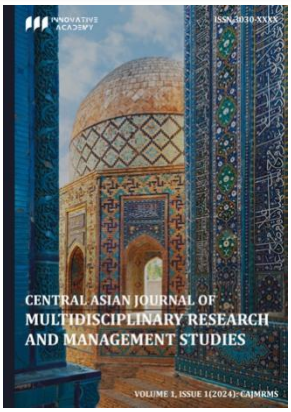

ИЧКИ ИШЛАР ОРГАНЛАРИНИНГ КИБЕР ЖИНОЯТЛАРГА ҚАРШИ КУРАШИШ БЎЛИНМАЛАРИ ФАОЛИЯТИНИ ТАКОМИЛЛАШТИРИШНИНГ АСОСИЙ ЙЎНАЛИШЛАРИ ВА ИСТИҚБОЛЛАРИ

Юсупов Джасур Хикматович
Ўзбекистон Республикаси ИИВ Академияси магистратураси "Ташкилий-стратегик бошқарув" мутахассислиги тингловчиси, подполковник

Худайбердиев Абдурашид Абдирасулович
Маъмурий ҳуқуқ кафедраси доценти ю.ф.б.ф.д (PhD) доцент

https://doi.org/10.5281/зенодо.15654366

ARTICLE INFO

Received: 01st June 2025
Accepted: 05th June 2025
Published: 13th June 2025

KEYWORDS

Киберхавфсизлик, кибер жиноятлар, ички ишлар органлари, қонунчилик, сунъий интеллект, блокчейн, трансмиллий жиноятлар, маълумот алмашинуви, тезкор жавоб бериш, хусусий сектор, фишинг, DDoS ҳужумлари, мутахассислар тайёрлаш, рақамли иқтисодиёт.

ABSTRACT

Мазкур мақолада Ички ишлар органларининг кибер жиноятларга қарши курашиш бўлинмалари фаолиятини такомиллаштиришнинг асосий йўналишлари ва истиқболларига бағишланган. Унда кибер жиноятларнинг хусусиятлари, уларнинг жамоат хавфсизлиги ва давлат барқарорлигига таъсири, шунингдек, Ўзбекистондаги мавжуд муаммолар – қонунчилик базасининг етарли эмаслиги, техник таъминлашнинг чекланганлиги ва малакали кадрларнинг тақчиллиги кўриб чиқилади. Хорижий тажриба, хусусан, Австралия, Япония, АҚШ ва Европа Иттифоқининг илғор амалиётлари таҳлил қилиниб, уларни Ўзбекистон шароитига мослаштириш бўйича таклифлар берилган. Маълумот алмашинуви тизимини жорий қилиш, тезкор жавоб бериш гуруҳларини ташкил қилиш, хусусий сектор билан ҳамкорликни кучайтириш ва замонавий технологиялар (AI, блокчейн) ни қўллаш каби ташкилий-тактик чоралар тавсия этилган. Шунингдек, махсус қонунчилик ишлаб чиқиш, Будапешт конвенциясига қўшилиш ва мутахассислар тайёрлаш бўйича амалий тавсиялар илгари сурилган.

Президент Шавкат Мирзиёев раислигида 2024 йил 10 январда ўтказилган видеоселектор йиғилишида таъкидланганидек, "Киберхавфсизликни таъминлаш ва кибер жиноятларга қарши курашиш фуқароларнинг хавфсизлиги ва давлат барқарорлиги учун муҳим омилдир. Бироқ, бу борадаги ишлар талаб даражасида эмас, соҳани такомиллаштириш бўйича қилинадиган ишлар кўп"[1]. Ушбу сўзлар кибер

[1] Мирзиёев Ш.М. "Киберхавфсизлик ва жамоат хавфсизлигини таъминлаш бўйича вазифалар" Халқ сўзи, 2024, 10 январь.

жиноятларга қарши курашиш бўлинмалари фаолиятининг самарадорлигини ошириш заруратини кўрсатади.

Кибер жиноятлар – бу интернет ва ахборот-коммуникация технологияларидан (АКТ) фойдаланиб содир этиладиган ноқонуний хатти-ҳаракатлар бўлиб, улар шахсий маълумотларни ўғирлаш, молиявий зарар келтириш, жамоат тартибини бузиш ёки давлат хавфсизлигига таҳдид солишга қаратилган бўлиши мумкин. Кибер жиноятларнинг асосий турларига фишинг, ransomware, DDoS ҳужумлари, маълумотларни ноқонуний олиш, киберфирибгарлик ва хакерлик киради[2].

