SUN’IY INTELLEKT ASOSIDAGI KIBERHUJUMLARNI ANIQLASH VA OLDINI OLISH MUAMMOLARI.

Muqimov Shahzodbek Ixtiyor o‘g‘li
Qarshi davlat texnika universiteti assistenti.
Toshmurodov A.B.
Qarshi davlat texnika universiteti talabasi.

Annotatsiya: Mazkur tadqiqotda sun’iy intellekt texnologiyalari yordamida amalga oshirilayotgan kiberhujumlar, ularning axborot tizimlariga ta’siri hamda zamonaviy himoya vositalarining samaradorligi tahlil qilindi. Tadqiqot natijasida sun’iy intellekt asosidagi IDS, IPS va SIEM tizimlarining kiberhujumlarni aniqlashdagi afzalliklari o‘rganilib, axborot xavfsizligini ta’minlash bo‘yicha amaliy tavsiyalar ishlab chiqildi.

Kalit so‘zlar: kiberxavfsizlik, kriptografiya, sun’iy intellekt, kiberhujum, axborot xavfsizligi, shifrlash algoritmlari, autentifikatsiya, post-kvant kriptografiya.

ISSUES IN THE DETECTION AND PREVENTION OF ARTIFICIAL INTELLIGENCE-DRIVEN CYBERATTACKS.

Muqimov Sh. I.
Assistant, Karshi State Technical University
Toshmurodov A.B.
Student, Karshi State Technical University

Abstract: This study analyzes cyberattacks carried out using artificial intelligence technologies, their impact on information systems, and the effectiveness of modern security solutions. The research examines the advantages of AI-based IDS, IPS, and SIEM systems in detecting cyberattacks and develops practical recommendations for ensuring information security.

Keywords: cybersecurity, cryptography, artificial intelligence, cyberattack, information security, encryption algorithms, authentication, post-quantum cryptography.

KIRISH

Bugungi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida inson faoliyatining barcha sohalari raqamlashtirilmoqda. Elektron hukumat

tizimlari, internet bank xizmatlari, masofaviy ta’lim platformalari, elektron tijorat hamda bulutli texnologiyalarning keng qo‘llanilishi axborot xavfsizligini ta’minlash masalasini yanada dolzarb qilib qo‘ymoqda. Shu bilan birga, internet tarmoqlarida sodir etilayotgan kiberjinoyatlar soni ham ortib bormoqda. Kiberhujumlar natijasida foydalanuvchilarning shaxsiy ma’lumotlari, bank rekvizitlari va maxfiy hujjatlari noqonuniy ravishda qo‘lga kiritilmoqda. Ayniqsa, sun’iy intellekt asosida yaratilayotgan avtomatlashtirilgan zararli dasturlar va murakkab hujum tizimlari an’anaviy himoya vositalari imkoniyatlarini cheklab qo‘ymoqda. Shu sababli zamonaviy kiberxavfsizlik texnologiyalarini ishlab chiqish va ularni amaliyotga tatbiq etish muhim ilmiy va amaliy ahamiyat kasb etadi. Raqamli texnologiyalarning jadal rivojlanishi natijasida axborot tizimlari hayotning barcha sohalariga kirib bormoqda. Elektron hukumat, masofaviy ta’lim, elektron tijorat va bulutli texnologiyalar keng qo‘llanilishi bilan bir qatorda kiberxavfsizlik masalalari ham dolzarb ahamiyat kasb etmoqda. So‘nggi yillarda sun’iy intellekt texnologiyalarining rivojlanishi kiberjinoyatchilar uchun yangi imkoniyatlarni yaratdi. Natijada avtomatlashtirilgan fishing hujumlari, deepfake texnologiyalari va aqlli zararli dasturlar paydo bo‘ldi.

Mazkur tadqiqotning maqsadi sun’iy intellekt asosidagi kiberhujumlarni tahlil qilish, ularni aniqlash va oldini olishning zamonaviy usullarini o‘rganishdan iborat.

ASOSIY QISM.

Kiberxavfsizlik sohasidagi asosiy muammolardan biri foydalanuvchi ma’lumotlarining noqonuniy o‘g‘irlanishi hisoblanadi. Hozirgi kunda fishing hujumlari, zararli dasturlar, ransomware, DDoS hujumlari va tarmoqqa noqonuniy kirish holatlari keng tarqalgan. Fishing hujumlari orqali foydalanuvchilarning login va parollari qo‘lga kiritiladi, ransomware dasturlari esa qurilmadagi fayllarni shifrlab, ularni tiklash uchun pul talab qiladi. DDoS hujumlari server faoliyatini izdan chiqarib, xizmat ko‘rsatishni to‘xtatib qo‘yadi. Bundan tashqari, IoT qurilmalarining ommalashuvi ham xavfsizlik muammolarini kuchaytirmoqda. Ko‘plab aqlli qurilmalar kuchsiz himoya tizimiga ega bo‘lgani sababli kiberjinoyatchilar uchun qulay nishonga aylanmoqda[2].

