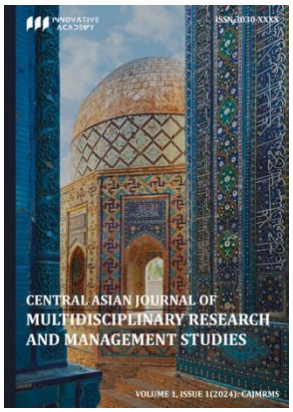

ИЧКИ ИШЛАР ОРГАНЛАРИНИНГ КИБЕР ЖИНОЯТЛАРГА ҚАРШИ КУРАШИШ БЎЛИНМАЛАРИ ФАОЛИЯТИГА ДОИР ИЛҒОР ХОРИЖ ТАЖРИБАСИНИНГ ИЛМИЙ ТАҲЛИЛИ

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.15654341

ARTICLE INFO

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

KEYWORDS

Киберхавфсизлик, кибер жиноятлар, ички ишлар органлари, сунъий интеллект, блокчейн, халқаро ҳамкорлик, миллий стратегия, қонунчилик, кадрлар тайёрлаш, рақамли инфратузилма, фишинг, криптовалюта фирибгарлиги, трансмиллий жиноятлар.

ABSTRACT

Ушбу мақола Ички ишлар вазирлигининг кибер жиноятларга қарши курашиш бўлинмалари фаолиятини такомиллаштириш масалаларига бағишланган бўлиб, унда Буюк Британия, АҚШ, Германия, Сингапур, Россия ва Хитой каби ривожланган давлатларнинг илғор тажрибаси таҳлил қилишга асосланади. Ушбу давлатларда киберхавфсизликни таъминлаш бўйича қонунчилик, технологик инфратузилма, кадрлар тайёрлаш ва халқаро ҳамкорлик механизмлари ўрганилиб, уларнинг ижобий жиҳатларини Ўзбекистон шароитига мослаштириш бўйича амалий тавсиялар ишлаб чиқилган. Мақолада сунъий интеллект ва блокчейн технологияларининг кибер таҳдидларга қарши курашишдаги аҳамияти, шунингдек, молиявий чекловлар, малакали кадрлар етишмаслиги ва қонунчилик тўсиқлари каби муаммолар кўриб чиқилади. Ўзбекистонда киберхавфсизликни кучайтириш учун миллий стратегия ишлаб чиқиш, махсус агентлик ташкил қилиш, хусусий сектор билан ҳамкорликни ривожлантириш ва халқаро ташкилотлар билан маълумот алмашинувини кенгайтириш каби таклифлар илгари сурилган.

Ички ишлар органларининг кибер жиноятларга қарши курашиш бўлинмалари фаолиятини такомиллаштириш масалаларини кўриб чиқар эканмиз, бу борада ривожланган давлатлар, хусусан, Буюк Британия, АҚШ, Германия, Сингапур, Россия ва Хитойнинг кибер жиноятларга қарши курашиш соҳасидаги илғор тажрибаларини таҳлил қилиш муҳим аҳамиятга эга. Ушбу давлатларда кибер жиноятларга қарши курашиш бўйича қонунчилик нормалари, технологик инфратузилма, кадрлар тайёрлаш тизими ва халқаро ҳамкорлик механизмлари қандай шакллантирилганлигини ўрганиш, уларнинг ижобий жиҳатларини Ўзбекистон шароитига мослаштириш ва миллий киберхавфсизлик тизимини янада ривожлантиришга қаратилган тавсиялар ишлаб чиқишга хизмат қилади.

