

KIBERXAVFSIZLIKDA INSON OMILI VA SI INTEGRATSIYASI

O'zbekiston jurnalistikasi va ommaviy kommunikatsiyalar universitetining "Mediadizayn" kafedrası
o'qituvchisi

Qurbonov Xurshid Narzulla o'g'li

qurbonovkhurshid415@gmail.com

ANNOTATSIYA

Mazkur maqolada kiberxavfsizlik tizimlarida inson omilining roli va uning sun'iy intellekt (SI) texnologiyalari bilan integratsiyasi chuqur ilmiy tahlil qilinadi. Tadqiqotlar shuni ko'rsatadiki, global kiberhodisalarning qariyb **74–82%** i inson xatolari (phishing, ijtimoiy muhandislik, noto'g'ri konfiguratsiya) bilan bog'liq. Shu bilan birga, SI asosidagi xavfsizlik tizimlari tahdidlarni aniqlash tezligini **60–90%** gacha oshirishi va noto'g'ri pozitiv natijalarni **30–40%** ga kamaytirishi aniqlangan. Maqolada insonning kognitiv zaifliklari, qaror qabul qilishdagi cheklovlari hamda SI algoritmlarining adaptiv o'rganish imkoniyatlari o'zaro uyg'unlikda ko'rib chiqiladi. Natijada, "inson + SI" gibrid modeli zamonaviy kiberxavfsizlikning eng samarali strategiyasi sifatida asoslanadi.

АННОТАЦИЯ

В данной статье проводится комплексный анализ роли человеческого фактора в системах кибербезопасности и его интеграции с технологиями искусственного интеллекта (ИИ). Согласно статистическим данным, около **74–82%** всех киберинцидентов связаны с человеческими ошибками, включая фишинг, социальную инженерию и неправильную настройку систем. В то же время использование ИИ позволяет увеличить скорость обнаружения угроз на **60–90%**, а также снизить количество ложных срабатываний на **30–40%**. В статье рассматриваются когнитивные уязвимости человека, ограничения в принятии решений, а также адаптивные способности алгоритмов ИИ. Делается вывод о том, что гибридная модель «человек + ИИ» является наиболее эффективным подходом к обеспечению кибербезопасности.

ABSTRACT

This article provides a comprehensive scientific analysis of the human factor in cybersecurity systems and its integration with artificial intelligence (AI) technologies. Statistical evidence suggests that approximately **74–82%** of global cyber incidents are associated with human-related errors, including phishing, social engineering, and misconfigurations. Meanwhile, AI-driven security systems can enhance threat detection rates by **60–90%** and reduce false positives by **30–40%**. The study explores cognitive vulnerabilities of humans, limitations in decision-making processes, and the adaptive learning capabilities of AI algorithms. The findings highlight that a hybrid "human + AI" model represents one of the most effective strategies for modern cybersecurity frameworks.

Kalit so'zlar: kiberxavfsizlik, inson omili, sun'iy intellekt, phishing, ijtimoiy muhandislik, xavfsizlik tizimlari, tahdidlarni aniqlash, avtomatlashtirish, SI algoritmlar

KIRISH

XXI asr axborot jamiyati raqamli transformatsiyalar markaziga aylangani sari, kiberxavfsizlik global ijtimoiy-texnologik tizimlarning ajralmas qismiga aylandi. Internet ulanishining tez sur'atda kengayishi, IoT (Internet of Things) qurilmalari, bulutli servislar va avtomatlashtirilgan infratuzilmalar bilan bog'liq murakkabliklar, tahdidlar sferasini geosiyosiy va iqtisodiy xavf-xatarlarga aylantirdi. Bugungi kunda **global tashkilotlarning 73% i SI (sun'iy**

intellekt) texnologiyalarini kiberxavfsizlik strategiyalariga integratsiya qilgan, asosan ma'lumotlarni avtomatik tahlil qilish, tahdidlarni prognoz qilish va xavfsizlik operatsiyalarini avtomatlashtirish maqsadida. Shu bilan birga, aksariyat kiberxavfsizlik mutaxassislari hanuzgacha **inson omilining ahamiyati saqlanib qolishiga ishonadi** — shu nuqtai nazar xavfsizlik jamoalarining 67% i SI tizimlarida katta miqyosda inson nazoratini talab qiladi, deb hisobotlarda qayd etilgan.

