Аъзамов Темур Нарзуллаевич
Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги, Сунъий интеллектни жорий қилиш ва ривожлантириш департаменти, Сунъий интеллектни ривожлантириш илмий-тадқиқот ишларини мувофиқлаштириш бўлими бош мутахассиси, техника фанлари бўйича фалсафа доктори
Насруллаев Парвиз
Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги, Сунъий интеллектни жорий қилиш ва ривожлантириш департаменти, Сунъий интеллект технологияларини ривожлантириш бўлими бошлиғи
Султанов Йўлдошбой Ўразметбоевич
Тошкент ахборот технологиялари университети докторанти

АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШДА СУНЪИЙ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРИДАН ФОЙДАЛАНИШНИНГ ДОЛЗАРБЛИГИ

Аъзамов Темур Нарзуллаевич
Доктор философии в области технических наук, главный специалист Отдела координации исследований в области искусственного интеллекта, Департамент внедрения и развития искусственного интеллекта Министерства развития информационных технологий и коммуникаций Республики Узбекистан
Насруллаев Парвиз
Начальник Отдела развития технологий искусственного интеллекта, Департамент внедрения и развития искусственного интеллекта Министерства развития информационных технологий и коммуникаций Республики Узбекистан
Султанов Йулдошбой Уразметбоевич
Докторант, Ташкентский университет информационных технологий

АКТУАЛЬНОСТЬ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Azamov Temur
Ministry of Information Technologies and Communications Development, Department of Introduction and Development of Artificial Intelligence, Chief Specialist, Artificial Intelligence Research Coordination Department Doctor of Philosophy in Technical Sciences

Nasrullayev Parviz
Ministry of Information Technologies and Communications Development, Department of Introduction and Development of Artificial Intelligence, Head of Artificial Intelligence Technology Development
Sultanov Yuldoshboy
Tashkent University of Information Technologies, Doctoral student

THE RELEVANCE OF USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES TO ENSURE INFORMATION SECURITY

Аннотация. *Мазкур мақолада ахборот хавфсизлигини таъминлашда сунъий интеллект технологияларидан фойдаланишнинг долзарблиги ўрганилган. Ахборот хавфсизлигини таъминлаш соҳасида сунъий интеллектдан фойдаланишнинг мумкин бўлган усуллари таҳлили ўтказилди ва ахборотга рухсатсиз киришнинг олдини олиш, шунингдек, ахборот хавфсизлиги бузилиши оқибатларини камайтиришда ушбу юқори технологиядан фойдаланиш имкониятлари ўрганилди.*

Калит сўзлар: *ахборот, сунъий интеллект, киберхавфсизлик, ахборот хавфсизлиги, маълумотлар.*

Аннотация. *В данной статье рассматривается актуальность использования технологий искусственного интеллекта в информационной безопасности. Проведен анализ возможных способов использования искусственного интеллекта в сфере информационной безопасности и изучены возможности использования данной высокой технологии для предотвращения несанкционированного доступа к информации, а также снижения последствий нарушений информационной безопасности.*

Ключевые слова: *информации, искусственный интеллект, кибербезопасность, информационная безопасность, сведения (данные).*

Abstract: *This article discusses the relevance of using artificial intelligence technologies in information security. In the field of information security, an analysis of possible ways of using artificial intelligence was carried out and the possibilities of using this high technology to prevent unauthorized access to information, as well as to reduce the consequences of information security violations, were studied.*

Key words: *data, cybersecurity, information security, artificial intelligence, information.*

“Ахборот хавфсизлиги нуқтаи назаридан сунъий интеллект атроф-муҳит ҳолатини талқин қилиш, унда содир бўлган воқеаларни таниб олиш ва керакли чораларни мустақил равишда амалга оширишга қодир дастурдир.

Машинали ўқитиш тизимлари инсон томонидан киритилган маълумотлар ва амалга оширилган ҳаракатлар натижалари бўйича мустақил равишда ўқитилиши мумкин бўлган дастурдир. Машинали ўқитиш воситалари ўтмишда содир бўлган воқеалар ҳақидаги маълумотларга асосланган прогнозларни яратишга қодир.

