INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

YANGI RENESSANS

RESPUBLIKA ILMIY JURNALI

+998335668868
www.innoworld.net

Google Scholar doi zenodo OpenAIRE

YANGI RENESSANS

RESPUBLIKA ILMIY JURNALI
TO'PLAMI

3 - JILD, 1 - SON
2026

www.innoworld.net

O'ZBEKISTON-2026

CHUQUR O‘RGANISH MODELLARI YORDAMIDA ZARARLI DASTURLAR VA FISHING HUJUMLARINI ANIQLASH USULLARI

Bekmurodov Ulugbek Bahrom o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali Dotsenti PhD,
Almardonov Asliddin Faxriddin o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali Magistranti

Annotatsiya. Ushbu maqolada chuqur o‘rganish texnologiyalaridan foydalangan holda zararli dasturlar va fishing hujumlarini aniqlash usullari o‘rganildi. Tadqiqot davomida an’anaviy imzoga asoslangan aniqlash usullarining cheklovlari tahlil qilinib, ularning o‘rnini bosuvchi zamonaviy chuqur o‘rganish modellari taklif etildi. Zararli dasturlarni aniqlashda dastur fayllarining statik va dinamik xususiyatlari, fishing hujumlarini aniqlashda esa URL manzillar va matnli xabarlar tahlil qilindi.

Tadqiqotda sun’iy neyron tarmoqlar (ANN), konvolyutsion neyron tarmoqlar (CNN) hamda rekurrent neyron tarmoqlar (RNN, LSTM) qo‘llanildi. Tajriba natijalari chuqur o‘rganish modellarining aniqlik, qamrov va F1-ko‘rsatkichlar bo‘yicha an’anaviy mashinaviy o‘rganish usullaridan ustun ekanligini ko‘rsatdi. Xususan, CNN modeli zararli dasturlarni, LSTM modeli esa fishing hujumlarini aniqlashda eng yuqori samaradorlikni namoyish etdi. Olingan natijalar chuqur o‘rganish texnologiyalarining zamonaviy kiberxavfsizlik tizimlarida muhim ahamiyatga ega ekanligini tasdiqlaydi.

Kalit so‘zlar (Keywords): Chuqur o‘rganish, kiberxavfsizlik, zararli dasturlarni aniqlash, fishing hujumlarini aniqlash, sun’iy intellekt, sun’iy neyron tarmoqlar, konvolyutsion neyron tarmoqlar (CNN), rekurrent neyron tarmoqlar (RNN), uzoq qisqa muddatli xotira (LSTM).

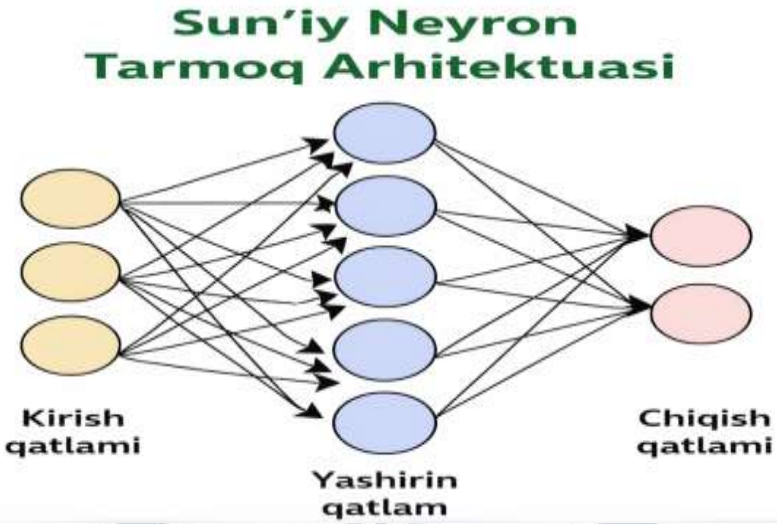
Kirish. So‘nggi yillarda raqamli texnologiyalar, internet xizmatlari va axborot tizimlarining jadal rivojlanishi jamiyatning deyarli barcha sohalarini qamrab oldi. Elektron tijorat, onlayn bank xizmatlari, masofaviy ta’lim va bulutli texnologiyalarning keng joriy etilishi axborot almashinuvi tezligini oshirgan bo‘lsa-da, bir vaqtning o‘zida kiberxavfsizlik bilan bog‘liq tahdidlarning keskin ortishiga ham sabab bo‘ldi. Bugungi kunda kiberjinoyatchilar tobora murakkab va yashirin usullardan foydalanib, foydalanuvchilarning shaxsiy ma’lumotlari, moliyaviy resurslari hamda muhim axborot infratuzilmalariga zarar yetkazishga intilmoqda.