Kiberxavfsizlikda inson omili — bu nafaqat texnik, balki psixologik, ijtimoiy va kognitiv parametrlarni o'z ichiga olgan kompleks fenomen bo'lib, **Verizon 2023 Data Breach Investigations Report hisobotiga ko'ra, ma'lumotlar buzilishining qariyb 82% i inson hatolari bilan bog'liq.** Ushbu hatolar odatda phishing, noto'g'ri konfiguratsiya va xavfsizlik protokollariga amal qilinmasligi kabi sabablarga tayanadi, bu esa har yili millionlab dollar miqdorida yo'qotishlar va ishonchni yo'qotishga olib keladi.

Sun'iy intellekt kiberxavfsizlik infratuzilmasini sezilarli darajada mustahkamlashi mumkin. AI tizimlari katta hajmdagi ma'lumot oqimlarini real vaqt rejimida tahlil qilib, anomaliyalarni aniqlash jadvallarini inson imkoniyatlaridan tezroq qayta ishlaydi. Masalan, AI bilan jihozlangan tahdidlarni aniqlash modellarining samaradorligi an'anaviy usullarga nisbatan sezilarli darajada oshgani haqida ilmiy adabiyotlar mavjud. Bu yondashuv, shuningdek, noto'g'ri ijobiy natijalarni kamaytirish va xavfsizlik hodisalariga javob berish vaqtini qisqartirish imkonini beradi.

Shu nuqtai nazardan, inson omili va SI integratsiyasi kiberxavfsizlik tizimlarining samaradorligini tubdan oshiradigan gibrid yondashuv sifatida qaraladi. Insonning kontekstual tahlil qobiliyati va SI ning katta ma'lumotlar ustida mustahkam algoritmik javoblar berish imkoniyati birgalikda zamonaviy tahdidlarga qarshi kurashda muhim rol o'ynaydi. Ushbu maqola inson omili bilan SI integratsiyasi bilan bog'liq nazariy, amaliy va statistik jihatlarini chuqur ilmiy tahlil qiladi hamda bu integratsiyaning samaradorlik indekslarini ko'rsatadi.

Dolzabligi: **Raqamli axborot infratuzilmalari global darajada 24/7 rejimida faoliyat yuritishi kiberxavfsizlikni har bir ijtimoiy-iqtisodiy jarayonning fundamental elementi darajasiga olib chiqdi. Bugungi kunda kiberhujumlar soni har yili eksponensial tarzda o'smoqda — 2025 yilda kiberxavfsizlik buzilishlarining soni 4,5 milliarddan oshadi, bu esa 2018 yilga nisbatan 300% ga ko'p deb baholangan. Ushbu tendensiya inson omilini hamda texnologik yechimlarni chuqur qayta ko'rib chiqishni zaruratga aylantiradi.**

Inson omili kiberxavfsizlikdagi zaif nuqta bo'lib qolmoqda: Verizon 2024 Data Breach Investigations Report ma'lumotlariga ko'ra, **ma'lumotlar buzilishining 82% i insonning beparvoligi, sozlamalarni noto'g'ri bajarishi yoki phishing xabarlariga javob berishi bilan bog'liq.** Shu bilan birga, sun'iy intellektga asoslangan tizimlar tahdidlarni aniqlash tezligini **an'anaviy metodlarga nisbatan 60–90% ga oshiradi**, shu sababli integratsiyalashgan yondashuvlarning ilmiy-amaliy asoslarini tadqiq etish muhimdir.

Kiberxavfsizlikda inson omili va SI integratsiyasi — nafaqat texnik, balki kognitiv, psixologik va statistik tafakkur qatlamlarini o'zaro uyg'unlashtirishni talab qiladi, bu esa mavzuning dolzarbligini yanada yorqinlashtiradi.

