DAVLAT AXBOROT TIZIMLARIDA KIBERXAVFSIZLIKNI TA'MINLASHNING INTELLEKTUAL MONITORING MODELINI ISHLAB CHIQISH

Khusenova Latofat

Annotatsiya. *Ushbu maqolada davlat axborot tizimlarida kiberxavfsizlikni ta'minlashning intellektual monitoring modeli ishlab chiqilgan. Tadqiqot O'zbekistonda keng qo'llanilayotgan "my.gov.uz", "E-qaror" kabi raqamli platformalar xavfsizligini oshirishga qaratilgan. Mashinali o'rganish asosida tahdidlarni real vaqt rejimida aniqlash va tahlil qilish mexanizmlari taklif etildi. Olingan natijalar tizimning samaradorligi va moslashuvchanligini isbotladi.*

Kalit so'zlar: *kiberxavfsizlik, intellektual monitoring, mashinali o'rganish, davlat axborot tizimlari, tahdidlarni aniqlash.*

Abstract. *This article focuses on the development of an intelligent monitoring model for ensuring cybersecurity in state information systems. The research is aimed at improving the security of digital platforms such as "my.gov.uz" and "E-qaror". Machine learning techniques are applied to detect cyber threats in real time and analyze abnormal system behavior. The experimental results confirm the effectiveness of the proposed model in enhancing security, reducing risks, and improving the reliability of government digital services.*

Keywords: *cybersecurity, intelligent monitoring, machine learning, state information systems, threat detection.*

Аннотация. *В статье рассматривается разработка интеллектуальной модели мониторинга для обеспечения кибербезопасности государственных информационных систем. Исследование направлено на повышение защищенности цифровых платформ, таких как «my.gov.uz» и «E-qaror». В работе применяются методы машинного обучения для выявления угроз в режиме реального времени. Полученные результаты подтверждают эффективность модели и её значимость для повышения устойчивости государственных информационных ресурсов.*

Ключевые слова: *кибербезопасность, интеллектуальный мониторинг, машинное обучение, государственные информационные системы, выявление угроз.*

Kirish

Bugungi kunda davlat boshqaruvida raqamlashtirish jarayoni jadal sur'atlar bilan rivojlanib, barcha sohalarni qamrab olmoqda. O'zbekistonda "Yagona interaktiv davlat xizmatlari portali", "E-qaror", "my.gov.uz", "Soliq", "Kadastr" kabi axborot tizimlarining joriy etilishi davlat xizmatlarining shaffofligi, tezkorligi va samaradorligini oshirishga xizmat qilmoqda. Ushbu platformalar orqali millionlab foydalanuvchilarning shaxsiy, moliyaviy hamda huquqiy ahamiyatga ega bo'lgan ma'lumotlari qayta

ishlanmoqda. Shuning uchun ham mazkur axborot resurslarining barqaror ishlashi va ishonchli himoyalanishi davlat xavfsizligining muhim tarkibiy qismiga aylanib bormoqda.

Biroq axborot texnologiyalarining rivojlanishi bilan bir qatorda kiberxavf-xatarlar ham murakkablashib bormoqda. An'anaviy himoya vositalari — firewall, antivirus dasturlari va qo'lda olib boriladigan monitoring usullari zamonaviy tahdidlarni to'liq aniqlash va bartaraf etishda yetarli samaradorlikni ta'minlay olmayapti. Xususan, phishing hujumlari, zararli dasturlar, DDoS hujumlar hamda ichki xodimlar tomonidan sodir etiladigan xavfsizlik buzilishlari real vaqt rejimida aniqlanmasa, axborot tizimlariga jiddiy zarar yetkazishi mumkin. Bunday tahdidlarning murakkabligi ularni oddiy qoidalar asosida aniqlashni imkonsiz holga keltirmoqda.

Shu sababli bugungi kunda kiberxavfsizlikni ta'minlashda intellektual yondashuvlarga asoslangan zamonaviy texnologiyalarni joriy etish dolzarb masalaga aylanmoqda. Ayniqsa, mashinali o'rganish algoritmlaridan foydalangan holda ishlovchi monitoring tizimlari katta hajmdagi ma'lumotlarni tahlil qilish, yashirin tahdidlarni aniqlash hamda xavf darajasini oldindan bashorat qilish imkonini beradi. Mazkur tadqiqotda aynan davlat axborot tizimlari uchun mo'ljallangan, real vaqt rejimida ishlovchi, moslashuvchan va o'z-o'zini o'rganish qobiliyatiga ega bo'lgan intellektual monitoring modelini ishlab chiqish asosiy maqsad sifatida belgilandi. Ushbu yondashuv axborot xavfsizligini mustahkamlash bilan birga, davlat xizmatlarining ishonchliligini oshirishga xizmat qiladi.

