

КИБЕРХАВФСИЗЛИКНИ ТАЪМИНЛАШ МАСАЛАЛАРИДА СУНЪИЙ ИНТЕЛЛЕКТ ИМКОНИЯТЛАРИ

Айсаев Искандар Музаффарович

“Киберхавфсизлик маркази” ДМ, Малака ошириш бўлими бошлиғи

i.aysaev@csec.uz

Аннотация: Мазкур мақолада сунъий интеллектнинг киберхавфсизликни таъминлаш масалаларидаги роли ва имкониятлари ўрганилади. Кибермакондаги таҳдидларнинг кўплиги ва мураккаблиги анъанавий ҳимоя чоралари билан курашишни мураккаблаштираётгани таъкидланади. Мақолада киберхавфсизлик соҳасидаги баъзи муаммолар таҳлили, сунъий интеллект имкониятлари, амалий ечимлар ва таклифлар ҳамда хулосалар келтирилган.

Калит сўзлар: киберхавфсизлик, сунъий интеллект, киберҳужумлар, аномалия аниқлаш, хавфсизлик технологиялари.

Аннотация: В данной статье рассматриваются роль и возможности искусственного интеллекта в вопросах обеспечения кибербезопасности. Отмечается, что многочисленность и сложность угроз в киберпространстве усложняют борьбу с традиционными мерами защиты. В статье представлен анализ некоторых проблем в области кибербезопасности, возможности искусственного интеллекта, практические решения, предложения и выводы.

Ключевые слова: кибербезопасность, искусственный интеллект, кибератаки, обнаружение аномалий, технологии безопасности.

Abstract: This article examines the role and capabilities of artificial intelligence in ensuring cybersecurity. It is noted that the multiplicity and complexity of threats in cyberspace complicate the fight against traditional protection measures. The article provides an analysis of some problems in the field of cybersecurity, the possibilities of artificial intelligence, practical solutions and suggestions, as well as conclusions.

Keywords: cybersecurity, artificial intelligence, cyberattacks, anomaly detection, security technologies.

Жаҳонда юз бераётган геосиёсий воқеалар, яъни асосий “куч марказлари” ўртасидаги қарама-қаршиликларнинг кескинлашуви, халқаро ахборот хавфсизлигини таъминлаш платформасида ҳам жиддий ўзгартиришлар киритилишига сабаб бўлмоқда. Ушбу ҳолатлар Ўзбекистон Республикаси ахборот инфратузилмаси киберхавфсизлигини таъминлашга мос равишда ташкилий ва техник қарорлар қабул қилинишига таъсир кўрсатувчи глобал омил сифатида юзага чиқмоқда.

Кибермаконда содир этилаётган турли таҳдид ва киберҳужумлар анъанавий бўлган хавфсизлик воситаларини қайсидир маънода чеклайди, сабаби жуда катта ҳажмдаги маълумотларни доимий тарзда қайта ишлашни талаб этади.

“Киберхавфсизлик маркази” давлат муассасасининг ўтган 2025 йил фаолияти бўйича ҳисоботидан келиб чиққан ҳолда фикр юритадиган бўлсак, республикада ахборот тизим ва ресурслари, муҳим ахборот инфратузилмаси объектларида сақланаётган, қайта ишланаётган маълумотларга нисбатан уюштирилаётган зарарли тармоқ сўровлари сезиларли даражада ошган.

Аниқланган заифликлар, шу жумладан, веб-сайтга “DDoS” ҳамда “Bruteforce” хужумлари уюштирилиши, ресурс контентини ўзгартириш, маълумотларни ўғирланиши ва сайтдан “фишинг” мақсадларида фойдаланиш, SQL-инъекция орқали маълумотлар базасидаги маълумотларнинг қўлга киритилиши, шахсга доир маълумотлар сақланаётган файллар, пароллар, пластик карта маълумотларига оид файлларга рухсатсиз кириш, юклаб олиш, маълумотлар устида рухсат этилмаган амалларни бажариш каби оқибатларга олиб келиши мумкин.

Таҳдидлар сони ва уларнинг турли даражада мураккаблигини ошириши туфайли анъанавий ҳисобланган ҳимоя чоралари тобора етарли бўлмай қолмоқда. Рақамли инфратузилма ва трансформация масалаларининг кенгайиши, булутли технология ва IoT (Internet of Things) қурилмаларининг кенг жорий этилиши ҳам кибертаҳдид ва хуружлар векторини кенгайтиради.