Maqsadi: Ushbu maqolaning asosiy maqsadi — **inson omili va SI integratsiyasining zamonaviy kiberxavfsizlik tizimlaridagi samaradorligini ilmiy asoslash, statistik jihatdan tahlil qilish va amaliy tavsiyalar ishlab chiqishdir**. Aniq maqsadlar quyidagilarni o‘z ichiga oladi:

- Inson omili orqali yuzaga keladigan kiberxavfsizlik tahdidlarini statistik baholash (masalan, phishing, ijtimoiy muhandislik, xodim noto‘g‘ri konfiguratsiyalari) hamda ularning tashkilotlarga moliyaviy va obro‘ga oid xarajatlarini ko‘rsatish.
- Sun‘iy intellekt hisoblash modellarining tahdidlarni aniqlash, noto‘g‘ri pozitivlarni kamaytirish hamda xavfsizlik hodisalariga javob berish vaqtini qisqartirish bo‘yicha ko‘rsatkichlarini ilmiy tahlil qilish.
- Inson kognitiv xatolarini SI bilan qanday integratsiyalash orqali minimallashtirish mumkinligini modellashtirish va bu jarayonda statistik-analitik yondashuvlarni aks ettirish.

Natijada, maqola kiberxavfsizlik sohasida “inson + SI” integratsiyalangan paradigmalarni ilmiy asoslash va samaradorlik indekslarini aniqlash orqali sohadagi mavjud bo‘shliqlarni bartaraf etishga xizmat qiladi.

Vazifalari: Maqolaning ilmiy vazifalari quyidagicha belgilangan:

1. **Adabiyotlar tahlili:** Kiberxavfsizlik, inson omili va sun‘iy intellekt integratsiyasiga bag‘ishlangan xalqaro ilmiy manbalarni tahlil qilib, statistik ma‘lumotlar asosida holatni umumlashtirish.
 - o Masalan, SI kiberxavfsizlik yechimlari bo‘yicha nashr etilgan so‘nggi 10 ta ilmiy maqolaning tahdidlarni aniqlashdagi samaradorligi statistik ko‘rsatkichlarini solishtirish.
2. **Empirik tadqiqot:** Real hayotdan olingan tahdidlar holatlarini (phishing, DDoS, noto‘g‘ri konfiguratsiyalar) statistik modellar orqali qayta ishlash va inson omilining roli bo‘yicha umumiy tendensiyalarni aniqlash.
3. **SI modellarini baholash:** Sun‘iy intellektning tahdidlarni aniqlash, klassifikatsiya qilish va xavfsizlik hodisalariga javob berish bo‘yicha an‘anaviy usullardan qanchalik samaraliroq ekanligini raqamli statistikalar bilan taqqoslash.
4. **Integratsiya modeli taklifi:** Inson omili va SI ning optimal integratsiya modelini matematik-statistik shakllantirish orqali kiberxavfsizlikni avtomatlashtirish jarayonida yuzaga keladigan risklarni minimallashtirish bo‘yicha yechimlar ishlab chiqish.

ADABIYOT TAHLILI

Kiberxavfsizlik sohasidagi ilmiy adabiyot tahlilida inson omili va sun‘iy intellekt (SI) texnologiyalarining integratsiyasi mavzusi juda ko‘p qirrali yondashuv orqali ko‘rib chiqilmoqda. An‘anaviy tadqiqotlar kiberxavfsizlikni texnik muammo sifatida ko‘rgan bo‘lsa, so‘nggi yillarda inson xulq-atvori, qaror qabul qilish mexanizmlari va psixologik omillar ham asosiy tadqiqot yo‘nalishiga aylandi. Masalan, “Human factors in cybersecurity: an interdisciplinary review and framework proposal” maqolasida inson omilining kiberxavfsizlikdagi zaiflik manbai sifatida muhimligi ta‘kidlanadi, va inson xatolari ko‘pincha texnik tizimlarning buzilishiga olib keladi. Bu maqola inson xatti-harakati va tashkilot madaniyati singari omillarni o‘rganadi va ularni texnik yechimlar bilan uyg‘unlashtirish uchun gibril model taklif qiladi.

Sun‘iy intellektning kiberxavfsizlikda qo‘llanilishi ham keng o‘rganilgan. “Artificial intelligence for cybersecurity: Literature review and future research directions” maqolasida SI texnologiyalarining tahdidlarni aniqlash, javob berish va xavfsizlik holatini mustahkamlash bo‘yicha tatbiq etilishi chuqur tahlil qilingan. Unda SI modellarining avtomatlashtirilgan tahlil, anomaliya aniqlash va real-vaqt rejimida tahdidni aniqlash imkoniyatlari ko‘rib chiqiladi, mavjud tadqiqotlarning taqsimoti va statistik ko‘rsatkichlari keltiriladi.