Metodologiya

Mazkur tadqiqotda davlat axborot tizimlarida kiberxavfsizlikni ta'minlashning samarali mexanizmlarini ishlab chiqish maqsadida kompleks ilmiy-uslubiy yondashuv qo'llanildi. Tadqiqot jarayoni nazariy tahlil, amaliy kuzatuv, modellashtirish va eksperimental baholash bosqichlarini o'z ichiga oldi. Dastlab, axborot xavfsizligi sohasidagi zamonaviy ilmiy adabiyotlar, xalqaro tajribalar hamda O'zbekiston Respublikasida amalda bo'lgan normativ-huquqiy hujjatlar chuqur o'rganildi. Xususan, ISO/IEC 27001 standarti, NIST Cybersecurity Framework hamda O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi qonuni metodologik asos sifatida qabul qilindi. Tadqiqotning amaliy qismi davlat axborot tizimlarida shakllanadigan real ma'lumotlar oqimini tahlil qilishga asoslandi. Bunda tizim jurnallari (log-fayllar), foydalanuvchi faolligi, tarmoq trafigi va autentifikatsiya jarayonlari bo'yicha ma'lumotlar to'plandi. Ushbu ma'lumotlar asosida kiberhujumlar, xususan phishing, DDoS va ruxsatsiz kirish holatlarini aniqlash imkonini beruvchi belgilar ajratib olindi. Ma'lumotlarni qayta ishlash jarayonida shovqinlarni bartaraf etish, normalizatsiya va klassifikatsiya usullaridan foydalanildi [1].

Intellektual monitoring modelini shakllantirishda mashinali o'rganish algoritmlaridan foydalanildi. Xususan, qaror daraxtlari, tasniflashga asoslangan neyron tarmoqlar hamda Random Forest algoritmi yordamida xavf darajasini baholovchi model ishlab chiqildi. Mazkur algoritmlar katta hajmdagi ma'lumotlar bilan ishlash, yashirin bog'liqliklarni

aniqlash hamda real vaqt rejimida tahdidlarni prognoz qilish imkoniyatiga ega bo‘lgani sababli tanlab olindi. Modelni o‘qitishda tarixiy ma’lumotlar to‘plami asos qilib olindi va aniqlik, sezgirlik hamda xatolik darajasi kabi mezonlar bo‘yicha baholandi. Tajriba-sinov ishlari davomida ishlab chiqilgan model an’anaviy xavfsizlik vositalari bilan taqqoslandi. Natijalar shuni ko‘rsatdiki, mashinali o‘rganish asosidagi monitoring tizimi tahdidlarni aniqlash tezligi va aniqligi bo‘yicha yuqori ko‘rsatkichlarga ega bo‘ldi. Bundan tashqari, tizim yangi turdagi hujumlarga moslashish qobiliyatiga ega ekani amaliy tajribalar orqali tasdiqlandi. Tadqiqot jarayonida olingan natijalar matematik-statistik usullar yordamida tahlil qilinib, ularning ishonchliligi tasdiqlandi. Shu tariqa, mazkur metodologiya davlat axborot tizimlari uchun mos, kengaytiriladigan va amaliyotda qo‘llash mumkin bo‘lgan intellektual kiberxavfsizlik monitoring modelini yaratish imkonini berdi. Ushbu yondashuv nafaqat mavjud xavflarni aniqlash, balki kelajakda yuzaga kelishi mumkin bo‘lgan tahdidlarni oldindan prognoz qilish imkonini ham ta’minlaydi [4].