Kriptografiya axborot xavfsizligini ta’minlashning eng muhim vositalaridan biri hisoblanadi. U ma’lumotlarni maxsus algoritmlar yordamida shifrlash orqali begona shaxslarning ulardan foydalanishini cheklaydi. Hozirgi vaqtda AES, RSA, SHA va

ECC kabi zamonaviy kriptografik algoritmlar keng qo‘llanilmoqda. AES algoritmi yuqori tezlik va ishonchlilikka ega bo‘lib, davlat va tijorat tashkilotlarida faol ishlatiladi. RSA algoritmi ochiq kalitli kriptografiya asosida ishlaydi va elektron raqamli imzo yaratishda muhim ahamiyatga ega. Kriptografiya ma’lumotlarning maxfiyligini ta’minlash, axborot yaxlitligini saqlash, foydalanuvchilarni autentifikatsiya qilish hamda tarmoq xavfsizligini kuchaytirish kabi vazifalarni bajaradi. Biroq kvant kompyuterlarining rivojlanishi mavjud kriptografik algoritmlar xavfsizligiga jiddiy tahdid tug‘dirmoqda. Shu sababli post-kvant kriptografiya yo‘nalishida yangi algoritmlar ustida ilmiy tadqiqotlar olib borilmoqda.

Sun’iy intellekt texnologiyalari kiberxavfsizlik tizimlarida keng qo‘llanilmoqda. Mashinaviy o‘qitish algoritmlari yordamida tarmoqdagi shubhali faoliyatni avtomatik ravishda aniqlash va tahdidlarni oldindan prognoz qilish mumkin. Sun’iy intellekt asosidagi IDS va IPS tizimlari tarmoqdagi g‘ayritabiiy harakatlarni aniqlab, hujumlarni bloklaydi. SIEM tizimlari esa turli manbalardan kelayotgan xavfsizlik ma’lumotlarini tahlil qilib, administratorlarga real vaqt rejimida ogohlantirish yuboradi. Bu esa kiberhujumlarning oldini olish va axborot tizimlari xavfsizligini oshirishda muhim rol o‘ynaydi.

Kiberxavfsizlikni kuchaytirish uchun bir qator zamonaviy yechimlardan foydalanish zarur. Jumladan, ko‘p bosqichli autentifikatsiya tizimini joriy etish foydalanuvchi akkauntlarini himoyalash samaradorligini oshiradi. Paroldan tashqari SMS kod, biometrik ma’lumot yoki mobil tasdiqlash tizimidan foydalanish xavfsizlik darajasini sezilarli oshiradi. Shuningdek, AES-256 va ECC kabi kuchli shifrlash algoritmlaridan foydalanish ma’lumotlar xavfsizligini ta’minlashda muhim hisoblanadi. Dasturiy ta’minotlarni muntazam yangilab borish ham xavfsizlikdagi zaifliklarni kamaytiradi. Bundan tashqari, xodimlarning kiberxavfsizlik savodxonligini oshirish maqsadida muntazam treninglar tashkil etish muhim ahamiyatga ega .

Tadqiqot metodologiyasi. Tadqiqot jarayonida ilmiy adabiyotlarni tahlil qilish, qiyosiy tahlil, statistik ma’lumotlarni o‘rganish hamda zamonaviy kiberxavfsizlik tizimlarining ishlash tamoyillarini baholash usullaridan foydalanildi. Sun’iy intellekt asosida ishlovchi IDS (Intrusion Detection System), IPS (Intrusion Prevention

System) va SIEM (Security Information and Event Management) tizimlarining imkoniyatlari o‘rganildi.

Shuningdek, AES, RSA va ECC kabi kriptografik algoritmlarning xavfsizlik darajasi tahlil qilinib, zamonaviy kiberhujumlarga qarshi qo‘llanilish samaradorligi baholandi.

Natijalar. Tadqiqot natijalari sun’iy intellekt texnologiyalarining nafaqat himoya vositasi, balki hujum vositasi sifatida ham qo‘llanilayotganligini ko‘rsatdi. Aniqlanishicha, generativ sun’iy intellekt yordamida yaratilgan fishing xabarlari oddiy fishing hujumlariga nisbatan foydalanuvchilarni chalg‘itish ehtimolini oshiradi.

Tahlillar natijasida IDS va IPS tizimlari yordamida tarmoqdagi g‘ayritabiiy faoliyatlarni real vaqt rejimida aniqlash imkoniyati mavjudligi aniqlandi. SIEM tizimlari esa turli manbalardan olingan ma’lumotlarni markazlashgan holda tahlil qilib, tahdidlar haqida tezkor ogohlantirish berishi kuzatildi.

