



РАҚАМЛИ ТРАНСФОРМАЦИЯ ВА СИ АЛГОРИТМЛАРИНИНГ
ОММАЛАШУВИ ШАРОИТИДА КИБЕРХАВФСИЗЛИКНИ
ТАЪМИНЛАШ

Арипов Алишер Сайфиддинович,

Навоий вилояти Ички ишлар бошқармаси

Кибержсиноятларга қарши курашиш бошқармаси ходими

E-mail: alisher7888aripov@gmail.com

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

Рақамли трансформация ва СИ алгоритмларининг оммалашуви киберхужумларнинг мураккаблик даражасини ва зарар етказиш миқёсини геометрик прогрессияда оширди. Ушбу таҳдидлар мазмунан қуйидагича турланади:

1. Deepfake (Синтетик медиа-сохталаштириш): Генератив-мусобақалашувчи тармоқлар (GAN) ва диффузион моделлар ёрдамида давлат арбоблари, мудофаа ва хавфсизлик тизими раҳбарларининг аудио ва видео тасвирларини юқори аниқликда сохталаштириш.

2. AI-driven Phishing (СИ назоратидаги фишинг): Катта тил моделлари (LLM) орқали муайян шахснинг рақамли изларини (маълумотлар базаси, ижтимоий тармоқлар) ўрганган ҳолда таржима ва контекст хатоларисиз, психологик мослашган, ўта юқори самарадорликка эга фишинг хабарларини автоматлаштирилган тарзда генерация қилиш.

3. Алгоритмик фирибгарлик: Финанс ва капитал бозорларида СИ алгоритмларини манипуляция қилиш, юқори частотали савдо (*High-Frequency Trading*) тизимларига сохта сигналлар юбориш ёки банклардаги идентификация тизимларини алгоритмик айланиб ўтиш.



4. Автоном киберхужумлар: Инсон аралашувисиз (*Human-out-of-the-loop*) нишон тизимларни сканерловчи, полиморф/метаморф кодлар орқали ҳимоя воситаларини четлаб ўтувчи ва нозик нуқталарни бевосита зарарловчи автоном кибер-куроллар (AI agents).

Янги авлод кибертаҳдидлари давлат хавфсизлигининг ягона контурига комплексли хавф туғдиради ва анъанавий мудофаа тизимларининг оператив имкониятларини чеклайди. Жумладан, таҳдидлар қуйидагича функцияга эга бўлади:

Deepfake ва синтетик аудио/видео-жамоатчилик онгини манипуляция қилиш, жамиятда дезинформация тарқатиш, сиёсий инқирозлар ва ижтимоий беқарорликни сунъий келтириб чиқариш.

AI-driven Phishing-давлат органлари, мудофаа ва энергетика тизимларининг махфий тармоқларига кириш ҳуқуқини ўғирлаш ҳамда киберайғоқчилик.

Алгоритмик фирибгарлик-банк-молия тизими барқарорлигини издан чиқариш, рақамли активлар ва давлат харидлари тизимларидан йирик миқдордаги маблағларни чиқариб кетиш.

Автоном киберхужумлар- стратегик объектлар (АЭС, сув омборлари, ҳарбий алоқа) бошқарув тизимларини мустақил равишда ишдан чиқариш ва фронт орти инфраструктурасини фалажлаш.

Янги авлод кибертаҳдидлари асимметрик хусусиятга эга бўлиб, хавфсизликни таъминлашда қуйидаги тизимли қийинчиликларни юзага келтиради:

1. **«Атрибуция» (Муаллифликни аниқлаш) муаммоси:** Автоном СИ тизимлари томонидан амалга оширилган киберхужумларнинг асл буюртмачисини (давлат ёки нодавлат

субъектларини) аниқлаш ва юридик жиҳатдан исботлаш имконияти кескин пасаяди.

2.Ахборот-коммуникация соҳасидаги оператив вақт дефицити: СИ-хужумлари сониялар ичида амалга оширилгани сабабли, киберхавфсизлик мутахассисларининг (инсон омилининг) реал вақт режимида реакция қайтариш имконияти чекланади.

3.Когнитив суверенитетнинг бузилиши: СИ томонидан яратилган ва кенг кўламда тарқатилган гибрид дезинформация жамиятдаги институционал ишончни пучга чиқаради ва давлат суверенитетининг ахборот сегментини заифлаштиради.

Хавфсизлик тизимини янги авлод кибертаҳдидларидан ҳимоя қилиш учун қуйидаги чора-тадбирларни амалга ошириш зарур:

Биринчидан, AI-powered SOC ва SIEM тизимларига ўтиш: Кибертаҳдидларга қарши курашда инсон омилидан автоном СИ-мудофаа (*AI vs AI defense*) концепциясига ўтиш ва таҳдидларни автоматик зарарсизлантирувчи тизимларни жорий этиш.

Иккинчидан, синтетик медиа ва Deepfake'ларни маркировка қилишнинг ҳуқуқий механизмини яратиш: Диффузион ва генератив тизимлар томонидан яратилган барча медиа-контентларни криптографик рақамли белгилар (Watermarking) билан мустаҳкамлаш ва буни қонуан мажбурий қилиш.

Учинчидан, критик инфраструктура объектларида «Zero Trust» (Ноль ишонч) ва ахборот гигиенаси стандартини кучайтириш: ДНК-аутентификация, кўп босқичли биометрик полиморфизм ва СИ-фишингга қарши персоналнинг когнитив чидамлилигини ошириш бўйича тизимли тренинглари йўлга қўйиш лозим.

Янги авлод кибертаҳдидлари шунчаки техник хавф бўлмай, балки давлат ва жамият барқарорлигига бевосита таҳдид солувчи стратегик омилга айланади. Deepfake, AI-driven phishing ва автоном киберхужумларнинг давлат ва жамият хавфсизлигига салбий таъсирини жиловлаш алгоритмик мудофаа ва миллий қонунчиликни янги таҳдидлар феноменига мослаштириш орқали комплексли ёндошувни талаб этади.

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.