Ўзбекистон Республикаси Президентининг 2026 йил 10 мартдаги

ПФ-38-сон Фармони билан тасдиқланган Ўзбекистон Республикасининг Киберхавфсизлик стратегияси ва кибержиноятчиликнинг олдини олиш тизимини такомиллаштиришга қаратилган меъёрий-ҳуқуқий ҳужжатда миллий кибербарқарорликни мустаҳкамлаш, муҳим ахборот ва давлат рақамли инфратузилмасини ҳимоя қилиш, киберхавфларни тизимли равишда камайтириш ва фуқаролар, хусусий сектор ва давлатнинг рақамли хавфсизлиги даражасини ошириш, кибержиноятчиликка қарши фаол курашиш, рақамли инновациялар, сунъий интеллект технологияларини ривожлантириш ва киберхавфсизлик соҳасида технологик мустақилликни мустаҳкамлаш каби устувор йўналишлар белгиланган.

Бу эса мамлакатда киберхавфсизликни мустаҳкамлашнинг стратегик зарурат эканини кўрсатади. Шу билан бирга, мавжуд технологияларнинг такомиллаштирилиши ва янги инновацион усулларни жорий қилиш талаб этилади. Ҳужжатдан бевосита кўришимиз мумкин, сунъий интеллект технологияларини ривожлантириш баробарида киберхавфсизликни таъминлаш масалаларида уларнинг ўрни ва ролини ошириш зарур.

Сунъий интеллект (СИ) – инсон кўникмаларини қайта ишлаб чиқариш учун мўлжалланган дастурлар тўплами ҳисобланади. Сунъий интеллект мавжуд муаммоларга ечим топиш, режалаштириш, билим олиш, ўз устида ишлаш каби вазифаларни ўз вақтида ва тўлиқ бажаришга ёрдам берадиган қобилиятдир. Умуман олганда, СИ олинган маълумотлар асосида муайян ҳулосалар чиқаришга қодир бўлган моделлар ва усуллар тўпламидир.

Киберхавфсизлик соҳасида СИ катта ҳажмидаги маълумотларни автоматик таҳлил қилиш имконини беради. У трафик ва тизим хатти-ҳаракатларида маскаланган нақшларни (паттерн) топиб, потентсиал таҳдидлар ёки камчиликларни инсон имкониятидан тезроқ аниқлай олади. Масалан,

СИ асосидаги тизимлар реал вақтда киритилаётган маълумотларни солиштириш ва машиналарни ўргатиш усуллари орқали билдирилмаган таҳдидларни (аномалияларни) юқори аниқлик билан ажратиб беради. Бу эса false positive - нотўғри огоҳлантиришлар ва false negative - жиддий таҳдидларни илғамаган ҳолатларнинг сонини сезиларли даражада камайтиришга ёрдам беради.

СИ доимий ўрганиш (machine learning) имконияти туфайли янги пайдо бўлаётган таҳдидлардан сабоқ олиб, хужум усулларига мослаша олади. Киберхавфсиз соҳасида СИ ечимлари таҳдидларни эрта аниқлаш, тезкор жавоб бериш ва умуман тизим хавфсизлик

ҳолатини яхшилашга ҳамда тизимни олдиндан чора кўришга имкон беради. Шу тарзда, СИ замонавий киберхавфсизликдаги мунофаа ва ҳужум ёндашувларини, ҳимояни тармоқ ва тизим ресурслари бўйлаб кенгайтиришга имкон яратади.

СИдан фойдаланишнинг асосий афзалликларидан яна бири киберхавфсизлик бўйича қайта-қайта такрорланадиган вазифаларни автоматлаштиришдир. СИ ёрдамида хавфсизлик тизимлари ўз-ўзини бошқариш даражасига эриша бошлайди, яъни таҳдид аниқланса, тизим керакли жавобни ходим иштирокисиз бажариши мумкин. Бунинг натижасида, мураккаб таҳдидларни таҳлил қилиш ва инновацион ечимлар ишлаб чиқишга эътибор кўпроқ қаратилади.

Киберхавфсизликда СИНинг реал қўлланилишига мисоллар сифатида қуйидаги амалий тизимлар ва технологияларни кўрсатиш мумкин:

Илғор тармоқ хавфсизлик деворлари (NGFW) – трафик оқимларини назорат қилувчи деворлар оддий қоидалар ўрнига СИ ёрдамида таҳдидлар ҳақидаги маълумотларни йиғи ва янги киберхавфларни аниқлайди. Улар трафикдаги шубҳали нақшларни автоматик аниқлаб, тегишли равишда блоклаш ёки огоҳлантириш чораларини кўриши мумкин.