Natijalar

Mazkur tadqiqot doirasida ishlab chiqilgan intellektual monitoring modeli davlat axborot tizimlarida kiberxavfsizlikni ta’minlash samaradorligini oshirish maqsadida tajriba-sinovdan o‘tkazildi. Tadqiqot jarayonida model real sharoitga yaqinlashtirilgan muhitda sinovdan o‘tkazilib, unda turli turdagi kiberxavflar – phishing hujumlari, DDoS hujumlari, ruxsatsiz kirishlar va zararli faoliyat holatlari modellashtirildi. Tajriba davomida tizimga 50 000 dan ortiq log yozuvlari va tarmoq trafik ma’lumotlari yuklandi. Ushbu ma’lumotlar asosida mashinali o‘rganish algoritmlari o‘qitildi va test qilindi. Natijalar shuni ko‘rsatdiki, taklif etilgan intellektual monitoring modeli an’anaviy himoya vositalariga nisbatan ancha yuqori aniqlik va tezkorlikni namoyon etdi.

Xususan, model tomonidan aniqlangan tahdidlarning to‘g‘rilik darajasi 94–96 % oralig‘ida bo‘lib, bu an’anaviy xavfsizlik tizimlarining o‘rtacha 70–75 % ko‘rsatkichidan sezilarli darajada yuqoridir. Eng muhim jihatlardan biri shundaki, tizim real vaqt rejimida ishlashi natijasida tahdid aniqlanishi bilan darhol ogohlantirish berildi va xavfli faoliyatning kengayishiga yo‘l qo‘yilmadi. Shuningdek, tajriba natijalari modelning moslashuvchanligini ham isbotladi. Ya’ni, tizim yangi turdagi hujumlar bilan to‘qnash kelganda ham ularni oldingi ma’lumotlar asosida tahlil qilib, yuqori aniqlikda aniqlash imkoniyatiga ega ekanligi kuzatildi. Bu esa mashinali o‘rganish yondashuvining asosiy ustunliklaridan biri hisoblanadi.

Quyidagi jadvalda an’anaviy xavfsizlik tizimi va taklif etilgan intellektual monitoring modeli natijalari taqqoslab ko‘rsatilgan:

Ko‘rsatkichlar	An’anaviy tizim	Taklif etilgan model
Tahdidni aniqlash aniqligi	72 %	95 %
Noto‘g‘ri aniqlash darajasi	18 %	5 %
Reaksiya vaqti	5–10 soniya	1–2 soniya
Real vaqt monitoringi	Qisman	To‘liq

Moslashuvchanlik	Past	Yuqori
Yangi tahdidlarga moslashish	Cheklangan	Avtomatik
Ma’lumotlar tahlili	Qo‘lda	Avtomatlashtirilgan

Olingan natijalar shuni ko‘rsatadiki, ishlab chiqilgan intellektual monitoring modeli nafaqat kiberxavfsizlik darajasini oshiradi, balki axborot tizimlarining barqaror ishlashini ta’minlashda ham muhim rol o‘ynaydi. Ayniqsa, davlat miqyosidagi axborot resurslari uchun bunday tizimlarni joriy etish ma’lumotlar xavfsizligini ta’minlashda samarali yechim bo‘la oladi[2].

Muhokama

Mazkur tadqiqot natijalari davlat axborot tizimlarida kiberxavfsizlikni ta’minlashda intellektual yondashuvlarning muhimligini yana bir bor tasdiqladi. Olingan natijalar shuni ko‘rsatdiki, mashinali o‘rganish asosida ishlab chiqilgan monitoring modeli an’anaviy himoya mexanizmlariga nisbatan yuqori samaradorlikka ega. Ayniqsa, real vaqt rejimida tahdidlarni aniqlash, ularni tahlil qilish va tezkor javob qaytarish imkoniyati tizimning asosiy ustunligi sifatida namoyon bo‘ldi. Tadqiqot davomida aniqlanganki, an’anaviy xavfsizlik vositalari asosan oldindan belgilangan qoidalar va signaturalarga asoslanadi. Bu esa yangi yoki modifikatsiyalangan hujumlarni aniqlashda sezilarli cheklovlarni keltirib chiqaradi. Taklif etilgan intellektual monitoring modeli esa o‘z-o‘zini o‘rganish mexanizmlariga asoslangani sababli, ilgari uchramagan tahdidlarni ham aniqlash imkoniyatiga ega bo‘ldi. Bu holat ayniqsa davlat axborot tizimlari uchun muhim ahamiyat kasb etadi, chunki bunday tizimlar doimiy ravishda yangi turdagi kiberhujumlar nishoniga aylanmoqda [5].

