СУНЪИЙ ИНТЕЛЛЕКТ ВОСИТАСИДА АМАЛГА ОШИРИЛАЁТГАН КИБЕРЖИНОЯТЛАР: ЯНГИ ШАКЛЛАР ВА УЛАРНИНГ ХАВФИ

Қобилов Шокир Анварович

Ўзбекистон Республикаси Президенти Ҳузуридаги

Ижтимоий ҳимоя миллий Агентлиги

Янгиҳаѐт тумани Инсон ижтимоий хизматлар

маркази ҳуқуқий масалаларда эксперт маслаҳатчиси

Аннотация:Ушбу мақолада сунъий интеллект (СИ) технологияларининг жадал ривожланиши натижасида юзага келаётган кибержиноятларнинг янги ва хавфли шакллари таҳлил қилинади. Хусусан, deepfake технологиялари, автоматлаштирилган ботлар, фишинг ҳужумлари ва зарарли дастурлар (malware, ransomware) каби СИ асосидаги воситалар орқали амалга оширилаётган жиноятлар мисолида глобал киберхавфсизлик тизимларининг мураккаблиги ва уларга қарши курашишдаги қийинчиликлар ёритиб берилади. Мақолада ушбу жиноятларнинг ижтимоий, иқтисодий ва сиёсий оқибатлари, жумладан, жамоатчилик ишончини йўқотиш, иқтисодий барқарорликка путур етказиш ва миллий ҳамда халқаро сиёсий муносабатларга салбий таъсири кенг қамровда кўриб чиқилади. Шу билан бирга, СИ'нинг ўзига хос икки томонлама табиати, яъни унинг ҳам ижобий, ҳам салбий таъсири ҳақида фикр юритилади. Муаммонинг ечими сифатида СИ технологияларидан киберхавфсизликни мустаҳкамлашда фойдаланиш, замонавий қонунчилик ислоҳотлари олиб бориш, трансмиллий ҳамкорликни кучайтириш, киберхавфсизлик мутахассисларини тайёрлаш ва кенг жамоатчиликни хабардор қилиш каби комплекс ёндашувлар таклиф этилади. Мақола, айни пайтда, янги таҳдидларга қарши самарали ва тизимли жавоб бериш механизмларини шакллантиришга доир илмий-амалий асосларни муҳокама қилади.

Калит сўзлар: сунъий интеллект (СИ), кибержиноятлар, deepfake технологияси, автоматлаштирилган ботлар, фишинг ҳужумлари, зарарли

дастурлар, ransomware, ахборот манипуляцияси, ижтимоий муҳандислик, киберхавфсизлик, маълумотлар ҳимояси, глобал таҳдидлар, қонунчилик ислоҳотлари, трансмиллий жиноятлар, жамоатчилик хабардорлиги, рақамли хавфсизлик, ахборот хуружлари, миллий хавфсизлик, киберҳужум, ижтимоий барқарорлик, иқтисодий оқибатлар

CYBERCRIMES COMMITTED BY ARTIFICIAL INTELLIGENCE: NEW FORMS AND THEIR DANGER

Kabilov Shokir Anvarovich

National Agency for Social Protection under the President of the Republic of Uzbekistan

Yangihayot District Human Social Services Center Expert Advisor on Legal Issues

Annotation: This article analyzes new and dangerous forms of cybercrimes emerging as a result of the rapid development of artificial intelligence (AI) technologies. In particular, the complexity of global cybersecurity systems and the difficulties in combating them are highlighted on the example of crimes committed using AI-based tools such as deepfake technologies, automated bots, phishing attacks, and malicious programs (malware, ransomware). The article comprehensively examines the social, economic and political consequences of these crimes, including the loss of public trust, the undermining of economic stability and the negative impact on national and international political relations. At the same time, it reflects on the unique dual nature of IS, that is, its positive and negative impact. As a solution to the problem, comprehensive approaches are proposed, such as the use of IS technologies to strengthen cybersecurity, modern legislative reforms, strengthening transnational cooperation, training cybersecurity specialists and informing the general public. The article also discusses the scientific and practical foundations for the formation of effective and systematic response mechanisms to new threats.

