SUN’IY INTELLEKT TEXNOLOGIYALARINING KIBERXAVFSIZLIKNI TA’MINLASHDAGI AHAMIYATI

Isxakova Nargiza
TDIU “Raqamli iqtisodiyot va axborot texnologiyalari” fakulteti
“Axborot tizimlari va texnologiyalari” kafedrasi PhD, Dotsent
Sabirova Sevara
Toshkent davlat iqtisodiyot universiteti
Magistratura fakulteti 2-bosqich magistranti

THE IMPORTANCE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN ENSURING CYBERSECURITY

Isxakova Nargiza
Faculty of “Digital Economy and Information Technologies,” Tashkent State University of Economics
Department of “Information Systems and Technologies” PhD, Associate Professor
Sabirova Sevara
Tashkent State University of Economics
2nd-year Master’s student, Faculty of Master’s Studies

ЗНАЧЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ

Исхакова Наргиза
Факультет «Цифровая экономика и информационные технологии» ТГЭУ
Кафедра «Информационные системы и технологии», PhD, доцент
Сабирова Севара
Ташкентский государственный экономический университет

Магистрант 2-го курса, факультет магистратуры

Annotatsiya. Raqamli texnologiyalar jadal rivojlanib borayotgan hozirgi davrda kiberxavfsizlik masalasi davlatlar, tashkilotlar va foydalanuvchilar uchun eng muhim yo‘nalishlardan biriga aylandi. Internet tarmog‘ida ma’lumotlar almashinuvi kengaygani sari, firibgarlik, ma’lumot o‘g‘irlash va zararli dasturlar orqali amalga oshiriladigan hujumlar soni ham ortmoqda. Ushbu holatda sun’iy intellekt texnologiyalari kiberxavfsizlik tizimlarini takomillashtirishning eng samarali vositalaridan biri sifatida qaralmoqda. Sun’iy intellekt asosidagi tizimlar katta hajmdagi ma’lumotlarni qisqa vaqt ichida tahlil qilib, anomaliyalarni erta aniqlash va tahdidlarning oldini olish imkonini beradi. Mashinaviy o‘rganish, chuqur o‘rganish va tabiiy tilni qayta ishlash texnologiyalari yordamida xavfli faoliyatni avtomatik tarzda aniqlash, real vaqt monitoringi va foydalanuvchi xatti-harakatlarini tahlil qilish imkoniyatlari kengaymoqda. Maqolada sun’iy intellektning kiberxavfsizlikdagi o‘rni, amaliy qo‘llanilish yo‘nalishlari, shuningdek, ushbu texnologiyaning afzalliklari va ehtimoliy xavf jihatlari tahlil qilinadi. Tadqiqot natijalari AI texnologiyalarini kiberxavfsizlik sohasiga keng joriy etish zarurligini, bu esa ma’lumotlarni himoya qilish samaradorligini oshirishda muhim ahamiyat kasb etishini ko‘rsatadi.

Kalit so‘zlar: sun’iy intellekt, kiberxavfsizlik, machine learning, deep learning, ma’lumotlarni himoya qilish, tahdidlarni aniqlash, intellektual tizimlar, raqamli xavfsizlik, tarmoq xavflari, avtomatlashtirilgan monitoring.

Abstract. In the modern era of rapid digital development, cybersecurity has become one of the most crucial areas for governments, organizations, and individual users. As data exchange on the Internet expands, the number of frauds, data thefts, and malicious software attacks continues to increase. In this context, artificial intelligence (AI) technologies are regarded as one of the most effective tools for enhancing cybersecurity systems. AI-based systems can analyze large volumes of data in a short time, detect anomalies early, and prevent potential threats. Through machine learning, deep learning, and natural language processing technologies, it becomes possible to automatically identify harmful activities, conduct real-time monitoring, and analyze user behavior patterns.This article examines the role of artificial intelligence in cybersecurity, its practical

applications, as well as its advantages and possible risks. The research highlights the necessity of integrating AI technologies into cybersecurity systems to enhance the effectiveness of data protection and threat detection.