Ахборот хавфсизлигини таъминлашда сунъий интеллектдан фойдаланиш икки омил билан оқланади: киберҳужум содир бўлган тақдирда тезкор чоралар кўриш зарурати ва кибермудофаа бўйича малакали мутахассисларнинг етишмаслиги. Дарҳақиқат, замонавий воқеликда ахборот хавфсизлиги бўйича кенг кўламли ҳодисалар тез ривожланиши даврида ходимлар рўйхатини зарур тажрибага эга бўлган малакали ахборот хавфсизлиги мутахассислари билан тўлдириш жуда қийин. Агар компанияда ахборот хавфсизлиги бўйича таҳлилчиларнинг кечаю кундуз навбатчилик тартиби бўлмаса, у ҳолда киберҳодисаларга тезкор мустақил жавоб бериш тизимисиз иш соатларидан кейин юқори сифатли ҳимояни таъминлаш жуда қийин бўлади. Бундан ташқари, “интернет тажовузкорлари” ўз ҳужумларидан олдин чалғитишни амалга оширишлари мумкин – масалан, DDoS ҳужумини бошлаш ёки тармоқни фаол сканерлаш кибермутахассисларни чалғитади. Бундай ҳолатларда сунъий интеллектга асосланган киберҳодисаларга жавоб бериш тизими ёрдам беради, бу бир вақтнинг ўзида кўплаб ахборот хавфсизлиги ҳодисаларини қайта ишлаш, ахборот хавфсизлиги бўйича таҳлилчиларнинг мунтазам ҳаракатларини автоматлаштириш ва инсон аралашувисиз ҳодисаларга тезкор жавоб беришни таъминлайди. Масалан Сесуритий Висион IRP/SOAP ечимида сунъий интеллект ва машинали ўқитиш механизмлари кенг қўлланилади ва бунда аввал ҳал қилинган ҳодисалар бўйича ўқитилган платформанинг ўзи таҳлилчига киберҳодиса тури ва унинг хусусиятларига қараб, тегишли жавоб ҳаракатини таклиф қилади. Тегишли билимга эга эксперт тизимлардан оптимал жавоб гуруҳи тайинланади ва атипик шубҳали ҳодисалар аниқланган тақдирда тизимнинг ўзи тегишли чоралар яратади ва бу ҳақда ахборот хавфсизлиги бўлими ходимларини хабардор қилади. IRP/SOAP Security Vision ечими кибер ҳодисаларга башоратли жавоб бериш учун алгоритмлардан фойдаланади ва ўқитилган тизим сизга ҳужум векторини ҳамда унинг инфратузилмадаги кейинги ривожланишини башорат қилиш, тенденцияларни кўрсатиш, кейин автоматик равишда зарарли ҳаракатларни тўхтатиш ва SOS таҳлилчиларига маслаҳат бериш имконини яратади.

Сунъий интеллектга асосланган ҳимоя тизимлари кўп сонли ахборот хавфсизлиги ҳодисаларида аномалияларни аниқлаш учун ажралмас ёрдамчи инструмент ҳисобланади. Масалан, бунга ахборот хавфсизлиги журналлари, SIEM тизимлари ёки SOAP ечимлари маълумотларини таҳлил қилиш тизимлари мисол бўла олади.

Классик дисперцияларни таҳлил қилиш тизимлари, одатда, операторлар томонидан олдиндан ўрнатилган баъзи қоидаларга асосланади: масалан, маълум трафик ҳажмидан ошиб кетиш, маълум миқдордаги муваффақиятсиз аутентификация уринишлари, маълум миқдордаги кетма-кет IPS триггерлари мисол бўлиши мумкин. Сунъий интеллектга асосланган тизимлар ахборот хавфсизлиги ходимлари томонидан илгари яратилган, ўз аҳамиятини йўқотиб қўйган ва ўзгартирилган АТ инфратузилмасини ҳисобга олмаган қоидаларга "орқага қарамай" мустақил равишда қарор қабул қилиши мумкин.