Ички ишлар органларининг кибер жиноятларга қарши курашиш бўлинмалари турли хилдаги замонавий технологиялар билан таъминланган бўлса-да, улар фаолиятига сунъий интелект технологияларидан фойдаланишнинг жорий қилинмаганлиги фойдаланишнинг асосий муаммолардан бири бўлиб, бу кибер хавфларни аниқлаш ва киберҗжиноятчиликнинг олдини олиш имкониятларини чекламоқда. Сунъий интелектга (AI)-асосланган таҳлил воситалари (масалан, Splunk, Darktrace) ва блокчейн-таҳлил платформалари (Chainalysis) каби илғор технологияларнинг йўқлиги фишинг ва криптовалюта фирибгарлиги жиоятчилиги каби жиноятларни тергов қилишни қийинлаштиради, чунки бу воситалар real-time (реал вақт) режимида маълумот таҳлили, жиноий транзакцияларни кузатиш ва автоматик чоралар кўриш имконини беради. Аммо, молиявий чекловлар, инфратузилма муаммолари ва малакали кадрларнинг етишмаслиги туфайли улар Ички ишлар органлари тизимида тўлиқ қўлланилмайди, бу эса кибер жиноятларга қарши кураш самарадорлигини пасаятиради.

Хорижий давлатларда кибер жиноятларга қарши курашиш бўлинмалари турли хилдаги замонавий технологиялар билан таъминланган бўлиб, бу соҳа уларнинг ҳар бирида алоҳида аҳамият касб этади. Жумладан, Германияда Федерал жиноят полицияси бўлими Darktrace ва FireEye каби сунъий интеллектга асосланган воситалардан фойдаланади. Улар кибер хужумларни аниқлаш ва улардан автоматик равишда ҳимояланиш имкониятига эга. Шунингдек, блокчейн-таҳлил воситалари криптовалюта билан боғлиқ жиноятларни тергов қилишда қўлланилади. Германияда киберхавфсизлик тизими қонун устуворлиги ва шаффофликка асосланади. Федерал жиноят полицияси махсус “Cybercrime Competence Center” орқали халқаро ташкилотлар (Europol, INTERPOL) билан маълумот алмашади. Технологиялар кўп ҳаражат талаб қилганлиги учун мазкур технологияларни жорий қилиш учун Германияда давлат-хусусий шерикчилик моделидан фойдаланилади.

Сўнгги йилларда рақамли технологияларнинг жадал ривожланиши кибер жиноятлар сони ва хилма-хиллигининг сезиларли ўсишига олиб келди. Халқаро маълумотларга кўра, 2023 йилда кибер жиноятлар глобал иқтисодиётга бир триллион АҚШ долларидан ортиқ зарар келтирди[1]. Ўзбекистонда интернет фойдаланувчилари сони 2025 йилга келиб 22 миллиондан ошди, бу эса киберхавфсизлик масалаларини Ўзбекистон ички ишлар органлари учун устувор вазифага айлантирди[2].

Кибер жиноятларнинг трансмиллий хусусияти, технологик мураккаблиги ва ижтимоий-иқтисодий оқибатлари ички ишлар органларидан замонавий ёндашувларни талаб қилади. Хорижий давлатларнинг илғор тажрибасини ўрганиш ва уни Ўзбекистон шароитига мослаштириш КЖҚКБ фаолиятини янада такомиллаштиришда муҳим аҳамиятга эга[3]. Жумладан, кибер жиноятларга фишинг, маълумотларни ўғирлаш, ransomware (тўлов талаб қилувчи зарарли дастурлар), кибертерроризм ва шахсий маълумотларни ноқонуний ишлатиш каби хавф-хатарлар киради. Ушбу жиноятларнинг асосий хусусиятлари қуйидагича:

1) Трансмиллий хусусият: Кибер жиноятлар кўпинча бир неча давлатни қамраб олади, бу эса халқаро ҳамкорликни талаб қилади[4];

[1]Cybersecurity Ventures. “Cybercrime Report 2023.” https://www.cybersecurityventures.com

[2] Ўзбекистон Республикаси Алоқа ва ахборотлаштириш агентлиги. “Интернет фойдаланувчилари статистикаси.” 2025.

[3] Smith, J. “Global Cybercrime Trends.” Journal of Cybersecurity, 2023.

