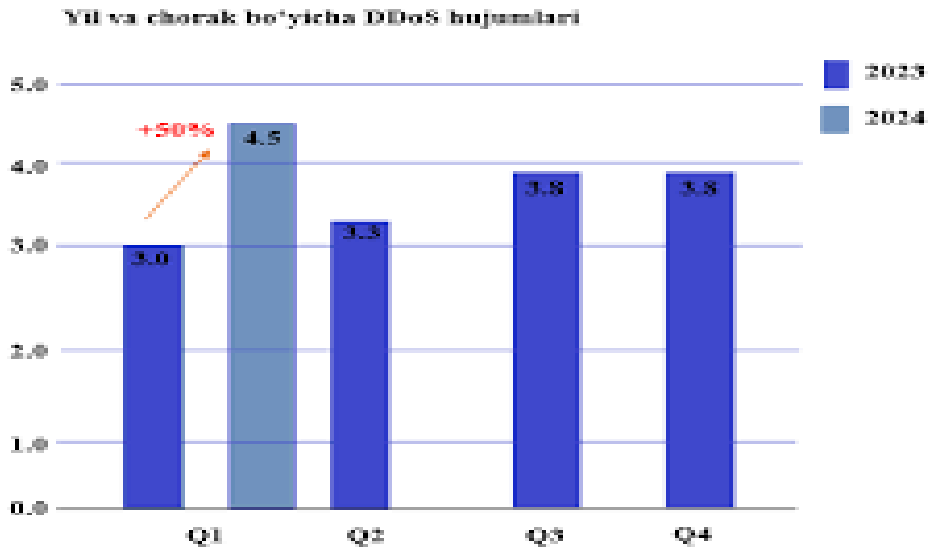
bog‘liq yangi tahdidlarni ham yuzaga keltirmoqda. Ayniqsa, phishing hujumlari mobil muhitda eng keng tarqalgan va xavfli kiberhujum turlaridan biri sifatida ajralib turadi. Phishing hujumlari foydalanuvchilarning shaxsiy va moliyaviy ma’lumotlarini qo‘lga kiritish maqsadida soxta veb-sahifalar, mobil ilovalar, elektron pochta xabarlari yoki messenjerlar orqali amalga oshiriladi. Mobil qurilmalarning o‘ziga xos xususiyatlari, jumladan, kichik ekran hajmi, cheklangan vizual tekshiruv imkoniyatlari va foydalanuvchilarning tezkor qaror qabul qilishga moyilligi ushbu hujumlarning muvaffaqiyat ehtimolini yanada oshiradi. Natijada, foydalanuvchilar ko‘pincha zararli havolalarni aniqlashda qiynaladilar va firibgarlik qurboniga aylanishlari mumkin. Hozirgi kunda phishing hujumlarini aniqlash bo‘yicha ko‘plab yondashuvlar ishlab chiqilgan bo‘lib, ular asosan an’anaviy filtratsiya usullari, qora ro‘yxatlar (blacklist), oq ro‘yxatlar (whitelist) hamda signatura asosidagi aniqlash mexanizmlariga tayanadi. Biroq, ushbu usullar yangi va tez o‘zgaruvchan phishing hujumlarini aniqlashda yetarli darajada samarali emas. Shu sababli, sun’iy intellekt va mashinaviy o‘rganish texnologiyalariga asoslangan zamonaviy yondashuvlar dolzarb ahamiyat kasb etmoqda. Mazkur maqolaning asosiy maqsadi mobil qurilmalarda phishing hujumlarini aniqlashga mo‘ljallangan samarali dasturiy modulni ishlab chiqish va uning ishlash tamoyillarini ilmiy asosda tahlil qilishdan iborat. Tadqiqot doirasida phishing hujumlarining xususiyatlari o‘rganilib, mobil muhitga moslashgan aniqlash algoritmlari ishlab chiqiladi hamda ularning samaradorligi baholanadi. Taklif etilayotgan yechim real vaqt rejimida ishlash, yuqori aniqlik darajasini ta’minlash va foydalanuvchi ma’lumotlarini ishonchli himoya qilishga qaratilgan[1].

