

КИБЕРТАХДИДЛАР ШАРОИТИДА КИБЕРХАВФСИЗЛИКНИ ТАЪМИНЛАШ

Арипов Алишер Сайфиддинович,

Навоий вилояти Ички ишлар бошқармаси

Кибержиноятларга қарши курашиш бошқармаси ходими

E-mail: alisher7888aripov@gmail.com

https://orcid.org/0009-0005-1409-6482

Рақамли ахборот маконининг ривожланиши кибертахдидларнинг сифат жиҳатидан янги босқичга ўтишини таъминлади. Ушбу эволюция учта асосий парадигмал босқичдан ўтади:

Биринчи босқич: Детерминистик босқич (Статик кодлар): Хужумлар олдиндан ёзилган статиклар (скриптлар, содда вируслар) орқали, инсон (хакер)нинг бевосита бошқаруви ва назорати остида амалга оширилади.

Иккинчи босқич: Автоматлаштирилган босқич (Ботнетлар ва эксплойтлар): Тармоқ аномалияларидан фойдаланувчи, лекин алгоритмик чекланган ва ўзгарувчан муҳитга мослаша олмайдиган тизимлар пайдо бўлади.

Учинчи босқич: Кобнотив-автоном босқич (СИ ва Нейротармоқлар): Диффузион моделлар, генератив-мусобақалашувчи тармоқлар (GAN) ва мустақил қарор қабул қилувчи автоном агентлар (AI agents) негизидаги киберхужумлар.

Замонавий СИ-кибертахдидлари ўзини ўзи ўргатувчи (*Self-learning*) ва кодларини реал вақтда мутация қилувчи (*Polymorphic/Metamorphic AI malware*) хусусиятга эга бўлиб, анъанавий киберҳимоя (SIEM ва SOC) тизимларини четлаб ўтиш имкониятини яратади.

Онтологик нуқтаи назардан СИ-кибертахдидлари оддий «техник қурол» чегарасидан чиқиб, **когнитив ва алгоритмик автономлик** феноменини намоён этади.

Алгоритмик субъектлик ва инсон омилининг узилиши (*Human-out-of-the-loop*): СИ-агентлар киберхужум жараёнида инсоннинг бевосита буйруғисиз нишонни танлаш, заифликларни аниқлаш ва ҳужум векторини ўзгартириш қарорини қабул қилади. Бу эса таҳдид манбаининг онтологик мақомини (инсоннинг иродавий ҳаракатидан алгоритмнинг автоном қарорига) ўзгартиради.

Синтетик ва гибрид воқеликнинг яратилиши: Deepfake ва овозли синтез (Audio Deepfake) орқали ижтимоий инженерия ҳужумлари когнитив даражада содир этилади. Бунда таҳдид муҳитнинг ўзини ва ахборотни алгоритмик сохталаштириш негизида юзага келади.

Сунъий интеллект ва автоном тизимлар инсоннинг бевосита иродавий иштирокисиз зарар етказиши мумкин. Бу ҳолатда асосий ҳуқуқий муаммо айб ва жавобгарликни кимга юклаш масаласидир. Жавобгарликни дастурчи (Developer), оператор (Operator) ёки СИ тизими (AI System) зиммасига юклаш масаласи мавжуд бўлиб, амалдаги ҳуқуқда СИ мустақил ҳуқуқ субъекти ҳисобланмаслиги ушбу муаммони янада мураккаблаштиради.

СИ томонидан юзага келтирилувчи кибертахдидларга қарши ҳуқуқий механизмларни шакллантириш учун қуйидаги стратегик йўналишлар таклиф этилади:

1. **ЖПК ва ЖКга алгоритмик криминал масъулият нормаларини киритиш:** СИ тизимларини кибержиноят қуроли сифатида ишлатганлик учун оғирлаштирувчи ҳолатларни белгилаш ва СИ орқали содир этилган киберхужумларда мажбурий СИ-алгоритмик экспертизасини жорий этиш.

2. **«Strict Liability» (Қатъий жавобгарлик) принципини қўллаш:** Юқори хавfli автоном СИ тизимларини яратувчи ва жорий этувчи субъектлар зиммасига, уларнинг айбидан қатъи назар, юзага келган киберзарар учун қатъий ҳуқуқий жавобгарлик юклаш.

3. **«Digital Chain of Custody» ва Блокчейн реестрини рақамлаштириш:** Автоном тизимларнинг хатти-ҳаракатлари ва рақамли изларини (log-файллар) ўзгармас электрон журналларда криптографик хешлаш орқали сақлаш тартибини қонунан мустаҳкамлаш.

СИ ва автоном тизимлар юзага келтираётган кибертахдидлар рақамли ҳуқуқ ва киберхавфсизлик доктринасини тубдан қайта кўриб чиқишни талаб қилади. Кибертахдидларнинг онтологик ўзгариши (инсон иродасидан автоном алгоритмга ўтиши) ҳуқуқий феноменологияда янги институтлар: алгоритмик экспертиза, қатъий деликт жавобгарлиги ва рақамли далилларнинг криптографик аслилигини таъминлаш каби механизмларни қонунчиликда зудлик билан мустаҳкамлашни тақозо этмоқда.

Фойдаланилган адабиётлар рўйхати

1. Ўзбекистон Республикасининг «Киберхавфсизлик тўғрисида»ги Қонуни, 2022 йил 15 апрель, ЎРҚ-764-сон.
2. Ўзбекистон Республикаси Президентининг «Рақамли Ўзбекистон — 2030» стратегиясини тасдиқлаш тўғрисида»ги Фармони.
3. Ўзбекистон Республикасининг Маъмурий жавобгарлик тўғрисидаги кодекси (амалдаги таҳрирда).
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

5. ENISA Threat Landscape Report 2024–2026. — European Union Agency for Cybersecurity.
6. NIST AI Risk Management Framework (AI RMF 1.0). — National Institute of Standards and Technology, 2023.
7. Cybersecurity Act of Singapore, 2018 (with subsequent amendments).
8. Каримов А.А. Рақамли иқтисодиёт шароитида киберхавфсизликни таъминлашнинг ҳуқуқий асослари: монография. — Тошкент: ТДЮУ, 2023.
9. Bathaee Y. The Artificial Intelligence Black Box and the Failure of Intent and Causation // Harvard Journal of Law & Technology. — 2018. — Vol. 31, No. 2.
10. Brundage M. et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. — Future of Humanity Institute, 2018.