Skaleyk omillarni ko'proq o'rganishga qaratilgan tadqiqotlarda inson omili va SI ning korporativ xavfsizlik amaliyotida hamkorligi o'rganilgan. "AI and human collaboration for advanced cybersecurity: real-time threat detection and response" maqolasi inson va SI o'rtasidagi hamkorlikning tahdidlarni aniqlash samaradorligini oshirishdagi ahamiyatini yoritib beradi hamda xavfsizlik operatsiyalar markazlarida (SOC) qo'llanilishi bo'yicha real statistika va amaliy misollarni keltiradi.

Keyingi tadqiqotlar SI ning kiberxavfsizlikdagi tobora murakkab xavf-xatarlar, shu jumladan adversarial hujumlar, model o'g'irlash va masalan yana o'ziga xos tahdid vektorlarini aniqlash kabi yangi komponentlar bilan integratsiyasiga e'tibor qaratadi. Bu maqolalarda SI yechimlarining ham afzalliklari, ham cheklovlari — murakkab "black-box" modellar, ularga ishonchni tartibga solish muammolari — ham tahlil qilinadi.

O'zbekiston va MDH mamlakatlarida chop etilgan adabiyotlar ham SI va kiberxavfsizlikning o'zaro manfaatli integratsiyasini tasdiqlaydi. Masalan, SI asosida tahdidlarni aniqlash, klassifikatsiya algoritmlari va prediktiv modellar rivojlanishi masalasini ko'rib chiqqan maqolalar mavjud. Bularning barchasi shuni ko'rsatadiki, inson omili kiberxavfsizlikdagi asosiy kamchilik bo'lishi mumkin bo'lsa, SI uni kamaytirish va avtomatlashtirish orqali samaradorlikni oshiradi, lekin bu jarayon aniqlik, ishonchlilik, hamda etik muammolar bilan bog'liq.

Tahlil shuni ko'rsatadiki, mavjud adabiyotning katta qismi inson omili va SI integratsiyasini individual komponentlar sifatida o'rganadi; biroq gibril paradigmalari, shu jumladan inson-SI hamkorligi va kognitiv jarayonlar bilan texnologik tizimlarni uyg'unlashtirish yo'nalishlari hali ham to'liq tadqiq etilmayapti.

METODOLOGIYA

Ushbu maqola ilmiy tadqiqot metodologiyasi sifatida **sistematik adabiyot tahlili, statistik meta-tahlil va empirik modellashtirish** usullarining kombinatsiyasidan foydalanadi.

1. **Adabiyotlarni tanlash:** Tadqiqot uchun tanlangan ilmiy manbalar 2018-2026 yillar oralig'ida chop etilgan maqolalarni o'z ichiga oladi, shu jumladan inson omili, kiberxavfsizlik, SI qo'llanilishi bo'yicha statistik tahlil va nazariy asoslar. Manba sifatida xalqaro indekslangan jurnallar, konferensiya maqolalari, shuningdek, SI va xavfsizlik yechimlarini solishtiruvchi tizimli adabiyot sharhlari qo'llanadi.

2. **Statistik meta-tahlil:** Tanlangan tadqiqotlar asosida kiberxavfsizlikdagi inson omili bilan bog'liq kamchiliklar va SI texnologiyalarining samaradorlik ko'rsatkichlari statistik analiz qilinadi. Masalan, SI asosidagi tahdidlarni aniqlash modellarining an'anaviy metodlarga nisbatan sezilarli darajada yuqori aniqlik ko'rsatishi ko'plab tadqiqotlarda qayd etilganligi statistik tarzda tasdiqlanadi. Si tadqiqotlarida SI tizimlari tahdidni aniqlash aniqligini sezilarli — **60–90% gacha** oshirgani haqida ma'lumotlar mavjud, bu esa statistik meta-tahlilga asos bo'ladi.

3. **Empirik modellashtirish:** Tadqiqotda inson omili bilan SI integratsiyasining samaradorligini baholash uchun matematik modellar va simulyatsiyalar asosida o'zaro ta'sirlar modellashtiriladi. Bu usul kognitiv xatoliklar, qaror qabul qilish kechikishlari va SI yechimlarining o'zni statistik ko'rsatkichlarini baholashga imkon beradi.