Kiberxavfsizlik tahdidlari orasida zararli dasturlar (malware) va fishing hujumlari eng keng tarqalgan va xavfli hujum turlari hisoblanadi. Zararli dasturlar kompyuter tizimlariga ruxsatsiz kirish, ma’lumotlarni o‘g‘irlash, tizim ish

faoliyatini izdan chiqarish yoki masofadan boshqarish kabi zararli amallarni bajarishga mo‘ljallangan bo‘lsa, fishing hujumlari asosan foydalanuvchilarni aldash orqali ularning maxfiy ma’lumotlarini qo‘lga kiritishga qaratilgan. Ushbu hujumlar nafaqat oddiy foydalanuvchilarga, balki yirik tashkilotlar va davlat muassasalariga ham katta iqtisodiy va axborot yo‘qotishlariga olib kelmoqda.

An’anaviy kiberxavfsizlik tizimlari asosan imzoga (signature) asoslangan aniqlash usullariga tayangan holda ishlaydi. Bunday yondashuvlar oldindan ma’lum bo‘lgan zararli dasturlarni aniqlashda samarali bo‘lsa-da, yangi, modifikatsiyalangan yoki nol-kun (zero-day) hujumlarni aniqlashda sezilarli cheklovlarga ega. Kiberjinoyatchilar tomonidan zararli kodlarning doimiy ravishda o‘zgartirib borilishi va murakkab yashirish texnikalarining qo‘llanilishi an’anaviy usullarning samaradorligini keskin pasaytiradi. Natijada, zamonaviy kiberxavfsizlik tizimlari uchun moslashuvchan, o‘z-o‘zini o‘rganishga qodir va yuqori aniqlikka ega bo‘lgan yangi yondashuvlarga ehtiyoj tug‘ilmoqda.

Shu nuqtai nazardan, sun’iy intellekt va mashinaviy o‘rganish texnologiyalarining kiberxavfsizlik sohasiga joriy etilishi muhim ahamiyat kasb etmoqda. Ayniqsa, chuqur o‘rganish (Deep Learning) modellari katta hajmdagi murakkab va tuzilmagan ma’lumotlarni tahlil qilish, yashirin naqshlarni aniqlash hamda hujumlarni avtomatik tarzda tasniflash imkoniyatiga ega ekanligi bilan ajralib turadi. Chuqur neyron tarmoqlar ko‘p qatlamli tuzilma orqali ma’lumotlar orasidagi murakkab bog‘liqliklarni aniqlab, an’anaviy usullar aniqlay olmaydigan hujumlarni ham samarali tarzda aniqlashi mumkin 1-rasm.



1-rasm. Sun’iy neyron tarmog‘ining soddalashtirilgan arxitekturasi (kirish, yashirin va chiqish qatlamlari)

Zararli dasturlar va fishing hujumlarini aniqlashda chuqur o‘rganish modellarining qo‘llanilishi axborot xavfsizligini ta’minlashda yangi bosqichni boshlab berdi. Ushbu yondashuvlar statik va dinamik tahlil usullari bilan birgalikda ishlatilganda, hujumlarni real vaqt rejimida aniqlash, noto‘g‘ri musbat va noto‘g‘ri manfiy natijalarni kamaytirish hamda tizimning umumiy ishonchliligini oshirish imkonini beradi.

Mazkur tadqiqot ishining asosiy maqsadi chuqur o‘rganish modellaridan foydalangan holda zararli dasturlar va fishing hujumlarini aniqlash usullarini har tomonlama o‘rganish, mavjud yondashuvlarni tahlil qilish hamda ularning samaradorligini baholashdan iborat. Tadqiqot doirasida chuqur o‘rganishga asoslangan modellarni qo‘llash orqali kiberxavfsizlik tahdidlarini aniqlashning nazariy va amaliy jihatlari yoritiladi hamda kelajakdagi tadqiqotlar uchun istiqbolli yo‘nalishlar belgilanadi.