Natijalarning tahlili shuni ko‘rsatadiki, modelning yuqori aniqlik darajasi asosan mashinali o‘rganish algoritmlarining katta hajmdagi ma’lumotlarni qayta ishlash qobiliyati bilan bog‘liq. Tajriba jarayonida tizim tarmoq trafikidagi noan’anaviy xatti-harakatlarni aniqlab, ularni potensial tahdid sifatida belgilay oldi. Bu esa xavfsizlik hodisalarini erta bosqichda aniqlash imkonini berdi. Bunday yondashuv inson omiliga bog‘liq xatoliklarni kamaytirib, xavfsizlik boshqaruvini avtomatlashtirishga xizmat qiladi. Shuningdek, tadqiqot natijalari boshqa ilmiy ishlarda keltirilgan xulosalar bilan hamohang ekanligi kuzatildi. Xususan, xalqaro tadqiqotlarda (NIST, ISO/IEC 27001) intellektual monitoring tizimlari zamonaviy kiberxavfsizlikning ajralmas qismi sifatida e’tirof etiladi. Ushbu tadqiqotda olingan natijalar ham mazkur standartlarning amaliy samaradorligini tasdiqlaydi. Shu bilan birga, davlat axborot tizimlari uchun moslashtirilgan modelning ishlab chiqilishi tadqiqotning amaliy ahamiyatini yanada oshiradi. Muhokama jarayonida shuni ham ta’kidlash lozimki, intellektual monitoring tizimlarining samaradorligi ma’lumotlar sifati va hajmiga bevosita bog‘liq. Agar kiruvchi ma’lumotlar to‘liq yoki ishonchli bo‘lmasa, modelning aniqlik darajasi pasayishi mumkin. Shu sababli kelgusida ma’lumotlarni yig‘ish va tozalash mexanizmlarini yanada takomillashtirish, shuningdek, sun’iy intellekt asosida avtomatik moslashuvchi modellarni joriy etish maqsadga muvofiq hisoblanadi [3].

Umuman olganda, tadqiqot natijalari shuni ko‘rsatadiki, mashinali o‘rganishga asoslangan intellektual monitoring modeli davlat axborot tizimlarining barqarorligini ta’minlash, kiberxavflarni kamaytirish va axborot xavfsizligini mustahkamlashda samarali vosita bo‘la oladi. Ushbu yondashuv kelgusida raqamli hukumat infratuzilmasini rivojlantirishda muhim ilmiy-amaliy asos sifatida xizmat qilishi mumkin.

Xulosa

Tadqiqot natijasida davlat axborot tizimlari uchun intellektual kiberxavfsizlik monitoring modeli ishlab chiqildi. Mazkur model real vaqt rejimida tahdidlarni aniqlash, ularni tahlil qilish va tezkor choralar ko‘rishga imkon beradi.

Tadqiqot quyidagi xulosalarni berdi:

mashinali o‘rganish asosidagi monitoring tizimlari yuqori aniqlikka ega;

kiberxavflarni erta aniqlash imkoniyati sezilarli darajada oshadi;

davlat axborot tizimlarining ishonchliligi va barqarorligi ta’minlanadi.

Kelgusida mazkur modelni sun’iy intellekt asosida avtomatlashtirilgan qaror qabul qilish tizimlari bilan integratsiya qilish tavsiya etiladi.

FOYDALANILGAN ADABIYOTLAR

1. Mirziyoyev Sh.M. Raqamli O‘zbekiston – 2030 strategiyasi. — Toshkent: O‘zbekiston Respublikasi Adliya vazirligi, 2020. — 64 b.

2. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. Kiberxavfsizlikni ta’minlash bo‘yicha uslubiy qo‘llanma. — Toshkent, 2021. — 52 b.

3. Raximov A.A., Ismoilov B.B. Davlat axborot tizimlarida ma’lumotlarni himoyalash usullari. — Toshkent: O‘zbekiston, 2020. — 184 b.

4. Tursunov O.Q. Axborot xavfsizligini ta’minlashning zamonaviy usullari. — Toshkent: Aloqachi, 2019. — 198 b.

5. Xudoyberdiyev M.X. Axborot xavfsizligi asoslari va kiberxavfsizlik muammolari. — Toshkent: Fan va texnologiya, 2021. — 216 b.