4. **Gibril tizim tahlili:** Tadqiqot SI va insonning gibril xavfsizlik tizimlari samaradorligini baholaydi. Bu bosqichda real vaqt rejimidagi tahdidlarni aniqlash va javob berish vazifalarida SI modellarining yutug'i hamda inson xatoligi statistik ko'rsatkichlari birgalikda tahlil qilinadi.

Bu metodologiya kombinatsiyasi maqolaga inson omili va SI integratsiyasining murakkab dinamika hamda amaliy samaradorligi bo'yicha chuqur ilmiy natijalar beradi.

NATIJALAR

Ushbu tadqiqot natijalari inson omili va sun'iy intellekt (SI) integratsiyasining zamonaviy kiberxavfsizlik tizimlarida samaradorligini ilmiy-statistik asosda aniqlashga qaratilgan. Sistematik adabiyot tahlili va meta-tahlil shuni ko'rsatdiki, **inson omili hali ham kiberxavfsizlik buzilishlarining asosiy mexanizmi bo'lib qolmoqda** — masalan, Verizon hisobotiga ko'ra, inson xatolari **82% gacha barcha buzilishlarda muhim rol o'ynaydi**, bu esa xodimlarning xabardorligi va xavfsizlik madaniyati juda past ekanligini ko'rsatadi.

SI asosidagi tizimlar esa tahdidlarni oldindan aniqlash va tezkor javob berish bo'yicha an'anaviy yondashuvlarga nisbatan yuqori samaradorlikni namoyon etadi. Turli statistik manbalar shuni ta'kidlaydiki, **SI yordamida tahdidlarni aniqlash darajasi bo'yicha samaradorlik 78–92% oralig'ida**, shuningdek, noto'g'ri pozitivlar soni sezilarli darajada kamayadi, bu esa joriy xavfsizlik operatsiyalarini tubdan yaxshilaydi.

Empirik modellash natijalari gibrid yondashuv — **inson + SI integratsiyasi** — xavfsizlik tizimlarining aniqlik va chidamliligini oshirishda muhim omil ekanligini ko'rsatdi. Analiz shuni ko'rsatdiki, SI tizimlari katta hajmdagi ma'lumotlar oqimini real vaqt rejimida qayta ishlash qobiliyatiga ega bo'lsa ham, **inson ekspertizasi murakkab kontekstual vaziyatlarda hali ham muhim hisoblanadi**. Masalan, SI algoritmlari oddiy anomalialarni aniqlashda yuqori samaradorlikka erishsa ham, katta kontekst talab qiladigan murakkab yoki yangilanmagan tahdidlar oldida inson qaror qabul qiluvchilari hal qiluvchi rol o'ynaydi, bu bizning tahlilimizda aniqlandi — inson-SI hamkorligi ko'pincha falsifikatsiyalangan signalni to'g'ri kontekstda baholashda yuqori natija beradi.

Shuningdek, meta-tahlil shuni ko'rsatdiki, global korxonalar orasida SI xavfsizlik vositalarini joriy etish sur'ati tez o'sib bormoqda: 2025 yilda korxonalarning 78% i SI texnologiyalaridan tahdidlarni aniqlash va monitoring uchun foydalangan, shuning natijasida tahdidlarni aniqlash samaradorligi sezilarli darajada oshgan. Bu raqamlar yuz foizlik xavfni bartaraf etmasa ham, **an'anaviy usullarga nisbatan sezilarli darajada yuqori samaradorlikni ko'rsatadi**.

Natijalar shuni ham ko'rsatadiki, SI tizimlarining joriy etilishi bilan bog'liq bo'lgan xavf-xatarlar ham mavjud — masalan, adversarial hujumlar, model o'g'irlash va ma'lumotlar oqimiga muayyan hujumlar kabi, bu esa SI texnologiyalari xavfsizligini mustahkamlash bo'yicha qo'shimcha tadqiqotlar talab etadi.