Keywords: artificial intelligence, cybersecurity, machine learning, deep learning, data protection, threat detection, intelligent systems, digital security, network threats, automated monitoring.

Аннотация. В современную эпоху стремительного развития цифровых технологий кибербезопасность становится одной из ключевых сфер для государств, организаций и пользователей. С ростом объёма обмена данными в сети Интернет увеличивается количество мошеннических действий, краж данных и атак с использованием вредоносных программ. В этих условиях технологии искусственного интеллекта рассматриваются как одно из наиболее эффективных средств совершенствования систем кибербезопасности. Системы на основе искусственного интеллекта способны анализировать большие объёмы данных за короткое время, своевременно выявлять аномалии и предотвращать потенциальные угрозы. Благодаря методам машинного обучения, глубокого обучения и обработки естественного языка становится возможным автоматическое выявление вредоносной активности, мониторинг в режиме реального времени и анализ поведения пользователей.В статье рассматривается роль искусственного интеллекта в обеспечении кибербезопасности, направления его практического применения, а также преимущества и потенциальные риски использования этих технологий. Результаты исследования показывают, что интеграция искусственного интеллекта в системы кибербезопасности способствует повышению эффективности защиты данных и своевременному выявлению угроз.

Ключевые слова: искусственный интеллект, кибербезопасность, машинное обучение, глубокое обучение, защита данных, обнаружение угроз, интеллектуальные системы, цифровая безопасность, сетевые угрозы, автоматизированный мониторинг.

Kirish. Zamonaviy jamiyatda raqamli transformatsiya jarayoni tobora chuqurlashib borar ekan, axborot texnologiyalariga asoslangan tizimlar inson faoliyatining deyarli barcha sohalariga kirib bormoqda. Biroq raqamli infratuzilmaning kengayishi bilan birga, kiberxavfsizlik tahdidlari ham ortib bormoqda. Xakerlik hujumlari, ma'lumotlar bazalariga noqonuniy kirish, zararli dasturlar orqali amalga oshiriladigan tahdidlar jahon miqyosida dolzarb muammo sifatida e'tirof etilmoqda. O'zbekistonda axborot-kommunikatsiya texnologiyalari tez sur'atlar bilan rivojlanib bormoqda, shuningdek davlat va biznes sohalarida raqamlashtirish jarayoni kengaymoqda. Biroq, shu bilan birga, kiberxavfsizlik sohasida bir qator muammolar mavjud. Birinchi navbatda, davlat va korxonalarda axborot tizimlarini himoya qilish bo'yicha yetarlicha malakali mutaxassislar yetishmaydi. Ikkinchidan, ko'plab tashkilotlar zamonaviy kiberxavfsizlik texnologiyalarini joriy etishda moliyaviy va texnik imkoniyatlarning cheklanganligi bilan duch keladi. Shuningdek, so'nggi yillarda kiberhujumlar soni oshgani, shaxsiy va moliyaviy ma'lumotlar xavfsizligining zaifligi, internet firibgarligi va elektron xizmatlar orqali sodir bo'layotgan hujumlar aholining axborot xavfsizligiga bo'lgan ishonchini susaytirmoqda. Shu sababli sun'iy intellekt texnologiyalarini qo'llash kiberxavfsizlikni oshirish, hujumlarni tez aniqlash va oldini olish hamda axborot tizimlarining barqarorligini ta'minlashda muhim ahamiyat kasb etadi. Mazkur muammolarni bartaraf etish maqsadida O'zbekiston Respublikasi Prezidentining 2024-yil 14-oktyabrdagi PQ-358-sonli " Sun'iy intelekt texnologiyalarini 2030- yilga qadar rivojlantirish" strategiyasini tasdiqlash tog'risidagi farmoni [3] qabul qilinganligini e'tirof etish mumkin. AI tizimlari real vaqt rejimida katta hajmdagi ma'lumotlarni tahlil qilib, anomaliyalarni avtomatik tarzda aniqlash, xatti-harakatlardagi g'ayrioddiylikni kuzatish va potentsial xavflarning oldini olishga yordam beradi. Sun'iy intellektning mashinaviy o'rganish, chuqur o'rganish va bashoratli tahlil kabi texnologiyalari orqali kiberxavfsizlik tizimlari yanada intellektual tus olmoqda. IBM Security hisobotlariga ko'ra, AI asosidagi himoya tizimlari an'anaviy usullarga nisbatan tahdidlarni aniqlash tezligini va samaradorligini sezilarli darajada oshirgan [1]. Shu bilan birga, NIST tomonidan ishlab chiqilgan "AI Cybersecurity Framework" konsepsiyasi bu yo'nalishda yagona metodologiyani shakllantirishga xizmat qilmoqda [2].