Keywords: artificial intelligence (AI), cybercrime, deepfake technology, automated bots, phishing attacks, malware, ransomware, information manipulation, social engineering, cybersecurity, data protection, global threats, legislative reforms, transnational crimes, public awareness, digital security, information attacks, national security, cyberattack, social stability, economic consequences

КИБЕРПРЕСТУПНОСТЬ, РАЗВИВАЮЩАЯСЯ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: НОВЫЕ ФОРМЫ И ИХ РИСКИ

Кабилов Шокир Анварович

В присутствии Президента Республики Узбекистан

Национальное агентство социальной защиты

Район Янгихает Социальные услуги

Центр является экспертом-консультантом по юридическим вопросам

Аннотация: В статье анализируются новые и опасные формы киберпреступности, возникающие в результате быстрого развития технологий искусственного интеллекта (ИИ). В частности, сложность глобальных систем кибербезопасности и трудности борьбы с ними подчеркиваются примерами преступлений, совершаемых с использованием инструментов на основе искусственного интеллекта, таких как технологии deepfake, автоматизированные боты, фишинговые атаки и вредоносные программы (вредоносное ПО, программы-вымогатели). В статье дается всесторонний обзор социальных, экономических и политических последствий этих преступлений, включая потерю общественного доверия, экономическую нестабильность и негативное влияние на национальные и международные политические отношения. При этом учитывается уникальная двойственная природа СИ, то есть ее как положительные, так и отрицательные эффекты. В качестве решения проблемы предлагаются комплексные подходы, такие как использование технологий искусственного интеллекта для усиления кибербезопасности, проведение современных законодательных реформ,

укрепление транснационального сотрудничества, обучение специалистов по кибербезопасности, информирование широких слоев населения. В статье также рассматриваются научные и практические основы формирования эффективных и системных механизмов реагирования на новые угрозы.

Ключевые слова: искусственный интеллект (ИИ), киберпреступность, технология deepfake, автоматизированные боты, фишинговые атаки, вредоносное ПО, программы-вымогатели, манипуляция информацией, социальная инженерия, кибербезопасность, защита данных, глобальные угрозы, законодательные реформы, транснациональные преступления, осведомленность общественности, цифровая безопасность, информационные атаки, национальная безопасность, кибератака, социальная стабильность, экономические последствия

Сунъий интеллект (СИ) технологиялари XXI асрнинг энг муҳим ихтироларидан бири сифатида инсоният ҳаётининг деярли барча жабҳаларини тубдан ўзгартирди. Тиббиётда аниқ ташхис қўйишдан тортиб, автоном транспорт воситаларини бошқариш, молиявий бозорларни таҳлил қилиш ва таълим тизимларини шахсийлаштиришгача бўлган соҳаларда СИ ўзининг мисли кўрилмаган самарадорлигини намоён этди. Ушбу технологиялар инсон меҳнатини оптималлаштириб, иқтисодий ўсишга ва ижтимоий фаровонликка хизмат қилмоқда. Бироқ, ҳар қандай кучли восита сингари, СИ ҳам икки томонлама табиатга эга. Унинг жадал ривожланиши билан бирга, кибержиноятчиларга янги имкониятлар очиб берди, бу эса глобал хавфсизликка жиддий таҳдид солмоқда. СИ воситасида амалга оширилаётган кибержиноятларнинг янги шакллари нафақат анъанавий хавфсизлик тизимларини четлаб ўтишга қодир, балки ижтимоий ишончни йўқотиш, иқтисодий барқарорликка путур етказиш ва сиёсий жараёнларга аралашиш орқали глобал миқёсда беқарорликни келтириб чиқармоқда. Ушбу мақола СИ асосидаги кибержиноятларнинг замонавий кўринишлари, уларнинг ижтимоий-иқтисодий оқибатлари, хавф даражаси ва уларга қарши курашиш

йўлларини кенгроқ таҳлил қилишга бағишланади. Мақола СИ технологияларининг киберхавфсизликка таъсирини чуқур ўрганиш орқали ушбу муаммонинг кўлами ва уни ечишда дуч келинаётган муаммоларни ёритишга ҳаракат қилади.

СИ технологиялари кибержиноятчиларга мисли кўрилмаган имкониятлар яратди.

СИ асосидаги кибержиноятларнинг яна бир хавфли шакли – бу deepfake технологиялари. Чуқур ўқитиш алгоритмлари ёрдамида яратилган сохта аудио ва видео материаллар кибержиноятчилар томонидан шантаж, молиявий фирибгарлик, ижтимоий муҳандислик ва ҳатто сиёсий манипуляциялар учун қўллнилмоқда. Масалан, СИ ёрдамида тузилагн сохта аудио орқали корпорация раҳбарининг овози тақлид қилиниб, ходимларга катта миқдорда пул ўтказиш буйруғи берилиши мумкин. Бундай ҳолатлар АҚШ, Европа Иттифоқи ва Осиё мамлакатларида 2023 ва 2024-йилларда бир неча бор қайд этилган бўлиб, молиявий йўқотишлар юз миллионлаб долларга етган. Deepfake'ларнинг хавфи шундаки, улар инсон кўзи ва қулоғига табиий кўринади ва анъанавий хавфсизлик тизимлари уларни аниқлашда қийналди. Ҳозирги кунда deepfake технологиялари шу даражада ривожланганки, ҳатто тажрибали мутахассислар ҳам сохта контентни ҳақиқийдан фарқлашда қийинчиликка дуч келмоқда. Бундан ташқари, deepfake'лар ижтимоий тармоқларда оммавий ахборот воситаларига таъсир қилиш, жамоатчилик фикрини манипуляция қилиш ёки шахсларнинг обрўсига путур етказиш учун ҳам ишлатиламоқда. Масалан, сохта видеолар орқали таниқли шахсларнинг сўзлари ёки ҳаракатлари нотўғри талқин қилиниб, ижтимоий низолар ёки оммавий тартибсизликлар келтириб чиқарилиши мумкин.

