SUN'IY INTELLEKT ASOSIDA MOLIYAVIY KIBERXAVFLARNI ANIQLASHNING KONSEPTUAL ASOSLARI

Shermatov Axlidin Sharobiddin o'g'li
Andijon davlat universiteti
Fizika-Matematika va IT injeneringi fakulteti
70610101-Kompyuter tizimlari va
ularning dasturiy ta'minoti ta'lim
yo'nalishi 2-bosqich magistranti
Elektron pochta: akhlidinshermatov00@gmail.com

Annotatsiya: Ushbu maqolalar kiberxavflarni boshqarish tizimlarining amaliy ishlab chiqilishi va joriy etilishida Sun (SI) texnologiyaning kontseptual asoslari tahlil etiladi. Moliyaviy sektorda firibgarlik (firibgarlik), fishing (o'g'irlash) va boshqa kibertahdidlarning tezkor evolyutsiyasi jarayoni, an'anaviy imzo-asosidagi himoya mexanizmlari samarali samaradorlikni ta'minlay olmaydi. Tadqiqot SIning adaptiv, dinamik va ma'lumotlarga yo'qotilganligini tahlil qiladi. Maqolada katta hajmdagi ma'lumotlarni (Big Data) qayta ishlash, real vaqt rejimida qaror qabul qilish hamda tizimlarning doimiy o'z-o'zini o'rganish (Continuous Learning) uchun muhokama qilingan.

Kalit so'zlar: Sun'iy Intellekt (SI), Firibgarlikni Aniqlash (Firibgarlikni aniqlash), moliyaviy inqiroz, internet tarmog'I, zararli mobil ilovalar.

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ОБНАРУЖЕНИЯ ФИНАНСОВЫХ КИБЕРРИСКОВ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация: В данной статье анализируются концептуальные основы технологии искусственного интеллекта (ИИ) в практической разработке и внедрении систем управления киберрисками. В процессе быстрой эволюции мошенничества, фишинга и других киберугроз в финансовом секторе традиционные механизмы защиты на основе сигнатур не могут обеспечить эффективную защиту. В исследовании анализируется адаптивный, динамический и подверженный потере данных характер ИИ. В статье рассматриваются обработка больших объемов данных (Big Data), принятие решений в реальном времени и непрерывное самообучение систем (Continuous Learning).

Ключевые слова: Искусственный интеллект (ИИ), Обнаружение мошенничества, финансовый кризис, Интернет, вредоносные мобильные приложения.

CONCEPTUAL BASIS OF FINANCIAL CYBERRISK DETECTION BASED ON ARTIFICIAL INTELLIGENCE

Abstract: This article analyzes the conceptual foundations of Artificial Intelligence (AI) technology in the practical development and implementation of cyber risk management systems. In the process of rapid evolution of fraud (fraud), phishing (theft) and other cyber threats in the financial sector, traditional signature-based protection mechanisms cannot provide effective effectiveness. The study analyzes the adaptive, dynamic and data-losing nature of AI. The article discusses the processing of large amounts of data (Big Data), real-time decision-making and continuous self-learning of systems (Continuous Learning).

Keywords: Artificial Intelligence (AI), Fraud Detection (Fraud Detection), financial crisis, Internet, malicious mobile applications.

Kirish. Kiberxavfsizlik bu axborot **xavfsizligi, butunligi yoki zarar** tashkilotga, yoki operatsion zararlanishi mumkin bo'lgan har qanday potentsial zarar yoki havfdir. Moliyaviy sektorda kiberxavflar o'z ichiga oladi:

1. **Firibgarlik (Fraud):** Hisobni egallash, to'lovlarni o'zgartirish yoki soxta tranzaksiyalarni amalga oshirish.
2. **Ma'lumotlar Sizib Chiqishi (Data Breach):** Mijozlarning shaxsiy ma'lumotlari (PII) yoki bank ma'lumotlarining ruxsatsiz olishi.
3. **Hujumlar (Malware/Phishing):** Zararli dasturlar yoki fishing orqali tizimga kirish huquqini olishga urinish.
4. **Tizim Uzilishi (DDoS/System Failure):** Xizmat ko'rsatishni rad etish hujumlari orqali quvvat olishning to'xtatib qo'yilishi.

Kiberxavf xatoliklari, zarar, soxta natija cheklar, fishing URL'lar va zaharli APK fayllar shaklidagi hujumlar murakkablashib, **Sun'iy Intellect (SI) asosidagi tizimli** muammolarga qarshi kurashda samarali choralar. Sun'iy Intellekt Asosida Soxta Moliyaviy Cheklar, Fishing URL'lar va Zararli APK Fayllarni Aniqlash Tizimining Arxitekturasi. Tizimning arxitekturasi **modullilik (modularity)** , **real vaqtda berish (real-time processing)** va **doimiy o'rganish (continuous learning)** natijalariga asoslanadi. U uchta asosiy integratsiya turini alohida, ammo birlashgan modullar orqali tahlil qiladi.

Ma'lumotlarni Yig'ish va Tayyorlash Moduli (Ma'lumotlarni yig'ish va oldindan ishlov berish)

SI model ishlash bevosita o'quv uchun moddiy ma'lumotlarning sifati va miqdoriga bog'liq.