Metodologiya. Mazkur tadqiqotda zararli dasturlar va fishing hujumlarini aniqlash uchun chuqur o‘rganish modellariga asoslangan kompleks metodologik yondashuv qo‘llanildi. Taklif etilgan yondashuv ma’lumotlarni yig‘ish va tayyorlashdan boshlab, chuqur o‘rganish modellarini qurish, o‘qitish hamda ularning samaradorligini baholashgacha bo‘lgan ketma-ket bosqichlarni o‘z ichiga oladi. Tadqiqot metodologiyasi zararli dasturlar va fishing hujumlarining xususiyatlarini chuqur tahlil qilish hamda ularni aniq va ishonchli aniqlashga qaratilgan.

1. Ma’lumotlar to‘plamini tayyorlash. Tadqiqotning dastlabki bosqichida chuqur o‘rganish modellarini o‘qitish va sinovdan o‘tkazish uchun mos va sifatli ma’lumotlar to‘plami shakllantirildi. Zararli dasturlarni aniqlash jarayonida dastur fayllarining **statik** va **dinamik** xususiyatlari asosiy axborot manbai sifatida tanlandi. Statik tahlil doirasida dastur ruxsatlari, import qilingan kutubxonalar va kod strukturasi o‘rganildi. Dinamik tahlil esa dastur ishga tushirilgandan keyingi xatti-harakatlarini, jumladan API chaqiriqlari, fayl tizimi va tarmoq faoliyatini kuzatishga asoslandi.

Fishing hujumlarini aniqlashda esa **URL manzillar**, **elektron pochta matnlari** va **veb-sahifa kontentlari** tahlil qilindi. URL tuzilmasidagi shubhali belgilar, domen uzunligi, maxsus kalit so‘zlar hamda matnli xabarlardagi manipulyativ iboralar asosiy belgilar sifatida ajratib olindi. Yig‘ilgan ma’lumotlar shovqin va takroriy yozuvlardan tozalandi, normallashtirildi hamda chuqur o‘rganish modellariga mos formatga keltirildi. Ushbu bosqich modelning umumlashuv qobiliyatini oshirishda muhim ahamiyat kasb etdi.

2. Chuqur o‘rganish modellarini tanlash va qurish. Tadqiqotda zararli dasturlar va fishing hujumlarini aniqlash uchun chuqur o‘rganishning bir nechta samarali modellari qo‘llanildi. Har bir model ma’lumotlarning turiga va xususiyatiga mos ravishda tanlandi. Sun’iy neyron tarmoqlar (ANN) asosiy tasniflash modeli sifatida ishlatildi. Ushbu model kiruvchi xususiyatlar va chiqish natijalari o‘rtasidagi murakkab bog‘liqliklarni aniqlashda samarali bo‘lib, umumiy aniqlash natijalarini taqqoslash uchun bazaviy model vazifasini bajardi 2-rasm.

2-rasm – Kiberxavfsizlik xizmatlari konseptual modeli.

Konvolyutsion neyron tarmoqlar (CNN) zararli kod strukturalari va fishing URL naqshlarini aniqlashda qo‘llanildi. CNN modellarining konvolyutsion qatlamlari kod va URL ichidagi lokal naqshlarni aniqlab, ularni yuqori darajadagi xususiyatlarga aylantirish imkonini berdi. Bu yondashuv, ayniqsa, yashirin va modifikatsiyalangan hujumlarni aniqlashda yuqori samaradorlik ko‘rsatdi.

Rekurrent neyron tarmoqlar (RNN) va ularning rivojlangan turi bo‘lgan LSTM modellar ketma-ketlikka asoslangan ma’lumotlarni tahlil qilish uchun tanlandi. API chaqiriqlari ketma-ketligi va matnli fishing xabarlarining vaqt bo‘yicha bog‘liqligini aniqlashda ushbu modellar muhim rol o‘ynadi. LSTM xotira mexanizmi uzoq muddatli bog‘liqliklarni saqlab qolish orqali hujumlarni yanada aniq aniqlash imkonini yaratdi.