СИ'нинг кибержиноятларда қўлланишининг муҳим йўналишларидан бири – бу автоматлаштирилган ботлар ва зарарли дастурлар (malware). СИ асосидаги ботлар ижтимоий тармоқларда дезинформация тарқатиш, жамоатчилик фикрини манипуляция қилиш, сайлов жараёнларига аралашиш

ёки ҳатто онлайн платформаларда оммавий троллинг кампанияларини ташкил қилиш учун ишлатилади. Бу ботлар фойдаланувчиларнинг ёзиш усулби, нутқ хусусиятлари ва ижтимоий одатларини тақлид қилиб, уларни ҳақиқий одамлардан фарқлашни деярли имконсиз қилади. Масалан, 2024-йилда бир қатор мамлакатларда СИ асосидаги ботлар орқали сохта янгиликлар тарқатилиб, иқтисодий бозорларда паник сотиш (panic selling) ҳолатлари юзага келган. Бундан ташқари, СИ ёрдамида ишлаб чиқилган зарарли дастурлар хавфсизлик тизимларининг тузилишини ўрганиб, уларнинг заиф нуқталарини аниқлай олади ва ҳужумни мослаштиради. Бундай дастурлар, масалан, ransomware (тўлов талаб қилувчи дастурлар) сифатида ишлатилиб, муҳим инфратузилмаларга, шу жумладан, соғлиқни сақлаш, энергетика ва транспорт тизимларига зарар етказмоқда. 2023-йилда СИ асосидаги ransomware ҳужумлари глобал миқёсда 20% га ошган бўлиб, бу эса кибержиноятчиларнинг технологик жиҳатдан қанчалик ривожланганлигини кўрсатади.

СИ асосидаги кибержиноятларнинг хавфи нафақат уларнинг техник мураккаблигида, балки ижтимоий-иқтисодий ва сиёсий оқибатларида ҳам намоён бўлади. Молиявий фирибгарликлар кичик ва ўрта бизнесга жиддий зарар етказмоқда, чунки улар СИ асосидаги ҳужумларнинг мураккаблигига қарши туриш учун етарли ресурсларга эга эмас. Катта корпорациялар эса маълумотлар оқиши, интеллектуал мулкнинг ўғирланиши ва операцион жараёнларнинг бузилиши туфайли миллиардлаб доллар йўқотмоқда. Масалан, 2024-йилда СИ ёрдамида амалга оширилган маълумотлар оқиши туфайли глобал технология компаниялари ўртача 4,5 миллиард доллар зарар кўрган. Ижтимоий жиҳатдан, deepfake ва дезинформация кампаниялари жамоатчилик ишончини йўқотишга, ижтимоий низоларни келтириб чиқаришга ва ҳатто миллий хавфсизликка таҳдид солмоқда. Сиёсий нуқтаи назардан, СИ асосидаги кибержиноятлар давлатлараро муносабатларга путур етказиши, халқаро ишончсизликни кучайтириши ва глобал барқарорликка хавф

туғдириши мумкин. Масалан, сохта видеолар ёки аудио материаллар орқали давлат раҳбарларининг сўзлари манипуляция қилиниб, дипломатик можаролар келтириб чиқарилган ҳолатлар қайд этилган.

Ушбу таҳдидларга қарши курашиш учун бир қатор стратегиялар ишлаб чиқилмоқда, аммо муаммонинг мураккаблиги туфайли бу жараён секин кечмоқда. Биринчи навбатда, СИ технологияларининг ўзи киберхавфсизликни мустаҳкамлаш учун қўллнилмоқда. Масалан, аномалияларни аниқлаш алгоритмлари СИ ёрдамида тармоқдаги ғайритабиий фаолиятни аниқлай олади, бу эса потенциал ҳужумларнинг олдини олишга ёрдам беради. Шунингдек, deepfake'ни аниқлаш учун махсус СИ асосидаги дастурлар ишлаб чиқилмоқда, улар сохта контентни таҳлил қилиб, унинг ҳақиқийлигини баҳолайди. Бироқ, бу технологиялар ҳали ҳам кибержиноятчиларнинг СИ асосидаги ҳужумларидан бир қадам ортда қолмоқда, чунки жиноятчилар доимий равишда янги усуллар ва алгоритмларни ишлаб чиқмоқда. Технологик ечимлардан ташқари, қонунчилик ислоҳотлари ҳам зарур. Кўпгина мамлакатларда кибержиноятларга қарши қонунлар ҳали ҳам эскирган бўлиб, улар СИ асосидаги жиноятларнинг мураккаблигини ҳисобга олмайди. Халқаро ҳамкорликнинг сустлиги эса муаммони янада чуқурлаштирмоқда, чунки кибержиноятлар кўпинча трансмиллий хусусиятга эга. Масалан, бир мамлакатда жойлашган сервер орқали бошқа мамлакатдаги фойдаланувчиларга ҳужум уюштирилши мумкин, бу эса жиноятчиларни аниқлаш ва жавобгарликка тортишни қийинлаштиради.