[4] Europol. “Internet Organised Crime Threat Assessment.” 2024.

2) Технологик мураккаблик: Жиноятчилар сунъий интеллект, блокчейн ва анонимлаштирувчи технологиялардан фойдаланиб, жиноятларни яширишда юқори даражадаги анонимликка эришади[5];
3) Иқтисодий ва ижтимоий зарар: Кибер жиноятлар нафақат молиявий зарар келтиради, балки фуқароларнинг хавфсизлиги ва давлат барқарорлигига таҳдид солади[6].
Кибер жиноятларнинг ўсиши ички ишлар органларидан янги ёндашувлар, замонавий технологиялар ва халқаро тажрибани ўрганишни талаб қилади.

Австралия киберхавфсизлик соҳасида дунёдаги илғор давлатлардан бири бўлиб, ушбу фаолият **Australian Cyber Security Centre (ACSC)** томонидан бошқарилади. ACSC 2014 йилда ташкил этилган бўлиб, кибер таҳдидларга қарши курашишда давлат органлари, хусусий сектор ва халқаро шериклар билан яқин ҳамкорлик қилади. Австралиянинг киберхавфсизлик стратегияси қуйидаги асосий йўналишларга эга:
– Миллий киберхавфсизлик стратегияси: Австралия 2020 йилда "Cyber Security Strategy"ни қабул қилди, унда кибер таҳдидларга қарши давлат ва хусусий секторнинг биргаликдаги фаолияти мувофиқлаштирилган. Ушбу стратегия доирасида 2023 йилда 1.67 миллиард AUD (тахминан 1.1 миллиард АҚШ доллари) киберхавфсизликни кучайтиришга йўналтирилди[7]. Бу маблағлар муҳим инфратузилмани ҳимоя қилиш, технологияларни ривожлантириш ва мутахассислар тайёрлашга сарфланди.
– Тезкор жавоб бериш ва мониторинг: ACSC'нинг Joint Cyber Security Centres (JCSCs) тизими кибер инцидентларга тезкор жавоб бериш ва маълумотлар алмашинувини таъминлайди. 2023 йилда ACSC томонидан 94 000 га яқин кибер инцидент хабар қилинган, уларнинг 30% дан ортиғи тезкор чоралар билан зарарсизлантирилди[8].
– Хусусий сектор билан интеграция: Австралияда хусусий сектор билан ҳамкорлик киберхавфсизликнинг асосий унсуридир. Telstra ва Optus каби телекоммуникация компаниялари ACSC билан биргаликда кибер таҳдидларни аниқлаш ва уларга қарши курашишда иштирок этади. Масалан, Telstra'нинг киберхавфсизлик бўйича махсус гуруҳи 2023 йилда DDoS ҳужумларига қарши самарали чоралар кўрди.
Австралия тажрибасининг Ўзбекистон учун муҳимлиги унинг миллий киберхавфсизлик стратегиясини ишлаб чиқиш ва хусусий сектор билан интеграцияда кўринади. Ўзбекистонда ACSC'га ўхшаш марказ ташкил қилиш ва унинг маълумот алмашинуви тизимидан фойдаланиш кибер таҳдидларга қарши самарали жавоб бериш имкониятини оширади.
Япония киберхавфсизлик соҳасида муҳим тажрибага эга бўлиб, ушбу фаолият **National Center of Incident Readiness and Strategy for Cybersecurity (NISC)** томонидан бошқарилади. NISC Япониянинг киберхавфсизлик сиёсатини мувофиқлаштиради ва давлат органлари, хусусий сектор ва халқаро ташкилотлар билан ҳамкорлик қилади. Япониянинг киберхавфсизлик стратегияси қуйидаги йўналишларга эга:
– Муҳим инфратузилмани ҳимоя қилиш: Японияда энергетика, транспорт ва молия каби муҳим инфратузилма объектлари кибер ҳужумлардан ҳимояланишга алоҳида эътибор берилади. 2023 йилда NISC томонидан ишлаб чиқилган "Cybersecurity Strategic Plan" муҳим инфратузилма операторлари учун қатъий хавфсизлик стандартларини белгилади[9].