3. Modelni o‘qitish va baholash. Chuqur o‘rganish modellarini baholash jarayonida ma’lumotlar to‘plami o‘quv va test qismlariga bo‘lindi. O‘quv to‘plami modelni o‘qitish uchun, test to‘plami esa uning umumlashuv qobiliyatini baholash uchun ishlatildi. Modelni o‘qitish jarayonida haddan tashqari moslashuv (overfitting) muammosini oldini olish maqsadida muntazamlashtirish va validatsiya usullaridan foydalanildi.

Baholash mezonlari sifatida aniqlik (accuracy), aniqlash darajasi (precision), qamrov (recall) va F1-ko‘rsatkichlar tanlandi. Ushbu mezonlar modellarni nafaqat umumiy aniqlik bo‘yicha, balki noto‘g‘ri musbat va noto‘g‘ri manfiy natijalarni hisobga olgan holda solishtirish imkonini berdi. Har bir modelning natijalari o‘zaro taqqoslanib, qaysi yondashuv zararli dasturlar va fishing hujumlarini aniqlashda samaraliroq ekanligi aniqlandi.

Natijalar. Mazkur tadqiqot doirasida o‘tkazilgan tajribalar natijalari chuqur o‘rganish modellarining zararli dasturlar va fishing hujumlarini aniqlashda an’anaviy mashinaviy o‘rganish usullariga nisbatan ancha yuqori samaradorlikka ega ekanligini yaqqol namoyon etdi. Tajribalar turli xil ma’lumotlar to‘plamlari va

baholash mezonlari asosida amalga oshirildi hamda har bir modelning aniqlash qobiliyati alohida tahlil qilindi 3-rasm.

3-rasm – Zararli dasturlar va fishing hujumlarini aniqlashda chuqur o‘rganish modellarining samaradorligi.

Zararli dasturlarni aniqlash bo‘yicha o‘tkazilgan tajribalar shuni ko‘rsatdiki, konvolyutsion neyron tarmoqlar (CNN) ushbu vazifada eng yuqori natijalarni qayd etdi. CNN modeli dastur kodlari va ularning statik hamda dinamik xususiyatlari ichidagi yashirin va murakkab naqshlarni samarali aniqlashga muvaffaq bo‘ldi. Ayniqsa, an’anaviy klassifikatsiya usullari aniqlay olmaydigan modifikatsiyalangan va ilgari noma’lum bo‘lgan zararli dasturlarni aniqlashda CNN modeli yuqori aniqlikni namoyish etdi.

Tajriba natijalari shuni ko‘rsatdiki, CNN modeli yordamida zararli dasturlarni aniqlashda aniqlik (accuracy) va aniqlash darajasi (precision) sezilarli darajada oshdi. Bu esa noto‘g‘ri musbat holatlarning kamayishiga va tizimning umumiy ishonchliligining ortishiga olib keldi. Natijada, zararli dasturlarni real vaqt rejimida aniqlash imkoniyati yaxshilandi.

Fishing hujumlarini aniqlash jarayonida esa rekurrent neyron tarmoqlar (RNN) va ayniqsa LSTM modeli eng samarali natijalarni ko‘rsatdi. LSTM modelining ketma-ketlikka asoslangan tuzilmasi matnli xabarlar va URL manzillaridagi vaqt va mantiqiy bog‘liqliklarni chuqur tahlil qilish imkonini berdi. Bu xususiyat fishing hujumlariga xos bo‘lgan manipulyativ iboralar va yashirin tuzilmalarni aniqlashda muhim rol o‘ynadi.

Natijalarga ko‘ra, LSTM modeli fishing xabarlarini aniqlashda yuqori qamrov (recall) ko‘rsatkichiga erishdi, ya’ni hujumlarning katta qismi muvaffaqiyatli aniqlangan. Shu bilan birga, noto‘g‘ri musbat natijalar sonining kamayishi foydalanuvchilarga keraksiz ogohlantirishlar sonini qisqartirdi va tizim samaradorligini oshirdi.

Tajriba natijalari shuni ko‘rsatdiki, chuqur o‘rganish modellariga asoslangan tizimlar yangi va ilgari uchramagan hujumlarni ham yuqori aniqlik bilan aniqlash qobiliyatiga ega. Bu esa ularni zamonaviy va tez o‘zgaruvchan kiberxavfsizlik muhitida qo‘llash uchun istiqbolli yechimga aylantiradi.