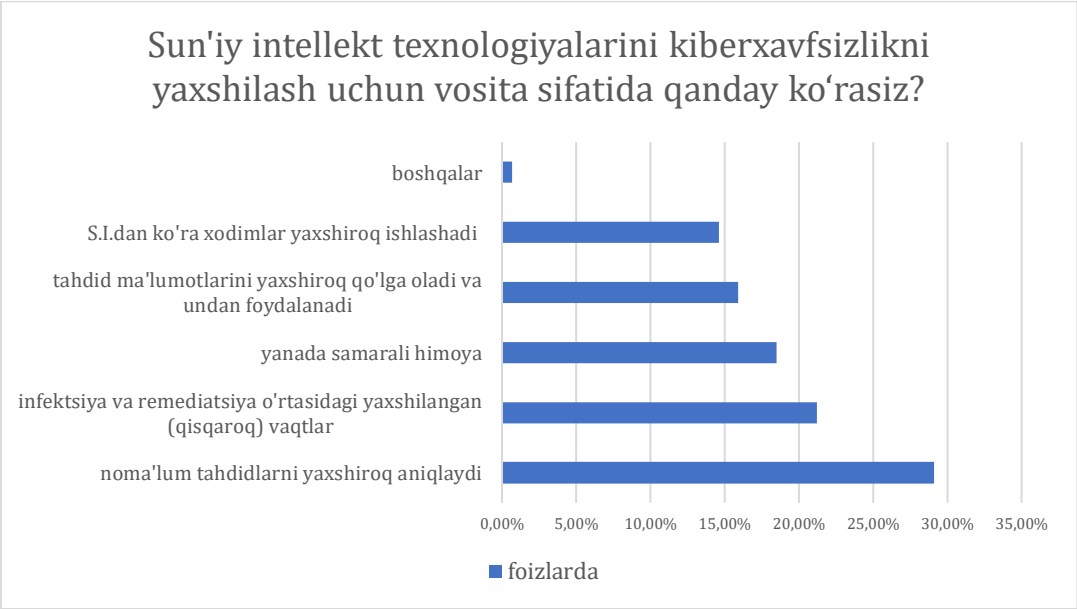
Аномалияларни аниқлаш фойдаланувчи маълумотларини ҳимоя қилишга ёрдам беради – масалан, онлайн-банкинг хизмати бузилган ҳисоблар рақамларни тезда аниқлаш учун мижоз намуналари (хусусиятлари, белгилари) ҳақидаги маълумотларни тўплаши ва таҳлил қилиши мумкин. Мисол учун, агар фойдаланувчи ўтган йил давомида иш кунларида Ўзбекистон IP-манзилидан хизматга уланган бўлса ва Интернет Explorer браузеридан фойдаланган бўлса, кўп вақт ўтмай бу мижоз Хитойдан тунда Mozilla FireFox браузери ёрдамида уланса, эҳтимол у ушбу фойдаланувчининг ҳисобини вақтинча блокировка қилиши ва унга огоҳлантириш юбориши мумкин. Молиявий институтлар, шунингдек, кредит олувчиларни тўлов қобилиятини баҳолаш, молиявий рискларни таҳлил қилиш ва фирибгарликка қарши тизимлардан фойдаланиш учун машинали ўқитиш ва сунъий интеллект тизимларидан фойдаланиши мумкин [1].

Киберхавфсизликда сунъий интеллект тизимларидан фойдаланишнинг яна бир модели ички қоидабузарлар билан ишлашдир. Масалан фойдаланувчининг одатий хатти-ҳаракатларини билиб, тизим ходимнинг иш моделида сезиларли ўзгаришлар юз берганда (шубҳали сайтларга ташриф буюриш, узоқ вақт ишламай қолиш) ахборот хавфсизлиги бўйича таҳлилчиларга огоҳлантириш юбориши мумкин. Компьютерли кўриш ва нутқни қайта ишлаш билан жиҳозланган хавфсизлик тизимлари нотаниш шахслар ёки бошқа бировнинг рухсатномасидан фойдаланган ҳолда ходимлар томонидан назорат-ўтказиш пункти орқали ўтишга уринишлар тўғрисида зудлик билан хабардор қилиш, веб-камералар ёрдамида ходимларнинг иш фаолиятини таҳлил қилиш, менежерлар ва бошқарувчилар ўртасидаги мулоқотнинг тўғрилигини баҳолаш имкониятига эга бўлади.

"Сунъий интеллект ва машинали ўқитиш, киберҳужум ва ахборот таҳдидларига жавоб беришни сезиларли даражада тезлаштиради, дейди "Nemertes Research" таҳлилчилари. Уларнинг фикрича, бугунги кунда у ҳақиқий эҳтиёж таъсирида шаклланган жиддий бозор. Nemertes ўтказган тадқиқот натижалари шуни кўрсатдики, ташкилотлар киберҳужумни аниқлаш ва унга жавоб бериш учун ўртача 39 кун давом этади, бироқ баъзи компаниялар сунъий интеллект технологиялари ёрдамида бу вақтнинг бир неча соатгача қисқартиришга муваффақ бўлишган [2]".