Adabiyotlar tahlili. So‘nggi yillarda kiberxavfsizlik tizimlarini mustahkamlashda sun’iy intellekt (AI) texnologiyalarining qo‘llanilishi keng miqyosda o‘rganilmoqda. Jahon miqyosidagi tadqiqotlar shuni ko‘rsatadiki, sun’iy intellekt xavfsizlik tizimlarida an’anaviy himoya usullarini to‘ldiruvchi emas, balki ularni yangi bosqichga olib chiqadigan asosiy omilga aylanmoqda. IBM Security (2023) tomonidan chop etilgan *“Cost of a Data Breach Report”* ma’lumotlariga ko‘ra, kiberhujumlar natijasida tashkilotlarga yetayotgan zarar hajmi yil sayin ortib bormoqda. Hisobotda ta’kidlanishicha, sun’iy intellekt asosidagi aniqlash va javob berish tizimlari kiberxavfga qarshi kurashish vaqtini sezilarli darajada qisqartiradi, bu esa iqtisodiy yo‘qotishlarni kamaytirishga xizmat qiladi [1]. NIST (2023) tomonidan ishlab chiqilgan *Artificial Intelligence Risk Management Framework* esa sun’iy intellekt tizimlarini kiberxavfsizlik jarayonlariga integratsiya qilishda xavf va mas’uliyatlarni boshqarish bo‘yicha muhim metodologiyani taqdim etadi. Ushbu hujjatda AI tizimlarining ishonchliligi, shaffofligi va barqarorligini ta’minlash asosiy tamoyil sifatida belgilangan [2].O‘zbekiston Respublikasi Prezidentining PQ–358-sonli qarori (2024) esa mamlakat miqyosida sun’iy intellektni 2030-yilgacha rivojlantirish strategiyasini belgilab berdi. Ushbu hujjat sun’iy intellektni kiberxavfsizlikni mustahkamlash, davlat boshqaruvi va iqtisodiyotning raqamli transformatsiyasiga joriy etish zarurligini alohida ta’kidlaydi [3]. Springer (2019) nashr etgan *“Artificial Intelligence: Foundations, Theory, and Algorithms”* asarida sun’iy intellektning nazariy asoslari, mashinaviy o‘rganish, neyron tarmoqlar va ularning kiberxavfsizlikdagi qo‘llanilishi batafsil yoritilgan. Bu manba kiberxavfsizlikdagi AI modellarining texnik jihatlarini tushunishda asosiy nazariy poydevor bo‘lib xizmat qiladi [4].Shuningdek, *“Advancing Cybersecurity: A Comprehensive Review of AI-Driven Approaches”* (Journal of Big Data, 2024) maqolasida sun’iy intellekt yordamida tahdidlarni oldindan aniqlash, xatti-harakatlarni tahlil qilish va avtomatik himoya mexanizmlarini yaratish imkoniyatlari keng tahlil qilingan. Mualliflar AI asosidagi yechimlar inson omilidan kelib chiqadigan xatoliklarni kamaytirishda samarali ekanini ta’kidlashgan [5].Oxirgi manba sifatida **GeeksforGeeks** platformasida joylashtirilgan *AI in Cybersecurity* maqolasi amaliy jihatdan dolzarb bo‘lib, unda sun’iy intellekt yordamida kiberxavf monitoringi, spam va fishingni aniqlash algoritmlari misollar orqali tushuntirilgan. Ushbu maqola mavzuning texnik amaliy tomonlarini o‘rganishda foydali bo‘ladi [6].Umuman olganda, tahlil qilingan adabiyotlar shuni ko‘rsatadiki, sun’iy intellekt texnologiyalari kiberxavfsizlik