Ko‘p bosqichli autentifikatsiya, AES-256 shifrlash algoritmi va biometrik identifikatsiya vositalari axborot xavfsizligini sezilarli darajada oshirishi aniqlandi.

MUHOKAMA. Bugungi kunda sun’iy intellekt texnologiyalarining rivojlanishi kiberxavfsizlik sohasida yangi imkoniyatlar yaratishi bilan birga, yangi tahdidlarning paydo bo‘lishiga ham sabab bo‘lmoqda. Jumladan, generativ sun’iy intellekt vositalari yordamida yaratilayotgan fishing xabarlari va deepfake texnologiyalari foydalanuvchilarni aldash darajasini oshirmoqda. Shu sababli an’anaviy xavfsizlik vositalari bilan bir qatorda sun’iy intellekt asosida ishlovchi himoya tizimlarini joriy etish zarur hisoblanadi. Bundan tashqari, tashkilotlarda muntazam xavfsizlik auditi o‘tkazish, xodimlarning kiberxavfsizlik bo‘yicha bilimlarini oshirish va ko‘p bosqichli autentifikatsiyadan foydalanish kiberhujumlar xavfini sezilarli kamaytiradi.

XULOSA

Tadqiqot natijalari shuni ko‘rsatdiki, raqamli texnologiyalar va internet xizmatlarining keng rivojlanishi bilan bir qatorda kiberxavfsizlik masalalari ham dolzarb ahamiyat kasb etmoqda. Ayniqsa, sun’iy intellekt texnologiyalarining rivojlanishi kiberjinoyatchilar uchun yangi imkoniyatlar yaratib, kiberhujumlarning murakkablashishiga sabab bo‘lmoqda. Fishing, ransomware, DDoS hujumlari,

deepfake texnologiyalari va avtomatlashtirilgan zararli dasturlar zamonaviy axborot tizimlari uchun jiddiy xavf tug‘dirmoqda.

Tadqiqot davomida sun’iy intellekt asosidagi IDS, IPS va SIEM tizimlarining kiberhujumlarni aniqlash va oldini olishdagi samaradorligi tahlil qilindi. Olingan natijalar mazkur tizimlar tarmoqdagi g‘ayritabiiy faoliyatlarni tezkor aniqlash, tahdidlarni prognozlash hamda real vaqt rejimida xavfsizlik monitoringini amalga oshirish imkonini berishini ko‘rsatdi. Shuningdek, zamonaviy kriptografik algoritmlar, jumladan AES, RSA va ECC texnologiyalarining ma’lumotlar maxfiyligi va yaxlitligini ta’minlashdagi ahamiyati yoritildi.

Kiberxavfsizlikni ta’minlashda faqat texnik vositalar bilan cheklanib qolmasdan, foydalanuvchilarning axborot xavfsizligi bo‘yicha bilim va ko‘nikmalarini oshirish ham muhim omil hisoblanadi. Xodimlar va foydalanuvchilarni muntazam ravishda o‘qitish, ko‘p bosqichli autentifikatsiya tizimlaridan foydalanish, dasturiy ta’minotlarni muntazam yangilab borish hamda xavfsizlik siyosatiga qat’iy rioya qilish kiberxavflarni kamaytirishga xizmat qiladi.

Foydalanilgan adabiyotlar

1. Muqimov Sh.I. Ta'lim tizimida sun'iy intelektdan foydalanish. http://www.tadqiqotlar.uz/ 26-to’plam dekabr 219-221b. 2023y.
2. Anderson, T. (2017). *The Theory and Practice of Online Learning*. AU Press.
3. Cisco Networking Academy. (2023). Introduction to Packet Tracer. Retrieved from
   Cisco Networking Academy
4. SR Ochilova, SI Muqimov, ZD Dilmurodov, M Usmonov. Zamonaviy robototexnik platformalarlarda qo‘llaniladigan mikrokontrollerlar. Молодые ученые, 2024
5. Kholikova, N. (2020). Poetic Features of Uzbek Poetry of the National Awakening Period. *ISJ Theoretical & Applied Science, 04*(84), 615–623.
6. Бекматов, А. К., & Рустамов, Т. С. (2024). Роль глубокого обучения в улучшении точности систем обнаружения вторжений. *Экономика и социум*, (6-1 (121)), 1582-1591.

7. Бекматов А.К., & Эргашов Ф.Т. (2025). ОБЕСПЕЧЕНИЕ АУТЕНТИФИКАЦИИ В СЕТИ ПЕРЕДАЧИ ДАННЫХ. Экономика и социум, (1-2 (128)), 1013-1017.