[5] Johnson, L. "AI in Cybercrime Detection." Cybersecurity Review, 2022.
[6] UNODC. "Cybercrime and Its Impact on Global Economy." 2023.

[7] Australian Government. "Cyber Security Strategy 2020." https://www.homeaffairs.gov.au/, 2024.
[8] ACSC. "Annual Cyber Threat Report 2023." https://www.cyber.gov.au/, 2023.
[9] NISC. "Cybersecurity Strategic Plan 2023." https://www.nisc.go.jp/, 2023.

– Халқаро ҳамкорлик: Япония Интерпол ва АҚШнинг CISA каби ташкилотлар билан яқин ҳамкорлик қилади. Масалан, 2024 йилда Япония ва АҚШ ўртасидаги биргаликдаги операция натижасида фишинг ва ransomware ҳужумларига қарши муҳим чоралар кўрилди[10].

– Киберхавфсизлик бўйича таълим ва тренинг: Японияда киберхавфсизлик мутахассисларини тайёрлашга катта эътибор берилади. NISC ва Токио университети каби таълим муассасалари биргаликда киберхавфсизлик бўйича махсус тренинг дастурларини ташкил қилади. 2023 йилда Японияда 5000 дан ортиқ мутахассис ушбу дастурлардан ўтди.

Япония тажрибасининг муҳим инфратузилмани ҳимоя қилиш ва мутахассислар тайёрлашдаги ёндашувида кўринади. Ўзбекистонда NISC'га ўхшаш марказ ташкил қилиш ва таълим муассасалари билан ҳамкорликни кучайтириш орқали киберхавфсизлик соҳасидаги малака оширишга эришиш мумкин[11].

Сингапур киберхавфсизлик соҳасида дунёдаги энг илғор давлатлардан бири сифатида тан олинган. Ушбу мамлакатда кибер жиноятларга қарши курашиш **Cyber Security Agency of Singapore (CSA)** томонидан бошқарилади, бу агентлик 2015 йилда ташкил этилган ва рақамли инфратузилмани мустаҳкамлашга алоҳида эътибор беради. Сингапурнинг киберхавфсизлик стратегияси қуйидаги асосий йўналишларга эга:

– Рақамли инфратузилмани ҳимоя қилиш: Сингапурда муҳим инфратузилма объектлари, жумладан, молия, телекоммуникация ва энергетика соҳалари кибер ҳужумлардан юқори даражада ҳимояланган. CSA томонидан ишлаб чиқилган "Cybersecurity Code of Practice" муҳим инфратузилма операторлари учун қатъий хавфсизлик стандартларини белгилайди[12].

– Замонавий технологиялардан фойдаланиш: Сингапур кибер таҳдидларни аниқлаш ва уларга қарши курашишда сунъий интеллект (AI) ва машинавий ўқитиш (machine learning) технологияларидан фойдаланади. Масалан, CSA'нинг AI асосидаги тизимлари фишинг ҳужумлари ва DDoS (Distributed Denial of Service) ҳужумларини реал вақтда аниқлайди[13].

– Жамоатчиликни хабардор қилиш: Сингапурда киберхавфсизлик бўйича фуқароларнинг хабардорлигини ошириш учун кенг кўламли тарғибот ишлари амалга оширилади. "Go Safe Online" тарғибот кампанияси фуқароларга кибер таҳдидлардан ҳимояланиш бўйича амалий тавсиялар беради[14].

Сингапурнинг тажрибасидан Ўзбекистон учун муҳим бўлган рақамли иқтисодиётни ривожлантириш билан бирга киберхавфсизликни таъминлашда муваффақиятли моделни жорий қилиш муҳим аҳамият касб этади. Ўзбекистонда CSA'га ўхшаш махсус агентлик ташкил қилиш ва унинг тажрибасидан фойдаланиш орқали миллий киберхавфсизлик тизимини кучайтириш зарур[15].