Киберхавфсизлик соҳасида малакали мутахассисларнинг етишмаслиги ҳам жиддий муаммо сифатида қолмоқда. СИ асосидаги кибержиноятларга қарши курашиш учун нафақат технологик билимлар, балки психология, ижтимоий муҳандислик ва ҳуқуқий жиҳатларни чуқур тушуниш талаб этилади. Ҳозирги кунда глобал миқёсда киберхавфсизлик мутахассисларига бўлган эҳтиёж 3 миллиондан ортиқни ташкил қилади, бу эса бўшлиқни тезда тўлдириш имконсиз эканлигини кўрсатади. Шу билан бирга, жамоатчилик

хабардорлигини ошириш ҳам муҳим аҳамиятга эга. Фойдаланувчиларнинг аксарияти СИ асосидаги фишинг ҳужумлари ёки deepfake’ларнинг хавфини тўлиқ англамайди, бу эса уларни осон нишонга айлантиради. Оммавий ахборот воситалари, таълим муассасалари ва давлат ташкилотлари киберхавфсизлик бўйича кенг кўламли маърифий кампаниялар олиб бориши зарур.

Хулоса қилиб айтганда, сунъий интеллект воситасида амалга оширилаётган кибержиноятлар замонавий дунёнинг энг мураккаб ва кўп қиррали таҳдидларидан биридир. Мослаштирилган фишинг ҳужумлари, deepfake технологиялари, автоматлаштирилган ботлар ва зарарли дастурлар нафақат анъанавий хавфсизлик тизимларини синовдан ўтказмоқда, балки ижтимоий ишончни йўқотиш, иқтисодий барқарорликка путур етказиш ва сиёсий жараёнларни бузиш орқали глобал миқёсда катта хавф-хатарларни келтириб чиқармоқда. Ушбу таҳдидларга қарши курашиш учун фақат технологик ечимларMover етарли эмас. Илғор СИ асосидаги хавфсизлик тизимлари билан бир қаторда, замонавий қонунчилик ислоҳотлари, халқаро ҳамкорликни кучайтириш, малакали киберхавфсизлик мутахассисларини тайёрлаш ва жамоатчилик хабардорлигини ошириш каби комплекс ёндашув зарур. СИ технологиялари инсоният учун чексиз имкониятлар очган бўлса-да, унинг салбий оқибатларини минималлаштириш ва жамиятни ушбу хавф-хатарлардан ҳимоя қилиш учун глобал миқёсда бирга ҳаракат қилиш муҳимдир. Фақат шу йўл билан СИ’нинг ижобий салоҳиятидан тўлиқ фойдаланиш ва унинг кибержиноятлардаги хавфли таъсирини бартараф этиш мумкин бўлади. Келажакда ушбу муаммони ҳал қилиш нафақат технологик ривожланишга, балки инсониятнинг ахлоқий ва ҳуқуқий масъулиятига ҳам боғлиқ бўлади.

Фойдаланилган адабиётлар рўйхати

1. А. Икромов. "Кибержиноятлар ва уларга қарши курашишнинг асосий принциплари." Тошкент: "Иқтисодий тараққиёт", 2022. – 320 б.
2. М. Жўраев. "Сунъий интеллект ва киберхавфсизлик." Тошкент: "Техника ва инновациялар", 2023. – 245 б.
3. Б. Давлатов. "Интернет хавфсизлиги: Янгиликлар ва таҳдидлар." Тошкент: "Ахборот технологиялари", 2021. – 185 б.
4. Н. Ахмедов. "Киберхавфсизлик ва интернет технологиялари." Тошкент: "Маърифат", 2020. – 267 б.
5. Ш. Абдуллаев. "Deepfake ва оммавий ахборот воситалари манипуляцияси." Тошкент: "Ижтимоий психология", 2022. – 212 б.
6. И. Усмонов. "Сунъий интеллект: таҳдид ва имкониятлар." Тошкент: "Математика ва фан", 2021. – 310 б.