Кибер жиноятларнинг ўзига хос хусусиятлари уларни анъанавий жиноятлардан фарқ қилувчи омилларга эга:

– Трансмиллий хусусият: Кибер жиноятлар кўпинча бир неча давлат чегараларидан ўтиб содир қилинади, бу эса уларни аниқлаш ва тергов қилишни қийинлаштиради. Масалан, Интерпол маълумотларига кўра, 2023 йилда кибер жиноятларнинг 60% трансмиллий характерга эга бўлган[3].

– Анонимлик: Кибер жиноятчилар VPN, Tor тармоқлари ва бошқа анонимлаштириш воситаларидан фойдаланиб, ўз шахсини яширишади[4].

– Жадал ривожланиш: Кибер жиноятларнинг усул ва воситалари технологиялар ривожланиши билан мунтазам ўзгариб боради. Масалан, сунъий интеллект (AI) асосидаги фишинг ҳужумлари 2024 йилда 25% га ошган[5].

– Иқтисодий ва ижтимоий зарар: Cybersecurity Ventures маълумотларига кўра, кибер жиноятлар глобал иқтисодиётга 2025 йилда йиллик 10,5 триллион АҚШ доллари зарар келтириши прогноз қилинмоқда[6].

Ўзбекистонда кибер жиноятларнинг ўсиши рақамли иқтисодиёт ва интернет фойдаланувчилари сонининг кўпайиши билан боғлиқ. 2025 йилга келиб, Ўзбекистонда интернет фойдаланувчилари сони 28 миллиондан ошди, бу эса кибер таҳдидларга қарши курашиш заруратини оширди[7].

Кибер жиноятлар Ўзбекистонда жамоат хавфсизлигига қуйидаги йўллар билан таъсир кўрсатмоқда:

– Молиявий зарар: 2023 йилда Ўзбекистонда киберфирибгарлик билан боғлиқ зарар 150 миллиард сўмдан ортиқни ташкил этди, бу асосан фишинг ва онлайн-банкингдан ноқонуний фойдаланиш билан боғлиқ[8].

– Фуқароларнинг ишончига путур: Кибер ҳужумлар фуқароларнинг давлат ва молиявий тизимларга бўлган ишончига салбий таъсир кўрсатади. Сўров натижаларига кўра, респондентларнинг 42,7% кибер таҳдидлар туфайли онлайн хизматлардан фойдаланишдан қўрқишади

– Жамоат тартибига таҳдид: Кибер жиноятлар, хусусан, ижтимоий тармоқлар орқали тарқаладиган дезинформация ва кибертерроризм, жамоат тартибини бузишга хизмат қилиши мумкин. 2024 йилда Ўзбекистонда ижтимоий тармоқларда фейк хабарлар тарқатиш билан боғлиқ 320 та ҳолат қайд этилди[9].

[2] UNODC. “Cybercrime and Its Impact on Global Economy” 2023.
[3] Interpol. “Global Cybercrime Programme” https://www.interpol.int/, 2024.
[4] Smith, J. “Global Cybercrime Trends” Journal of Cybersecurity, 2023.
[5] Lee, K. “AI in National Cybersecurity” Cybersecurity Journal, 2024.
[6] Cybersecurity Ventures. “Cybercrime Report 2023.” https://www.cybersecurityventures.com, 2023.
[7] Ўзбекистон Республикаси Алоқа ва ахборотлаштириш агентлиги. “Интернет фойдаланувчилари статистикаси” 2025.
[8] Ўзбекистон Ички ишлар вазирлиги. “Киберфирибгарлик бўйича ҳисобот” Тошкент, 2024.
[9] Ўзбекистон Ички ишлар вазирлиги. “Ижтимоий тармоқларда дезинформация тарқатиш ҳолатлари” 2024.

– Давлат хавфсизлигига таъсир: Кибер ҳужумлар муҳим инфратузилма объектларига, масалан, энергетика ва телекоммуникация тизимларига йўналтирилган бўлиб, миллий хавфсизликка хавф туғдиради[10].

Ўзбекистонда кибер жиноятларга қарши курашиш ИИО фаолиятининг муҳим йўналиши сифатида кўрилади. Бироқ, мавжуд муаммолар, жумладан, қонунчилик базасининг етарли эмаслиги, моддий-техник таъминлашнинг чекланганлиги ва мутахассисларнинг етишмаслиги соҳанинг самарадорлигини пасайтиради[11]. Сўровда иштирок этган мутахассисларнинг 55,3% ИИО кибер жиноятларга қарши курашиш бўлинмалари фаолиятининг ҳуқуқий асослари етарли даражада мукаммал эмаслигини таъкидлади.