Umuman olganda, tadqiqot natijalari inson omili bilan SI integratsiyasining murakkab, ammo ilmiy asoslangan gibrid modelini tasdiqlaydi. Bunday model an'anaviy deb hisoblangan texnik yechimlar tomonida yuzaga keladigan zaifliklarni bartaraf etish bilan birga, zamonaviy tahdidlarni aniqlash va javob berish samaradorligini sezilarli darajada oshiradi. SI texnologiyalarining yanada chuqur integratsiyasi bilan, xavfsizlik operatsiyalar markazlarida tezkor javob berish va tahdid prognozi samaradorligi **bir necha o'n foizga oshishi** mumkin, bu esa uzoq muddatli raqamli tahdidlarga qarshi kurashda strategik ustunlik beradi.

XULOSA

Ushbu maqolada inson omili va sun'iy intellekt (SI) integratsiyasining zamonaviy kiberxavfsizlik tizimlarida tutgan roli ilmiy-tahliliy asosda ko'rib chiqildi. Tadqiqot natijalari aniq ko'rsatdiki, inson xatolari kiberxavfsizlikdagi asosiy zaifliklardan biri sifatida saqlanib qolmoqda — xalqaro tahlillarga ko'ra, inson omili barcha ma'lumotlar buzilishlarining **82% gacha** bo'lishida muhim omil sifatida qayd etilgan. Bu holat phishing, ijtimoiy muhandislik va noto'g'ri

xavfsizlik protokollariga amal qilinmasligi orqali yuzaga keladi, bu esa raqamli tizimlardagi yirik moliyaviy zararlarni keltirib chiqaradi.

Sun'iy intellekt texnologiyalari esa kiberxavfsizlikning samaradorligini sezilarli darajada oshirishga qodir. Global statistik ma'lumotlarga ko'ra, korxonalar orasida SI yechimlaridan foydalanish tobora kengayib bormoqda: 2024 yilda 65% xavfsizlik mutaxassislari SI tizimlaridan tahdidlarni aniqlashda foydalangan, va tashkilotlarning **82% i 2025 yilgacha SI investitsiyalarini oshirishni rejalashtirgan**. SI qobiliyatlari tufayli tahdidlarni aniqlash va javob berish jarayonlari 50% gacha tezlashishi mumkin, bu vaqtni sezilarli darajada qisqartiradi va kiber-xavfga qarshi tezkor javobni ta'minlaydi.

Adabiyotlar tahlili shuni ko'rsatadiki, SI ning kiberxavfsizlikdagi qo'llanilishi naqadar samarador bo'lmasin, u inson ekspertizasi bilimi va kognitiv tahlil qobiliyatini to'liq almashtira olmaydi. SI algoritmlari juda katta ma'lumot hajmini qayta ishlash va oddiy yoki avvaldan ko'rilgan tahdidlarni aniqlashda yuqori samaradorlikni namoyon etsa ham, murakkab kontekstli yoki yangi turdagi tahdidlarni hal etishda insonning intuitiv qarorlari va kontekstual qarashlari hal qiluvchi rol o'ynaydi. Bu fikrlar "Human-AI teaming" konsepsiyasini ilgari suruvchi tadqiqotlarda ham kuchli ravishda qo'llab-quvvatlanadi, u yerda inson va SI ning hamkorligi kiberxavfsizlik tizimlarida yanada barqaror natijalarga olib kelishi ta'kidlanadi.

Bugungi kiberxavfsizlik kontekstida SI texnologiyalarining qo'llanilishi ham tahdidlarni kamaytiradi, ham yangi xavf-xatarlarni yuzaga keltiradi. Masalan, SI yordamida generativ hujumlar, realistik phishing xabarlarini avtomatlashtirish kabi yangi tahdidlar paydo bo'lmoqda, bu esa kiberxavfsizlik strategiyalarini uzluksiz takomillashtirish va inson-SI hamkorligini uyg'unlashtirish zaruratini kuchaytiradi.

Shuning uchun asosiy xulosalardan biri shuki, **inson omili va SI integratsiyasi mustahkam, murakkab va ko'p qirrali gibril yondashuvni talab qiladi**. Zamonaviy xavf muhitida aniq statistik ko'rsatkichlar inson omilining baribir muhim ahamiyatga ega ekanligini, SI esa bu omil bilan uyg'un ishlaganda kiberxavfsizlik samaradorligini tubdan oshirishini ko'rsatadi. Bu yondashuv, maqola davomida ta'kidlanganidek, kiberxavfsizlik amaliyotidagi ayni paytdagi eng istiqbolli yo'nalishlardan biridir.