tizimlarida tahdidlarni aniqlash, javob berish tezligini oshirish va inson omilini kamaytirish orqali samaradorlikni oshiradi. Shu sababli, bu yo‘nalishda ilmiy izlanishlar nafaqat texnik, balki strategik ahamiyat kasb etmoqda.

Tadqiqot metodologiyasi. Ushbu maqolada tahlil, sintez, nazariy umumlashtirish, induksiya, deduksiya va boshqa usullardan foydalanilgan. Asosiy manba sifatida sun’iy intelekt va kiberxavfsizlik bo‘yicha mavjud ilmiy adabiyotlar o‘rganildi. Shuningdek, raqamli texnologiyalar joriy etilishidan oldin va keyingi davrdagi ko‘rsatgichlar solishtirildi.

Tahlil va natijalar muhokamasi. Sun’iy intellekt (SI) — bu kompyuter tizimlariga inson aqlini taqlid qilish imkonini beruvchi texnologiyalarning majmuasidir. SI texnologiyalarining nazariy asoslari quyidagi asosiy yo‘nalishlarni o‘z ichiga oladi: Machine Learning — bu kompyuterlarga ma’lumotlar asosida o‘rganish va qarorlar qabul qilish imkonini beruvchi algoritmlar va modellarning rivojlanishini o‘rganadigan soha. Bu soha, ma’lumotlar asosida o‘rganish va qarorlar qabul qilish imkonini beruvchi algoritmlar va modellarning rivojlanishini o‘rganadi. Deep Learning — bu ko‘p qatlamli neyron tarmoqlarini qo‘llab-quvvatlaydigan va murakkab ma’lumotlarni tahlil qilish imkonini beruvchi metodlarni o‘z ichiga oladi. Bu metodlar, katta hajmdagi ma’lumotlar asosida murakkab neyron tarmoqlarini yaratish va o‘rgatish imkonini beradi. Natural Language Processing — bu inson tilini tushunish va ishlab chiqish uchun zarur bo‘lgan metodlar va texnologiyalarni o‘rganadi. Bu soha, kompyuterlarga inson tilini tushunish va ishlab chiqish imkonini beruvchi metodlar va texnologiyalarni rivojlantirishga qaratilgan. Algoritmlar va modellar - SI tizimlarining ishlashini ta’minlovchi asosiy komponentlar bo‘lib, ular ma’lumotlarni qayta ishlash va qarorlar qabul qilish jarayonlarini amalga oshiradi. Algoritmlar va modellar, SI tizimlarining samarali ishlashini ta’minlash uchun zarur bo‘lgan asosiy komponentlardir. Statistik nazariya va matematik asoslar - SI tizimlarining samarali ishlashini ta’minlash uchun zarur bo‘lgan statistik va matematik metodlarni o‘z ichiga oladi. Bu metodlar, SI tizimlarining samarali ishlashini ta’minlash uchun zarur bo‘lgan asosiy komponentlardir[4].