Кибер жиноятларнинг тез ўзгарувчан табиати ва уларнинг жамоат хавфсизлигига таъсири ИИО бўлинмалари фаолиятини такомиллаштириш заруратини кўрсатади. Бу борада хорижий тажрибалар, хусусан, Австралия, Япония, АҚШ ва Европа Иттифоқининг илғор амалиётлари муҳим аҳамиятга эга.

Ўзбекистонда кибер жиноятлар сонининг ортиши интернет инфратузилмасининг кенгайиши ва рақамли хизматларнинг оммалашуви билан боғлиқ. 2025 йилга келиб, интернет фойдаланувчилари сони 28 миллиондан ошди, бу кибер таҳдидларнинг кўпайишига олиб келди. ИИО маълумотларига кўра, 2023 йилда кибер жиноятлар билан боғлиқ 12 500 та ҳолат қайд этилган бўлиб, уларнинг 45% фишинг, 30% онлайн-фирибгарлик ва 15% маълумотларни ноқонуний олиш билан боғлиқ. Бу рақамлар 2022 йилга нисбатан 22% га кўпайганини кўрсатади[12].

Кибер жиноятларнинг асосий турлари қуйидагилардан иборат:

– Фишинг: Фуқароларнинг шахсий маълумотларини ўғирлашга қаратилган қалбаки веб-сайтлар ва электрон хабарлар. 2023 йилда фишинг ҳужумлари туфайли 50 миллиард сўмдан ортиқ зарар кўрилди[13].

– Онлайн-фирибгарлик: Интернет-магазинлар ва ижтимоий тармоқлар орқали амалга оширилган фирибгарликлар.

– DDoS ҳужумлари: Муҳим инфратузилма объектларига, хусусан, банк тизимларига қарши йўналтирилган хизматдан чиқариш ҳужумлари.

Сўров натижаларига кўра, мутахассисларнинг 52,3% кибер жиноятларнинг ортишини рақамли хизматларнинг кенгайиши ва аҳолининг киберхавфсизлик бўйича билимларининг етарли эмаслиги билан изоҳлайди.

Ўзбекистонда кибер жиноятларга қарши курашиш ИИО’нинг махсус бўлинмалари, хусусан, Киберхавфсизлик ва ахборот хавфсизлиги бошқармаси томонидан амалга оширилади. Ушбу бўлинма 2018 йилда ташкил этилган бўлиб, қуйидаги вазифаларни бажаришга масъул:

– Кибер жиноятларни аниқлаш ва тергов қилиш;

– Муҳим инфратузилма объектларини кибер таҳдидлардан ҳимоя қилиш;

– Фуқаролар ва ташкилотларни киберхавфсизлик бўйича хабардор қилиш[14].

Бироқ, бўлинманинг фаолиятида бир қатор муаммолар мавжуд:

– Қонунчилик базасининг етарли эмаслиги: Кибер жиноятларга қарши курашишни тартибга солувчи махсус қонун йўқ, мавжуд норматив-ҳуқуқий ҳужжатлар эса умумий характерга эга[15].

– Моддий-техник таъминлашнинг чекланганлиги: Кибер таҳдидларни аниқлаш учун зарур бўлган замонавий технологиялар ва дастурий таъминот етишмайди.

---

[10] Rahimov, A. “Ўзбекистонда киберхавфсизлик муаммолари” Илмий мақолалар тўплами, 2023.

[11] Qodirov, S. “Киберхавфсизлик қонунчилиги” Юридик фанлар журнали, 2024.

[12] Qodirov, S. “Киберхавфсизлик қонунчилиги” Юридик фанлар журнали, 2024.

[13] Ўзбекистон Ички ишлар вазирлиги. “Фишинг ҳужумлари бўйича статистика” Тошкент, 2024.

[14] Ўзбекистон Ички ишлар вазирлиги. “Киберхавфсизлик бошқармаси фаолияти” Тошкент, 2023.

[15] “Ахборот хавфсизлиги тўғрисида”ги Ўзбекистон Республикаси қонуни. 2019.

– Кадрлар етишмаслиги: Киберхавфсизлик соҳасида малакали мутахассисларнинг тақчиллиги мавжуд.
– *Технологик инфратузилманинг етарли эмаслиги:* Замонавий кибер таҳдидларни аниқлаш ва уларга жавоб бериш учун зарур бўлган юқори тезликдаги интернет, серверлар ва дастурий таъминот етишмайди.
– *Мутахассисларнинг малакаси:* Киберхавфсизлик бўлинмалари ходимларининг аксарияти замонавий кибер таҳдидлар билан ишлаш учун етарли тажриба ва билимга эга эмас.