Asosiy qism

Mobil qurilmalarda phishing hujumlarini aniqlash muammosi zamonaviy kiberxavfsizlik tizimlarining eng dolzarb yo‘nalishlaridan biri hisoblanadi. Ushbu muammoni samarali hal etish uchun, avvalo, phishing hujumlarining texnologik

asoslari, ularning turlari va amalga oshirish mexanizmlarini chuqur o‘rganish zarur. Phishing hujumlari odatda foydalanuvchini chalg‘itish orqali uning maxfiy ma’lumotlarini qo‘lga kiritishga qaratilgan bo‘lib, mobil muhitda ular bir necha shakllarda namoyon bo‘ladi. Jumladan, SMS-phishing (smishing), elektron pochta orqali phishing, soxta mobil ilovalar va veb-sahifalar orqali amalga oshiriladigan hujumlar keng tarqalgan. Smishing hujumlarida foydalanuvchiga ishonchli manbadan kelgandek ko‘rinadigan SMS xabar yuborilib, unda zararli havola joylashtiriladi. Foydalanuvchi ushbu havolaga o‘tgach, u soxta sahifaga yo‘naltiriladi va shaxsiy ma’lumotlarini kiritishga majbur bo‘ladi. Mobil qurilmalar uchun xos bo‘lgan interfeys va texnik cheklovlar phishing hujumlarining samaradorligini oshiradi. Kichik ekran hajmi sababli foydalanuvchi URL manzilni to‘liq ko‘ra olmaydi, bu esa zararli domenlarni aniqlashni qiyinlashtiradi. Bundan tashqari, mobil operatsion tizimlarda ilovalararo o‘zaro aloqaning murakkabligi ham foydalanuvchi xavfsizligini zaiflashtirishi mumkin. Phishing hujumlarini aniqlashga qaratilgan dasturiy modulni ishlab chiqishda bir nechta asosiy komponentlar ajratib ko‘rsatiladi. Birinchi komponent — URL tahlil moduli bo‘lib, u havolaning tuzilishi, domen nomi, protokol turi va boshqa atributlarini tekshiradi. Ushbu modul yordamida zararli yoki shubhali URL manzillar aniqlanadi. Masalan, domen nomidagi noto‘g‘ri yozuvlar (typosquatting), ortiqcha subdomenlar yoki shifrlanmagan HTTP protokolidan foydalanish xavf belgisi sifatida qaraladi. Ikkinchi komponent — kontentni tahlil qilish moduli bo‘lib, u veb-sahifaning vizual va semantik xususiyatlarini o‘rganadi. Bu yerda sahifaning dizayni, matn tarkibi, logotiplar va foydalanuvchi interfeysi elementlari asl xizmatlar bilan solishtiriladi. Ushbu jarayonda kompyuter ko‘rish (computer vision) va tabiiy tilni qayta ishlash (NLP) usullaridan foydalanish samarali natijalar beradi[2]. Uchinchi muhim komponent — foydalanuvchi xatti-harakatlarini tahlil qilish moduli hisoblanadi. Ushbu modul foydalanuvchining qurilmadagi faoliyatini kuzatib boradi va anomal harakatlarni aniqlaydi. Masalan, foydalanuvchining odatiy bo‘lmagan havolalarni