Tahdid Turi	Ma'lumot Manbalari	Tayyorlash usullari
Soxat Cheklar	Bank cheklari tasvirlari (haqiqiy va soxta namunalari), skanerlangan matnlar (OCR).	**Tasvirni normallashtirish** , **tasvirni segmentlash** , **Optical Character Recognition (OCR)** matnni olish va **ishlab chiqarishni vektorlashtirish** .
Fishing URL'lari	Haqiqiy va fishing URL ma'lumotlar bazalari, DNS yozuvlari, WHOIS ma'lumotlari.	**Leksik kimyoviy mahsulot** (masalan, domen mahsulot, maxsus asboblar), **xostga jarohat** (masalan, IP-manzil, domenning yoshi).
Zarar APK	VirusTotal API, kompaniyalari ma'lumotlari, mobil ilovalarning disassembler yordami.	**Statik tahlil** (kod omillar, ruxsatlar), **dinamik tahlil** (sandbox muhitida-dazatishni saqlash), **API chaqiruvlari ketma-ketligini vektor** .

Fishing Hujumlari (Phishing Attacks) va Moliyaviy Firibgarlik

Fishing hujumi – bu, firibgarlar o'zlarini ishonchli manba (masalan, bank, elektron pochta xizmati provayderi yoki mashhur kompaniya) deb ko'rsatgan holda, shaxsiy va moliyaviy ma'lumotlaringizni (parollar, kredit karta raqamlari, login ma'lumotlari) aldov yo'li bilan qo'lga kiritishga urinishidir.

Fishing Turlari

1. **Elektron Pochta Fishingi (Email Phishing):** Eng keng tarqalgan usul. Foydalanuvchi "shoshilinch" deb ko'rsatilgan elektron pochta xabaridagi havola orqali soxta veb-saytga yo'naltiriladi.
2. **Spear Phishing:** Ma'lum bir shaxs yoki tashkilotga yo'naltirilgan, juda aniq va ishonarli qilib tayyorlangan hujum.
3. **Smishing (SMS Phishing):** Matnli xabarlar (SMS) orqali amalga oshiriladi.
4. **Vishing (Voice Phishing):** Telefon orqali amalga oshiriladi, bunda avtomatik ovozli xabarlar yoki inson operatorlari qo'llaniladi.

Moliyaviy Mexanizmi

Firibgarlar maqsadi – bank hisobiga kirish, kartadan pul o'tkazish yoki o'g'irlangan ma'lumotlarni qora bozorda sotish orqali moliyaviy foyda ko'rish. Zararli dastur

(Malware - Malicious Software) – bu kompyuter tizimiga zarar yetkazish, uni ishdan chiqarish, noqonuniy nazorat o'rnatish yoki maxfiy ma'lumotlarni o'g'irlash uchun maxsus yaratilgan har qanday dasturiy ta'minot.

Tahlil va Himoya Strategiyalari.Moliyaviy firibgarliklarni tahlil qilish va oldini olishda quyidagi himoya strategiyalari muhim:

1. **Xabardorlik va Ta'lim:** Foydalanuvchilarni fishing belgilari, xavfsiz parollar yaratish va shaxsiy ma'lumotlarni qanday himoya qilish kerakligi haqida doimiy o'qitish.
2. **Ko'p Faktorli Autentifikatsiya (MFA/2FA):** Moliyaviy va muhim tizimlarga kirishda paroldan tashqari qo'shimcha tasdiqlash usulidan foydalanishni majburiy qilish.
3. **Antivirus va Antimalware Dasturlari:** Tizimga kirishga urinayotgan zararli dasturlarni aniqlash va bloklash uchun sifatli himoya dasturlaridan foydalanish.
4. **Doimiy Yangilanishlar (Patch Management):** Operatsion tizimlar, brauzerlar va ilovalarni eng so'nggi xavfsizlik yangilanishlari (patchlar) bilan doimiy yangilab borish, bu orqali ma'lum zaifliklarni bartaraf etish.
5. **Elektron Pochta Filtrlash:** Fishing xabarlarini avtomatik ravishda bloklaydigan kuchli filtr va spamlardan himoya tizimlarini joriy etish.

Adabiyotlar ro'yhati

1. Zararli dasturlar orqali amalga oshiriladigan kiberxavfsizlik ... https://csec.uz/uz/news/maqolalar/zararli-dasturlar-orqali-amalga-oshiriladigan-kiberxavfsizlik-tahdidlari/
2. Sun'iy intellekt va mashinani o'rganish yordamida kiberxavfsizlik tahdidlarini aniqlash - Hostragons® https://www.hostragons.com/uz/blog/suniy-intellekt-va-kiberxavfsizlik/
3. ILMIY TADQIQOTLAR VA ULARNING YECHIMLARI JURNALI https://worldlyjournals.com/index.php/ituy/article/download/10536/15049/28334
4. Kiberxavfsizlikka qarshi yetti tahdid https://ict.xabar.uz/uz/xavfsizlik/kiberxavfsizlikka-qarshi-etti-tahdid.
5. T A D Q I Q O T L A R jahon ilmiy – metodik jurnali https://scientific-jl.com/tad/article/download/12184/11815/23643