Endpoint (тузун) хавфсизлик ечимлари – компьютер, смартфон ва IoT каби қурилмаларни ҳимоя қилувчи дастурлар ҳам СИдан фойдаланади. Улар қурилмаларда ишлаётган дастур ва операцион тизимларни таҳлил қилиб, эскирган ва заиф элементларни ҳамда ўрнатилган зарарли кодларни аниқлайди. Ҳужум аниқланганда СИ дарҳол таҳдид манбаини изоляция қилади ёки четлатади.

Тармоқдаги ҳужумларни аниқлаш ва олдини олиш тизимлари (IDS/IPS) – бу воситалар тармоқ трафикини кузатиб, номақбул ҳаракатларни олдиндан аниқлашга қаратилган. СИ уларнинг сезувчанлигини ошириб, катта ҳажмли лог (журнал)ларни таҳлил қилади ва рухсатсиз кириш ҳаракатларини блоклайди ҳамда ҳужумни давом этишидан олдин бартараф этади.

Булутли инфратузилмалар хавфсизлиги – кўп сонли булутли хизматлар ва маълумот марказларида СИ таҳлил қуввати зарур. СИ булутдаги барча манбалардан келаётган маълумотларни йиғиб, уларни таҳлил қилади, заифликлар ва потентсиал киберҳужумларни аниқлайди ҳамда хавфсизлик бўйича глобал манзара тасвирини шакллантиради.

IoT (Internet of Things) хавфсизлиги – корхоналарда кўплаб саноат ва уй-рўзгор IoT қурилмалари ишлатилади. СИ ёрдамида ҳар бир IoT қурилмаси ҳолати таҳлил қилинади: трафикда ёки хатти-ҳаракатларда оддийдан четга чиқиш ҳолати аниқланса, у бошқалардаги ўхшаш нақшлар билан солиштирилади. Бу масалан, битта қурилма ҳузурини бузган бўлса, тезда бошқа қурилмаларга қарши ҳужумни олдиндан огоҳлантиради.

XDR ва SIEM платформалари – кенгайтирилган таҳдидларни аниқлаш (XDR) ва хавфсизлик маълумотларини бошқариш (SIEM) тизимлари турли маҳсулотлар ва манбалардан (логс, таҳдид хабарлар базаси ва бошқ.) маълумот тўплайди. СИ бу маълумотни бирлаштириб таҳлил қилади, ташқи таҳдид омилларини ҳам ҳисобга олган ҳолда атрофли таҳлиллар ҳосил қилади ва корхона ёки ташкилот хавфсизлик ҳолати бўйича кенг қўламли тасаввур беради.

Юқоридаги технологиялар корхона ва давлат органларида хавфсизлик инфраструктураси сифатини сезиларли даражада оширади. Улардан фойдаланиш

тизимларни ҳимоя қилишда тез-тез учрайдиган вазифаларни автоматлаштиради ва ходимларни киберхавфли вазиятларга эътибор қаратишга имкон яратади.

Шу тариқа, киберхавфларга қарши курашишда СИ муҳим имкониятлар тақдим этади. СИ маълумотларни таҳлил қилиш ва таҳдидларни аниқлашни сезиларли даражада тезлаштиради, бу эса анъанавий усуллар ёрдамида амалга ошириб бўлмайдиган таҳдидларга қарши самарали жоралар кўрсатишга ёрдам беради. Амалий ечимлар (NGFW, EDR, IDS/IPS, булут ва IoT ҳимояси, XDR/SIEM ва бошқ.) Шу билан бирга, ишончли ва маълумотга асосланган ёндошувлар ёрдамида СИ тизимларининг ўзини ҳам ҳимоя қилиш механизмларини яратиш талаб этилади. Хулоса ўрнида айтиш мумкинки, киберхавфлардан ҳимояда СИдан оқилона фойдаланиш миллий ва корпоратив хавфсизлик салоҳиятини янги поғонага олиб чиқади.

Фойдаланилган адабиётлар:

1. А.Б.Менисов Киберщит. Искусственный интеллект
2. и кибербезопасность. EDP Hub. – 2024. – 162 с.
3. С.И.Самыгин, А.В.Кузнецова Искусственный интеллект
4. и информационная безопасность общества. Монография. – М., - 2025. – 118 с.
1. А.Б.Менисов Киберщит. Искусственный интеллект
2. и кибербезопасность. – М., - 2024 – 189 с.
4. Russell, S., & Norvig, P. Artificial Intelligence: A Modern Approach. Pearson, 2021.
5. Goodfellow, I., Bengio, Y., & Courville, A. Deep Learning. MIT Press, 2016.
6. Kshetri, N. Cybersecurity and Artificial Intelligence: The Next Frontier. Springer, 2022.