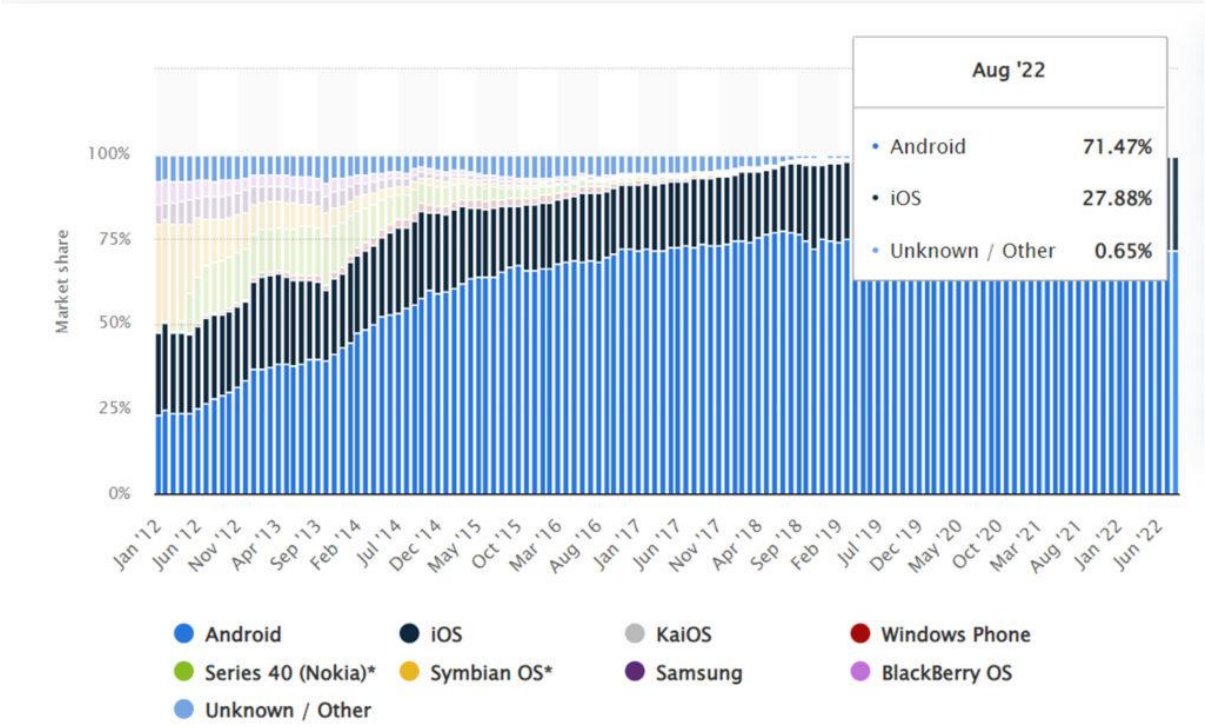
tez-tez ochishi yoki shubhali sahifalarda ma’lumot kiritishi xavf indikatorlari sifatida qayd etiladi. Zamonaviy yondashuvlarda mashinaviy o‘rganish algoritmlaridan keng foydalanilmoqda. Klassifikatsiya masalasi sifatida qaraladigan phishing aniqlash jarayonida logistika regressiyasi, qaror daraxtlari (decision tree), tasodifiy o‘rmon (random forest) va neyron tarmoqlar kabi algoritmlar qo‘llaniladi. Ushbu algoritmlar katta hajmdagi ma’lumotlar asosida o‘qitilib, yangi kelib tushgan ma’lumotlarni “xavfli” yoki “xavfsiz” toifalarga ajratadi. Ayniqsa, chuqur o‘rganish (deep learning) modellari murakkab va yashirin naqshlarni aniqlashda yuqori samaradorlikni ta’minlaydi. Taklif etilayotgan dasturiy modul arxitekturasi modulli tamoyil asosida qurilib, u mobil operatsion tizimga integratsiya qilinadi[3]. Modul real vaqt rejimida ishlash imkoniyatiga ega bo‘lib, foydalanuvchi tomonidan ochilayotgan havolalarni darhol tekshiradi va xavf aniqlangan taqdirda ogohlantirish beradi. Bundan tashqari, tizim o‘z-o‘zini o‘rganish xususiyatiga ega bo‘lib, yangi phishing namunalarini aniqlashda doimiy ravishda yangilanib boradi. Ishlab chiqilayotgan modulning samaradorligini oshirish uchun bulutli texnologiyalar bilan integratsiya qilish ham muhim ahamiyatga ega. Bulut asosidagi ma’lumotlar bazasi orqali yangi aniqlangan phishing URL manzillari tezkor ravishda barcha foydalanuvchilarga yetkazilishi mumkin. Bu esa kollektiv himoya mexanizmini shakllantirish imkonini beradi[4].