Kompyuter tarmoqlarining rivojlanishi jamiyatlarning faoliyatini tubdan o‘zgartirdi va natijada kiberhujumlar chastotasi va murakkabligi oshdi. Kiberhujumlar — bu kompyuter tizimlari, tarmoqlar yoki ma’lumotlarga qaratilgan buzuvchi faoliyatlar bo‘lib, odatda ular rejalashtirilgan va uyushgan bo‘lib, maqsadlariga erishish uchun bir qator sinxronlashtirilgan qadamlarni o‘z ichiga oladi. Ushbu hujumlar zarar yetkazish, ruxsatsiz kirish yoki xizmatlarning to‘xtatilishiga olib keladigan faoliyatlarni maqsad qilgan bo‘lib, natijada jiddiy ma’lumot yo‘qotilishi yoki moliyaviy zarar yuzaga keladi va ko‘pincha uzoq muddatli oqibatlarga olib keladi. Shuningdek, ichki tahdidlar — bu kiberhujumlarning sezilarli va ortib borayotgan segmentini tashkil etuvchi holatlar bo‘lib, odatda norozilik bildirgan yoki qonuniy vakolatini suiiste’mol qilgan xodimlar tomonidan amalga oshiriladi; ular ma’lumotlarni o‘g‘irlash yoki zarar yetkazish maqsadida mavjud ruxsatlardan foydalanadi. Bu tahdidlar shuningdek foydalanuvchilar tasodifan qurilmalariga o‘rnatgan, ruxsatsiz kirish huquqiga ega ilovalardan ham paydo bo‘lishi mumkin, bu ilovalar esa sezgir ma’lumotlarga kirish va ularni noto‘g‘ri foydalanish imkonini beradi. Ushbu tahdidlarni bartaraf etish maqsadida ilg‘or xulq-atvor anomaliyasini aniqlash va avtomatik chidamlilik mexanizmlari ishlab chiqilmoqda, ular xodimlar va ilovalar darajasida zararli harakatlarni oldindan aniqlash va yumshatishga qaratilgan. Kiberhujumlarning keng spektri mavjud bo‘lib, ular raqamli dunyodagi turli tahdidlarni ifodalaydi. Adabiyotlarda ta’kidlangan va 1-jadvalda umumlashtirilgan ushbu hujumlarning bir nechta muhim turlari haqida ma’lumotlar berilgan. Ushbu ma’lumotlar kiber tahdidlarning murakkabligi va keng doirasini ko‘rsatib, bugungi kunda tashkilotlar va shaxslar duch kelishi mumkin bo‘lgan ko‘plab hujumlarni yoritadi. Botnetlar — yana bir muhim kiber tahdid bo‘lib, bu tarmoqqa ulanishgan kompyuterlarning hujumchi tomonidan boshqariladigan va DDoS hujumlari, ma’lumot o‘g‘irligi va spam kabi uyushgan zararli faoliyatlarni amalga oshirish uchun ishlatiladigan tarmoqlardir. Bu tarmoqlar juda keng bo‘lishi mumkin, minglab yoki hatto millionlab zaiflashtirilgan qurilmalarni o‘z ichiga oladi, bu esa ularni yo‘q qilishni nihoyatda qiyinlashtiradi. Botnet operatorlari qurilmalarni infektsiya qilish va nazoratni saqlash uchun ilg‘or usullarni qo‘llaydi va doimiy ravishda aniqlanishdan qochish maqsadida texnikalarini rivojlantirib boradi[5].

Kiber – hujum turlari

1- jadval[5].