Muhokama va xulosa. O‘tkazilgan tadqiqot natijalari chuqur o‘rganish texnologiyalarining zararli dasturlar va fishing hujumlarini aniqlashda yuqori samaradorlikka ega ekanligini tasdiqlaydi. Tadqiqot davomida qo‘llanilgan modellar an’anaviy imzoga asoslangan va klassik mashinaviy o‘rganish usullariga nisbatan murakkab va yashirin hujumlarni aniqlashda ancha ustun natijalarni namoyish etdi. Bu holat chuqur o‘rganish modellarining katta hajmdagi ma’lumotlar ichidan yashirin naqshlar va murakkab bog‘liqliklarni avtomatik aniqlash qobiliyati bilan izohlanadi.

4-rasm. Chuqur o‘rganish texnologiyalarining zararli dasturlar va fishing hujumlarini aniqlashdagi samaradorligi

Muhokama jarayonida aniqlanganki, konvolyutsion neyron tarmoqlar zararli dasturlarni aniqlashda ayniqsa samarali bo‘lib, kod strukturasi va xatti-harakatlardagi lokal xususiyatlarni aniqlashda muhim rol o‘ynaydi. Rekurrent neyron tarmoqlar va LSTM modellar esa fishing hujumlariga xos bo‘lgan matn va URL ketma-ketliklaridagi vaqt va mantiqiy bog‘liqliklarni chuqur tahlil qilish imkonini beradi. Ushbu modellar real muhitda tez-tez uchraydigan modifikatsiyalangan va ilgari noma’lum bo‘lgan hujumlarni aniqlashda yuqori aniqlikni ta’minladi.

Kelgusidagi tadqiqotlar uchun chuqur o‘rganish modellarini optimallashtirish, ularni yengillashtirilgan arxitekturalar asosida qurish va real vaqt

rejimida ishlashga moslashtirish istiqbolli yo‘nalishlardan biri hisoblanadi. Shuningdek, gibrid yondashuvlar — ya’ni chuqur o‘rganish modellarini an’anaviy aniqlash usullari bilan birgalikda qo‘llash orqali kiberxavfsizlik tizimlarining aniqligi va barqarorligini yanada oshirish mumkin. Avtomatik o‘rganish, transfer learning va federativ o‘rganish kabi zamonaviy yondashuvlar ham ushbu sohada katta salohiyatga ega.

Xulosa qilib aytganda, chuqur o‘rganishga asoslangan yondashuvlar zamonaviy kiberxavfsizlik muammolarini hal etishda muhim ilmiy va amaliy ahamiyat kasb etadi. Ushbu texnologiyalar zararli dasturlar va fishing hujumlariga qarshi kurashda yuqori aniqlik, moslashuvchanlik va istiqbolli rivojlanish imkoniyatlarini ta’minlaydi. Kelajakda chuqur o‘rganish modellarining takomillashuvi kiberxavfsizlik tizimlarining asosiy texnologik poydevorlaridan biri bo‘lib qolishini kutish mumkin.

Adabiyotlar ro‘yxati (References)

1. Goodfellow, I., Bengio, Y., & Courville, A. Deep Learning. MIT Press, 2016.
2. Bishop, C. M. Pattern Recognition and Machine Learning. Springer, 2006.
3. Saxe, J., & Berlin, K. “Deep Neural Network Based Malware Detection Using Two Dimensional Binary Program Features.” 10th International Conference on Malicious and Unwanted Software (MALWARE), 2015.
4. Raff, E., Barker, J., Sylvester, J., Brandon, R., Catanzaro, B., & Nicholas, C. “Malware Detection by Eating a Whole EXE.” Workshops at the Thirty-Second AAAI Conference on Artificial Intelligence, 2018.
5. LeCun, Y., Bengio, Y., & Hinton, G. “Deep Learning.” Nature, vol. 521, no. 7553, 2015, pp. 436–444.
6. Hochreiter, S., & Schmidhuber, J. “Long Short-Term Memory.” Neural Computation, vol. 9, no. 8, 1997, pp. 1735–1780.
7. Sahingoz, O. K., et al. “Machine Learning Based Phishing Detection from URLs.” Expert Systems with Applications, vol. 117, 2019, pp. 345–357.
8. Shafiq, M. Z., et al. “A Framework for Efficient Mining of Malware Data.” Proceedings of the 2012 ACM SIGSAC Conference on Computer and Communications Security, 2012.