Ташкилий-тактик муаммоларни бартараф қилиш учун қуйидаги чора-тадбирларни амалга ошириш тавсия этилади:
– Маълумот алмашинуви тизимини жорий қилиш: ИИО бўлинмалари ўртасида ва бошқа давлат идоралари билан реал вақтда маълумот алмашинувини таъминловчи ягона платформа яратиш. Масалан, кибер жиноятлар тўғрисида маълумотларни тўплаш ва таҳлил қилиш учун махсус маълумотлар базаси ишлаб чиқилиши мумкин[16].
– Тезкор жавоб бериш гуруҳларини ташкил қилиш: Кибер жиноятларга 24/7 жавоб беришга қодир махсус тезкор жавоб гуруҳлари (Cyber Incident Response Teams) ташкил қилиниши керак. Бу гуруҳлар кибер ҳужумларни тез зарарсизлантириш ва далилларни сақлаб қолишга хизмат қилади.
– Хусусий сектор билан ҳамкорликни кучайтириш: Телекоммуникация компаниялари (масалан, Ucell, Beeline) ва IT-компаниялар билан биргаликда кибер таҳдидларни аниқлаш ва уларга қарши курашиш бўйича лойиҳаларни кенгайтириш. Масалан, хусусий сектор билан DDoS ҳужумларига қарши биргаликдаги симуляция ўйинлари ўтказилиши мумкин.
– *Вилоятда бўлинмаларини кучайтириш:* Вилоятлардаги киберхавфсизлик бўлинмаларига қўшимча молиявий ва техник ресурслар ажратиш, шунингдек, мутахассисларни махсус тренинглар билан таъминлаш.
– Тактик ёндашувларни такомиллаштириш: AI ва машинавий ўқитиш асосидаги тизимларни жорий қилиш орқали кибер таҳдидларни аниқлашни тезлаштириш, тергов жараёнларини автоматлаштириш ва превентив чораларни кучайтириш. Масалан, фишинг хабарларини аниқлаш учун AI асосидаги фильтрлар қўлланиши мумкин[17].

Юқоридаги таклифларни амалга ошириш ИИО кибер жиноятларга қарши курашиш бўлинмаларининг ташкилий-тактик фаолиятини сезиларли даражада яхшилайди. Маълумот алмашинуви тизимини жорий қилиш кибер жиноятларга жавоб бериш вақтини қисқартиради, хусусий сектор билан ҳамкорлик эса ресурсларни оптималлаштиришга хизмат қилади.

Кибер жиноятларга қарши курашиш бўлинмалари фаолиятини такомиллаштириш учун қуйидаги амалий тавсиялар таклиф қилинади:

– Ҳуқуқий базани такомиллаштириш. “Кибер жиноятларга қарши курашиш тўғрисида”ги махсус қонун ишлаб чиқиш ва 2026 йилгача қабул қилиш. Ушбу қонун кибер жиноятларнинг турлари (фишинг, ransomware, DDoS ҳужумлари), тергов тартиб-қоидалари ва мутахассислар ваколатларини аниқ белгилаши керак.
– Жиноят кодексига сунъий интеллект (AI) асосидаги ҳужумлар ва криптовалюта билан боғлиқ жиноятлар учун алоҳида моддалар киритиш.
– Будапешт конвенциясига қўшилиш бўйича музокараларни бошлаш ва Интерпол билан маълумот алмашинувини тартибга солувчи шартномаларни кенгайтириш.

[16] Karimov, N. “Киберхавфсизликда маълумот алмашинуви” Илмий мақолалар тўплами, 2024.
[17] Global Cybersecurity Forum. “Best Practices in Cybercrime Prevention” 2024.

– ИИО бўлинмалари ўртасида реал вақтда маълумот алмашинувини таъминловчи ягона платформа яратиш. Бу платформа кибер жиноятлар тўғрисида маълумотларни тўплаш ва таҳлил қилиш учун маълумотлар базасини ўз ичига олади.
– 24/7 режимида ишлайдиган тезкор жавоб бериш гуруҳлари (Cyber Incident Response Teams) ташкил қилиш, ҳар бир вилоятда камида 10 нафар мутахассисдан иборат гуруҳларни жойлаштириш.
– Хусусий сектор билан ҳамкорликда кибер таҳдидларга қарши биргаликдаги симуляция ўйинлари ўтказиш, масалан, Ucell ва Beeline билан DDoS ҳужумларига қарши машғулотлар.
– ИИВ Академияси ва Тошкент ахборот технологиялари университетida AI, блокчейн ва квант хисоблашни ўз ичига олган замонавий киберхавфсизлик дастурларини жорий қилиш.
Мутахассислар учун инглиз тили бўйича махсус курслар ташкил қилиш ва хорижий тиллар билимини текширувчи имтиҳонларни мажбурий қилиш.