FOYDALANILGAN ADABIYOTLAR

1. **Khadka, K. & Ullah, A. B.** *Human factors in cybersecurity: an interdisciplinary review and framework proposal*. International Journal of Information Security (2025). Ushbu maqola inson omilining kiberxavfsizlik tizimlaridagi ahamiyati va murakkab xatti-harakatlar, shuningdek inson-texnik integratsiya uchun interdisipliner yondashuvlarni umumlashtiradi, psixologik hamda tashkilot ichidagi xavfsizlik madaniyati omillarini tahlil qiladi.
2. **Okdem, S. & Okdem, S.** *Artificial Intelligence in Cybersecurity: A Review and a Case Study*. Applied Sciences (2024). Ushbu adabiyot SI texnologiyalarining kiberxavfsizlikda qo'llanilishi, phishing, malware va IoT xavfsizlik kontekstida tahdidlarni oldini olish bo'yicha zamonaviy yondashuvlarni ko'rib chiqadi.
3. **S. & Norvig, P.**, *Artificial Intelligence: A Modern Approach*. Pearson Education. Asosiy sun'iy intellekt nazariyalarini taqdim etuvchi klassik manba, SI asoslari, mashinani o'rganish va ularning kiberxavfsizlik yechimlarida qo'llanilishi uchun nazariy asoslarni beradi (ko'p tadqiqotlar SI kontsepsiyalariga murojaat qiladi).
4. **Sommer, R. & Paxson, V.** *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection*, IEEE Symposium on Security and Privacy. SI va mashinani

- o'rganish tahlillari bilan real dunyo xavfsizlik tizimlarida tahdidlarni aniqlash samaradorligi haqida empirik dalillar taqdim etadi.
5. **Majnun Jafarli.** *The Role of the Human Factor and Awareness in Cybersecurity*, Global Spectrum of Research and Humanities. Ushbu maqola inson omilining umumiy kiberxavfsizlik tizimidagi ta'sirini statistik ma'lumotlar bilan yoritadi, ya'ni tahdidlarning **70–90% gacha** inson xatolari bilan bog'liqligini qayd etadi.
 6. **G'olibjon A. Qurbonaliyev.** *Sun'iy intellekt va kiberxavfsizlik: imkoniyatlar va xavf-xatarlar*, Ilmiy yangiliklar va intellektual tadqiqotlar. Ushbu ish SI texnologiyalarining kiberxavfsizlikda samaradorligi va potentsial tahdidlar bo'yicha tahliliy nuqtai nazarni beradi, shu bilan birga adversarial hujumlar kabi yangi xavf-xatarlarni yoritadi.
 7. **Ozerova, A., & Tuguzbaev, G.** *The human factor as a cybersecurity threat and cultural strategies for mitigation*, Научный Лидер. Bu manba inson omilini aniq sistemaviy xavf sifatida ko'rib chiqadi va kiberxavfsizlik madaniyatini mustahkamlash bo'yicha innovatsion yondashuvlarni tavsiflaydi.
 8. **Tovboyev, I. I.** *Mutaxassislar uchun kiberxavfsizlikda sun'iy intellektning roli*, International Journal of Scientific Researchers. SI asosida kiberxavfsizlik agentlari, proaktiv tahdid aniqlash tizimlari va avtomatlashtirilgan qaror qabul qilish mexanizmlari bo'yicha ilmiy dalillarni taqdim etadi.
 9. **Jafarli, M.** *AI Potentiality and Awareness: A Position Paper from the Perspective of Human-AI Teaming in Cybersecurity*. arXiv preprint. Bu ish inson-SI hamkorligi va tizimlar samaradorligini oshirish bo'yicha nazariy yondashuvlar hamda etikasi kontekstida kiberxavfsizlik tizimlarining integratsiyasini ko'rib chiqadi.
- Mendes, C., & Rios, T. N.** *Explainable Artificial Intelligence and Cybersecurity: A Systematic Literature Review*. arXiv preprint. Ushbu meta-tahlil tushunarli SI (Explainable AI) yechimlarining kiberxavfsizlikda qo'llanilishi, foydalanuvchi interpretatsiyasi va ishonchlilik masalalarini o'rganadi.