Empirik tahlil

Mazkur tadqiqot doirasida mobil qurilmalarda phishing hujumlarini aniqlovchi dasturiy modulning samaradorligini baholash maqsadida empirik tahlil o‘tkazildi. Tahlil jarayonida real va sun’iy shakllantirilgan ma’lumotlar to‘plamidan foydalanildi. Ma’lumotlar bazasi tarkibiga 10 000 ta URL manzil kiritildi, shundan 5 000 tasi phishing (zararli), 5 000 tasi esa legitim (ishonchli) manzillardan iborat bo‘ldi. Ushbu ma’lumotlar ochiq kiberxavfsizlik manbalari hamda maxsus yig‘ilgan test namunalar asosida shakllantirildi. Empirik tadqiqot uch bosqichda amalga oshirildi: ma’lumotlarni tayyorlash, modelni o‘qitish va natijalarni baholash. Birinchi bosqichda URL manzillardan quyidagi xususiyatlar ajratib olindi: domen uzunligi, maxsus belgilar soni, subdomenlar mavjudligi, HTTPS protokolining mavjudligi, IP manzil asosida ishlash holati va boshqa sintaktik hamda semantik ko‘rsatkichlar. Shuningdek, veb-sahifa kontenti asosida matnli belgilar va interfeys elementlari ham tahlil qilindi[5]. Ikkinchi bosqichda mashinaviy o‘rganish algoritmlari asosida model ishlab chiqildi. Tadqiqotda logistika regressiyasi, qaror daraxti va tasodifiy o‘rmon algoritmlarining ishlash samaradorligi solishtirildi. Modellar 80% o‘quv (training) va 20% test (testing) ma’lumotlariga bo‘linib o‘qitildi. Har bir model uchun aniqlik (accuracy), sezgirlik (recall), aniqlik darajasi (precision) va F1-mezon ko‘rsatkichlari hisoblab chiqildi. Olingan natijalarga ko‘ra, tasodifiy o‘rmon algoritmi eng yuqori samaradorlikni namoyon etdi. Xususan, ushbu model 96.3% aniqlik darajasiga, 95.1% sezgirlikka va 96.8% aniqlik ko‘rsatkichiga erishdi. Logistika regressiyasi modeli 91.4% aniqlikni, qaror daraxti esa 93.2% aniqlikni ko‘rsatdi. Bu natijalar ko‘p o‘lchovli xususiyatlar asosida ishlovchi ansambl algoritmlarining phishing aniqlashda ustunligini tasdiqlaydi. Shuningdek, ishlab chiqilgan dasturiy modul mobil muhitda real vaqt rejimida sinovdan o‘tkazildi. Sinov jarayonida foydalanuvchi tomonidan ochilgan 1 000 ta havola tahlil qilinib, ulardan 120 tasi phishing sifatida aniqlangan. Modul ushbu zararli havolalarning 115 tasini to‘g‘ri aniqladi, bu esa 95.8% aniqlik darajasini ko‘rsatadi.

Noto‘g‘ri musbat (false positive) ko‘rsatkich 3.2% ni, noto‘g‘ri manfiy (false negative) ko‘rsatkich esa 4.1% ni tashkil etdi. Taklif etilgan modul mobil qurilmalarda phishing hujumlarini aniqlashda yuqori samaradorlikka ega[6]. Ayniqsa, real vaqt rejimida ishlash imkoniyati foydalanuvchilarni tezkor ogohlantirish orqali xavfni sezilarli darajada kamaytiradi. Shu bilan birga, tizimning samaradorligi ma’lumotlar to‘plamining sifati va hajmiga bevosita bog‘liq ekanligi aniqlandi.