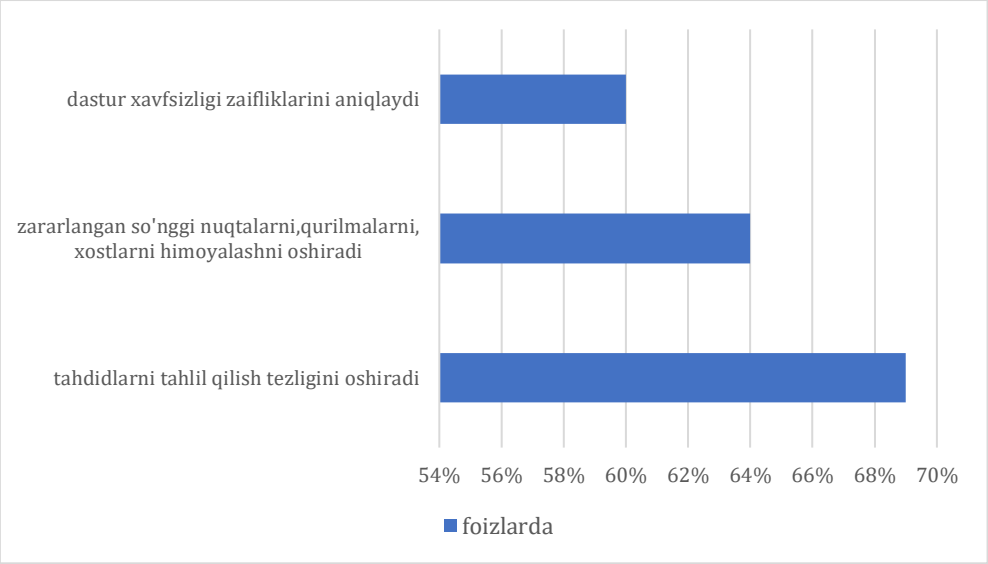
“Ҳозирги кунда компаниялар хавфсизлик таҳдидларини аниқлаш ва уларга жавоб бериш учун сунъий интеллект ва машинали ўқитишдан кенг фойдаланиб келинмоқда. Мисол учун, “Barslays Africa” банкида маҳаллий корпоратив тармоқ ва булутли тизимларнинг келишув белгиларини аниқлаш учун сунъий интеллектни фойдаланишади.

“Барча маълумотлар тизимлари учун сунъий интеллект технологиялари номаълум таҳдидларни аниқлаш самарадорлигини оширишга имкон беради. “SANS institute” томонидан хавфсизлик мутахассислари ўртасида сунъий интеллект технологияларини киберхавфсизликни яхшилаш учун восита сифатида қандай қарашларини аниқлаш мақсадида сўровнома ўтказилган. Сўровнома натижалари 1-расмда келтирилган [3]”.



1-расм. Хавфсизлик мутахассислари ўртасида сунъий интеллект технологияларини киберхавфсизликни яхшилаш учун восита сифатида қандай қарашларини аниқлаш мақсадида ўтказилган сўровнома натижаси.

“Ponemon Institute” маълумотларига кўра, ахборот хавфсизлиги бўйича мутахассисларнинг қарийб 60 фоизи ахборот хавфсизлигида сунъий интеллект технологияларидан фойдаланиш сўнгги нуқталар ва иловалардаги таҳдидларни таҳлил қилиш ҳамда аниқлаш тезлигини оширади, деб ҳисоблашади.



3-расм. СИ технологияларини қўллашдан кейин ахборот хавфсизлиги кўрсаткичларини яхшилаш бўйича статистик маълумотлар.

“Сунъий интеллект замонавий ахборот таҳдидларига қарши курашга катта ҳисса қўшмоқда. Хусусан, аксарият ҳолларда ташкилотнинг ахборот хавфсизлигига SI технологияларини жорий этиш, хавфсизлик муаммоларини аниқлаш ва ҳодисаларга жавоб бериш вақтини, шунингдек, ходимларни бошқариш харажатларини қисқартиради. Операторлар номаълум таҳдидларни аниқлаш самарадорлиги, шунингдек, сўнгги нуқталар ва иловалардаги зарарли фаолиятни таҳлил қилиш ҳамда аниқлаш тезлиги ошишини қайд этишган [4].

ФОЙДАЛАНГАН АДАБИЁТЛАР РЎЙҲАТИ:

1. https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-securit.
2. https://www.osp.ru/cio/2017/10/13053561.
3. https://www.lanit.ru/press/smi/iskusstvennyy-intellekt-dlya-effektivnoy-sistemy-bezopasnosti/.
4. https://www.iksmedia.ru/articles/5682996-Iskusstvennyj-intellekt-v-informaci.html.