Kiberhujum turlari	Tavsifi
Phishing	- ushbu hujum turida shaxslar aldab, ulardan login ma’lumotlari yoki moliyaviy ma’lumotlarni olishga harakat qilinadi. Huquqbuzarlar ishonchli elektron xabar sifatida o‘zlarini ko‘rsatib, shaxsiy yoki korporativ ma’lumotlarga ruxsatsiz kirish olishadi.
Malware	- bu viruslar, virmlar (worm), trojanlar va ransomware kabi zararli dasturlarni o‘z ichiga oladi. U kompyuter tizimlariga va ma’lumotlarga zarar yetkazish yoki ruxsatsiz kirish uchun mo‘ljallangan. Malware turli xil kiberhujumlarda qo‘llaniladi.
DDoS	- Denial of Service (DoS) yoki Distributed Denial of Service (DDoS) hujumlari tizim resurslarini to‘ldirib, uni haqiqiy so‘rovlarni qabul qilmasligiga olib keladi. DDoS hujumlari ko‘plab buzilgan kompyuter tizimlaridan bir vaqtning o‘zida hujum jo‘natish orqali amalga oshiriladi.
MitM	- Man-in-the-Middle hujumida ikki tomon o‘rtasidagi aloqa bilmasdan ushlanadi. Huquqbuzarlar xabarlarni o‘g‘irlashi, o‘zgartirishi yoki soxta xabarlar yaratishi mumkin, bu esa ma’lumotlar buzilishi yoki yashirin kuzatishga olib keladi.
SQL inyeksiya hujumi	- bu hujum texnikasi ma’lumotlar bazasi bilan ishlovchi veb-saytlardagi zaifliklardan foydalanadi, zararli SQL buyruqlarini so‘rovga kiritadi. Ama’lumotlarni shifrlab, ular qayta ishlatilmay qolishini ta’minlaydi. Huquqbuzar ma’lumotni ochish uchun pul talab qiladi. Bu shaxslar va tashkilotlar uchun moliyaviy xavfni yuzaga keltiradi. gar hujum muvaffaqiyatli bo‘lsa, huquqbuzar ma’lumotlarni o‘qishi, o‘zgartirishi yoki o‘chirishi mumkin.
Zero-Day Exploit	- Bu hujum, dasturiy ta’minot ishlab chiqaruvchisi zaiflikni aniqlashidan oldin yoki birinchi kunida amalga oshiriladi. Zero-Day hujumlar tezda aniqlanmagan zaifliklardan foydalanganligi sababli, ularni himoya qilish juda qiyin.
Ransomware	- Ransomware ma’lumotlarni shifrlab, ular qayta ishlatilmay qolishini ta’minlaydi. Huquqbuzar ma’lumotni ochish uchun pul talab qiladi. Bu shaxslar va tashkilotlar uchun moliyaviy xavfni yuzaga keltiradi.
XSS	- hujumlari uchinchi tomon veb-resurslarini ishlatib, qurbonning brauzerida yoki skript ishlay oladigan dasturda zararli skriptlarni bajaradi.hujumida shaxs yoki guruh tarmoqka ruxsatsiz kirib, uzoq vaqt davomida sezilmay qoladi.
APT	- Bu orqali ular muhim ma’lumotlarni o‘g‘irlashi mumkin, va tashkilot xavfsizlik xodimlari bu holatni tezda aniqlay olmaydi.
BEC	- hujumlarida moliyaviy vakolatga ega xodimlar maqsad qilinadi. Huquqbuzarlar puxta tadqiqot olib, xodimni pulni o‘z hisob raqamlariga yuborishga aldashadi.
Crypto-jacking	- hujumida qurbonning hisoblash resurslari yashirin tarzda kriptovalyuta qazib olish uchun ishlatiladi. Bu tashkilot tarmoqlarining resurslarini sezilmay kamaytiradi.
Password Attack	- parol hujumlari foydalanuvchi parollarini buzishga qaratilgan bo‘lib, Brute-Force, Dictionary, Rainbow Table, Credential Stuffing, Password Spraying, Keylogger va phishing kabi usullarni o‘z ichiga oladi..
Insider Threat	- ichki tahdidlar tashkilot xodimlaridan kelib chiqadi, ular ruxsatli kirish huquqlarini suiiste’mol qilib, tizim va ma’lumotlarga zarar yetkazadi.botnet hujumida buzilgan kompyuterlar tarmog‘i masofadan boshqariladi va muvofiqlashtirilgan zararli faoliyatlar amalga oshiriladi.
Botnet Attack	- botnet hujumida buzilgan kompyuterlar tarmog‘i masofadan boshqariladi va muvofiqlashtirilgan zararli faoliyatlar amalga oshiriladi.