Россияда кибер жиноятларга қарши курашиш Ички ишлар вазирлигининг "К" бўлими (Кибер жиноятларга қарши курашиш бўйича махсус бўлим) томонидан амалга оширилади. Ушбу бўлим киберхавфсизлик соҳасида муҳим тажрибага эга ва қуйидаги йўналишларда фаолият юритади:

– Маълумотлар базасини яратиш: "К" бўлими кибер жиноятчиларнинг фаолиятини кузатиш ва уларнинг таҳдидларини аниқлаш учун кенг кўламли маълумотлар

[10] Interpol. "Japan-US Joint Cybercrime Operation." https://www.interpol.int/, 2024.
[11] Smith, J. "Global Cybercrime Trends." Journal of Cybersecurity, 2023.
[12] Cyber Security Agency of Singapore. "Cybersecurity Code of Practice." https://www.csa.gov.sg/, 2024.
[13] Lee, K. "AI in National Cybersecurity." Cybersecurity Journal, 2024.
[14] CSA Singapore. "Go Safe Online Campaign." https://www.csa.gov.sg/gosafeonline, 2024.
[15] Global Cybersecurity Forum. "Best Practices in Cybercrime Prevention." 2024.

базасини шакллантирган. Бу база кибер ҳужумларнинг тарихи ва жиноятчиларнинг ҳаракатларини таҳлил қилишда муҳим аҳамиятга эга[16].

Хорижий давлатларнинг кибер жиноятларга қарши курашиш соҳасидаги тажрибасини таҳлил қилиш асосида Ўзбекистонда киберхавфсизликни кучайтириш учун қуйидаги амалий таклифлар ишлаб чиқилди. Ушбу таклифлар Европа Иттифоқи, АҚШ, Сингапур ва Россия тажрибасидан келиб чиқиб, Ўзбекистоннинг миллий хусусиятларини инобатга олади.

Киберхавфсизлик соҳасида самарали фаолият юритиш учун қонунчилик базасини мукаммаллаштириш муҳимдир. Европа Иттифоқининг GDPR (General Data Protection Regulation) қонунчилигига асосланиб, Ўзбекистонда шахсий маълумотларни ҳимоя қилиш ва кибер жиноятларга қарши жазо чораларини кучайтиришга қаратилган қонун лойиҳасини ишлаб чиқиш мақсадга мувофиқ. Масалан, кибер жиноятчиларга нисбатан жарима ва қамоқ жазоси каби қатъий чораларни жорий қилиш зарур[17]. Бундан ташқари, киберхавфсизлик стандартларига риоя қилмаган ташкилотлар учун молиявий жарималар белгилаш фуқаролар маълумотларининг хавфсизлигини оширишга хизмат қилади[18].

Хорижий тажриба, хусусан, Сингапур ва АҚШдаги амалиёт кўрсатадики, сунъий интеллект (AI) ва блокчейн технологиялари кибер таҳдидларни аниқлаш ва уларга қарши курашишда муҳим ўрин тутади. Ўзбекистонда кибер жиноятларга қарши курашиш бўйича махсус бўлинмаларнинг техник таъминотини кучайтириш учун AI асосидаги мониторинг тизимларини жорий қилиш тавсия этилади. Масалан, фишинг ҳужумлари ва ransomware'ни аниқлашда машинавий ўқитиш алгоритмларидан фойдаланиш мумкин[19]. Бундан ташқари, блокчейн технологиясидан фойдаланиб, давлат ва хусусий сектор маълумотлар базаларининг хавфсизлигини ошириш зарур[20].