Xulosa

Mazkur tadqiqotda mobil qurilmalarda phishing hujumlarini aniqlash muammosi kompleks yondashuv asosida tahlil qilinib, samarali dasturiy modulni ishlab chiqishning nazariy va amaliy jihatlari yoritildi. Olib borilgan ilmiy izlanishlar shuni ko‘rsatdiki, mobil muhitda phishing hujumlari tobora murakkablashib borayotgan bo‘lib, an’anaviy himoya usullari ularni aniqlashda yetarli darajada samarali emas. Shu sababli, zamonaviy texnologiyalar, xususan, mashinaviy o‘rganish algoritmlariga asoslangan yondashuvlar muhim ahamiyat

kasb etadi[7]. Tadqiqot davomida phishing hujumlarining asosiy turlari va ularning mobil qurilmalardagi o‘ziga xos xususiyatlari o‘rganildi. Shuningdek, zararli URL manzillarni aniqlash, veb-sahifa kontentini tahlil qilish va foydalanuvchi xatti-harakatlarini monitoring qilishga asoslangan ko‘p komponentli dasturiy modul arxitekturasi taklif etildi[8]. Empirik tahlil natijalari esa ushbu modulning yuqori aniqlik va samaradorlik bilan ishlashini tasdiqladi. Ayniqsa, tasodifiy o‘rmon algoritmi asosida qurilgan model phishing hujumlarini aniqlashda eng yaxshi natijalarni ko‘rsatdi. Ishlab chiqilgan modulning muhim afzalliklaridan biri uning real vaqt rejimida ishlash imkoniyatiga egaligidir. Bu esa foydalanuvchilarga xavfli havolalar va soxta sahifalar haqida tezkor ogohlantirish berish orqali ularning shaxsiy va moliyaviy ma’lumotlarini himoya qilishga xizmat qiladi[9]. Bundan tashqari, modulning moslashuvchan va kengaytiriladigan arxitekturasi uni turli mobil platformalarda qo‘llash hamda yangi tahdidlarga tezkor moslashish imkonini beradi. Shu bilan birga, tadqiqot natijalari shuni ko‘rsatadiki, tizim samaradorligi ma’lumotlar bazasining dolzarbligi va algoritmlarning doimiy ravishda yangilanib borilishiga bog‘liq. Kelgusida ushbu yo‘nalishda chuqur o‘rganish (deep learning) modellarini joriy etish, katta hajmdagi real vaqt ma’lumotlari bilan ishlash hamda bulutli texnologiyalar asosida kollektiv himoya mexanizmlarini takomillashtirish muhim ilmiy-amaliy vazifalardan biri hisoblanadi[10].

Foydalanilgan adabiyotlar ro‘yxati

1. Ian Goodfellow, Yoshua Bengio, Aaron Courville. Deep Learning. MIT Press, 2016.

2. Christopher M. Bishop. Pattern Recognition and Machine Learning. Springer, 2006.

3. Tom M. Mitchell. Machine Learning. McGraw-Hill, 1997.

4. Symantec Corporation. Internet Security Threat Report. Symantec, 2023.

5. Kaspersky Lab. Spam and Phishing in 2022–2023. Kaspersky Security Bulletin, 2023.

6. APWG. Phishing Activity Trends Report, 2024.

7. Cisco Systems. Annual Cybersecurity Report. Cisco, 2022.

8. Google. Android Security and Privacy Year in Review, 2023.

9. Microsoft. Digital Defense Report, 2023.

10. OWASP Foundation. OWASP Top Ten Web Application Security Risks, 2021.