Sun’iy intellekt (AI) texnologiyalari kiberxavfsizlik sohasida tahdidlarni aniqlash, hodisalarga tezkor javob berish hamda xavfsizlik jarayonlarini avtomatlashtirishda muhim ahamiyat kasb etadi. U katta hajmdagi ma’lumotlarni real vaqt rejimida tahlil qilish orqali kiberhujumlar, zararli dasturlar (malware), fishing va ransomware kabi tahdidlarni an’anaviy usullarga qaraganda tezroq aniqlash imkonini beradi. AI qo‘llanilgan kiberxavfsizlik tizimlarining asosiy ustunliklari — tahdidlar haqidagi ma’lumotlarni avtomatik tahlil qilish, foydalanuvchi xatti-harakatlarini kuzatish, xavf darajasini baholash, tizimga noqonuniy kirish holatlarini aniqlash va faol tahdidlarni qidirishdir. Ushbu yondashuvlar kiberhujumlarning zararini kamaytirish va ularning oldini olishda samarali natija beradi. Bugungi kunda AI texnologiyalari xavfsizlik devorlari (firewall), yakuniy nuqta himoyasi (endpoint security), xavfsizlik hodisalarini boshqarish tizimlari (SIEM), kengaytirilgan aniqlash va javob tizimlari (XDR), shuningdek firibgarlikni aniqlash dasturlarida keng qo‘llanilmoqda. Bu tizimlar tarmoq, bulutli muhit va ma’lumotlar xavfsizligini yanada mustahkamlaydi.Kiberxavfsizlik tahdidlari shaklan va usul jihatidan murakkablashib borayotgan bir paytda, AI asosidagi himoya tizimlari real vaqtli monitoring, tezkor javob va hujumlarning oldini olish imkoniyatini yaratadi. Shu sababdan tashkilotlar o‘z kiberhimoya strategiyalarini yanada kuchaytirishlari zarur[6].

Sun’iy intellekt (AI) texnologiyalarining kiberxavfsizlikdagi o‘rni zamonaviy axborot tizimlarini himoya qilishda muhim ahamiyatga ega. U inson tomonidan boshqariladigan an’anaviy usullardan farqli o‘laroq, tahdidlarni aniqlash, tahlil qilish va ularga javob berish jarayonlarini o‘zlashtirib, ularni avtomatlashtirish imkonini beradi. AI tizimlari kiberhujumlarning murakkablashib borayotgan sharoitida xavfsizlikni ta’minlashning ishonchli mexanizmlaridan biri hisoblanadi. Quyida sun’iy intellektning bu boradagi asosiy jihatlari keltiriladi:

1. Tahdidlarni aniqlash (Detection).
Sun’iy intellekt tizimlari katta hajmdagi ma’lumotlarni real vaqt rejimida tahlil qilish orqali odatiy holatlardan chetga chiqadigan harakatlarni tezda aniqlaydi. Masalan, tizimga bir necha bor muvaffaqiyatsiz kirish urinishlari yoki shubhali fayl yuklash holatlari aniqlansa, AI ularni potentsial tahdid sifatida qayd etadi.

2. Bashorat qilish (Prediction).
AI ilgari sodir bo‘lgan hujumlar, ularning sabablari va oqibatlarini o‘rganib, kelajakdagi xavf-xatarlarni oldindan prognozlash imkoniyatiga ega. Shu tarzda u kiberhujumlar sodir bo‘lishidan avval ularni bashorat qiladi va tizimni tayyor holatga keltiradi.

3. Moslashuvchanlik(Adaptation). Sun’iy intellekt o‘z faoliyatida doimiy o‘rganish tamoyiliga asoslanadi. Har bir yangi tahdid yoki hujum holatidan keyin tizim ma’lum tajriba orttiradi va kelajakda shunga o‘xshash vaziyatlarda tezroq hamda samaraliroq choralar ko‘rishni o‘rganadi.

4. Avtomatlashtirish (Automation).
AI yordamida kiberxavfsizlik tizimlarida ko‘plab jarayonlar inson aralashuvisiz amalga oshiriladi. Masalan, zararli IP manzillarni bloklash, virus aniqlanganda uni karantin rejimiga o‘tkazish yoki ma’lum turdagi tahdidlar uchun standart javob choralarini ishga tushirish kabi amallar avtomatik bajariladi. Bu esa mutaxassislarning vaqtini tejab, ularni strategik muammolarga e’tibor qaratishga imkon beradi.

5. Javob berish (Response).
Sun’iy intellekt tahdid aniqlanganda darhol tizimni himoya holatiga o‘tkazadi yoki zarur ogohlantirishlarni yuboradi. Bu tezkor javob mexanizmi kiberhujumlarning ta’sir doirasini kamaytiradi va zarar yetkazish ehtimolini minimal darajaga tushiradi[6].

1-rasm. Kiberxavfsizlikda sun'iy intellektning 7 ta asosiy qo'llanilishi [6]

Xulosa. Zamonaviy raqamli davrda kiberxavfsizlikni ta'minlash masalasi milliy xavfsizlikning ajralmas tarkibiy qismiga aylanmoqda. Axborot oqimining keskin ortishi, kiberhujumlarning murakkablashuvi va ularning iqtisodiy hamda ijtimoiy oqibatlari sun'iy intellekt texnologiyalaridan samarali foydalanishni zaruratga aylantirdi.Tadqiqot natijalari shuni ko'rsatadiki, sun'iy intellekt asosidagi tizimlar kiberxavfsizlikda an'anaviy usullarga nisbatan tezroq aniqlash, bashorat qilish va avtomatik qaror qabul qilish imkonini beradi. Masalan, mashinaviy o'rganish algoritmlari tarmoqdagi noodatiy faoliyatni real vaqt rejimida aniqlab, xavf manbaini bartaraf etishda muhim rol o'ynaydi. Shuningdek, davlat siyosatida ham bu yo'nalish ustuvor ahamiyat kasb etmoqda. Jumladan, O'zbekiston Respublikasi Prezidentining 2024-yil 14-oktabrdagi PQ–358-son qarorida "Sun'iy

intellekt texnologiyalarini 2030-yilgacha rivojlantirish strategiyasi” tasdiqlanib, ushbu texnologiyalarni kiberxavfsizlik tizimlariga keng joriy etish zarurligi qayd etilgan. Xulosa o‘rnida aytish mumkinki, kiberxavfsizlikni mustahkamlashda sun’iy intellekt texnologiyalarini joriy etish — nafaqat himoya darajasini oshiradi, balki milliy raqamli infratuzilmaning barqaror rivojlanishiga ham xizmat qiladi. Shu bois, kelgusida bu yo‘nalishda ilmiy tadqiqotlar va amaliy loyihalar o‘rtasida uzviy integratsiyani kuchaytirish zarur.

Foydalanilgan adabiyotlar:

1. IBM Security (2023). *Cost of a Data Breach Report.* IBM Corporation.
2. National Institute of Standards and Technology (NIST). (2023). *Artificial Intelligence Risk Management Framework.*
3. PQ-358-сон 14.10.2024. Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida
4. "Artificial Intelligence: Foundations, Theory, and Algorithms", Springer, 2019.
5. “Advancing cybersecurity: a comprehensive review of AI-driven approaches” (Journal of Big Data, 2024)
6. AI in Cybersecurity - GeeksforGeeks

Used literature:

1. IBM Security (2023). *Cost of a Data Breach Report.* IBM Corporation.
2. National Institute of Standards and Technology (NIST). (2023). *Artificial Intelligence Risk Management Framework.*
3. PQ-358, 14.10.2024. On approving the Strategy for the Development of Artificial Intelligence Technologies until 2030.
4. "Artificial Intelligence: Foundations, Theory, and Algorithms", Springer, 2019.
5. “Advancing cybersecurity: a comprehensive review of AI-driven approaches” (Journal of Big Data, 2024)

6. AI in Cybersecurity - GeeksforGeeks

Использованная литература:

1. IBM Security (2023). *Cost of a Data Breach Report.* IBM Corporation.
2. National Institute of Standards and Technology (NIST). (2023). *Artificial Intelligence Risk Management Framework.*
3. Постановление ПҚ-358 от 14.10.2024. О утверждении Стратегии развития технологий искусственного интеллекта до 2030 года.
4. "Artificial Intelligence: Foundations, Theory, and Algorithms", Springer, 2019.
5. “Advancing cybersecurity: a comprehensive review of AI-driven approaches” (Journal of Big Data, 2024)
6. AI in Cybersecurity - GeeksforGeeks