Европа Иттифоқи ва Россия тажрибаси кибер жиноятларнинг трансмиллий хусусияти туфайли халқаро ҳамкорликнинг муҳимлигини кўрсатади. Ўзбекистон Europol, Интерпол ва АҚШнинг CISA каби ташкилотлар билан маълумот алмашинуви ва биргаликдаги операцияларни кучайтириши керак. Масалан, Интерполнинг "Global Cybercrime Programme" доирасида Ўзбекистон иштирокини кенгайтириш кибер таҳдидларга қарши тезкор жавоб бериш имкониятларини оширади[21]. Бундан ташқари, хорижий ташкилотлар билан биргаликда тренинг дастурлари ташкил қилиш Ўзбекистон мутахассисларининг малакасини оширишга хизмат қилади[22].

АҚШ ва Сингапур тажрибаси киберхавфсизлик мутахассисларини тайёрлашнинг муҳимлигини таъкидлайди. Ўзбекистонда киберхавфсизлик соҳасида малакали кадрлар тайёрлаш учун махсус таълим дастурларини жорий қилиш зарур. Масалан, Тошкент ахборот технологиялари университетида киберхавфсизлик бўйича махсус магистратура ва тренинг курслари ташкил қилиниши мумкин[23]. Бундан ташқари, хорижий мутахассисларни жалб қилиб, тажриба алмашиш ва малака ошириш курсларини ташкил қилиш тавсия этилади[24].

Масалан, Ўзбекистондаги "Uzcard" ва "Humo" каби молиявий платформалар билан биргаликда кибер фирибгарликка қарши махсус лойиҳаларни амалга ошириш мумкин.

---

[16] Russian Ministry of Internal Affairs. "Cybercrime Division Report." 2023.
[17] European Union. "General Data Protection Regulation (GDPR)." 2018
[18] Qodirov, S. "Киберхавфсизлик қонунчилиги." Юридик фанлар журнали, 2024.
[19] Lee, K. "AI in National Cybersecurity." Cybersecurity Journal, 2024.
[20] Brown, T. "Blockchain in Cybersecurity." Tech Journal, 2023.
[21] Interpol. "Global Cybercrime Programme." https://www.interpol.int/, 2024.
[22] Cybercrime Training Academy. "Global Training Programs." 2023.
[23] Saidov, M. "Киберхавфсизлик мутахассисларини тайёрлаш." Илмий тадқиқотлар журнали, 2024.
[24] Xolmurodov, B. "Халқаро ҳамкорлик ва киберхавфсизлик." Тошкент, 2023.

Бундай ҳамкорлик молиявий транзакцияларнинг хавфсизлигини оширишга хизмат қилади[25]. Бундан ташқари, хусусий сектор билан биргаликда киберхавфсизлик бўйича инновацион стартапларни қўллаб-қувватлаш учун махсус фондлар ташкил қилиш тавсия этилади. Бу Сингапурдаги "Cybersecurity Startup Incubator" тажрибасига асосланади, унда стартаплар киберхавфсизлик соҳасида инновацион ечимлар ишлаб чиқиш учун молиявий ёрдам олади[26].

Хорижий тажриба, хусусан, Сингапур ва АҚШдаги амалиёт кўрсатадики, киберхавфсизлик соҳасида узоқ муддатли муваффақиятга эришиш учун миллий стратегия зарур. Ўзбекистонда киберхавфсизлик бўйича яхлит стратегия ишлаб чиқиш, унда қонунчилик, технологиялар, мутахассислар тайёрлаш ва халқаро ҳамкорлик каби йўналишлар аниқ белгиланиши керак. Ушбу стратегия доирасида махсус киберхавфсизлик агентлиги ташкил қилиш тавсия этилади, бу агентлик барча давлат органлари ва хусусий сектор ўртасидаги фаолиятни мувофиқлаштиради[27].

Хорижий тажрибани Ўзбекистонда муваффақиятли қўллаш учун молиявий ресурслар ва институционал тузилмаларни ривожлантириш муҳим аҳамиятга эга. Европа Иттифоқи, АҚШ ва Сингапур тажрибаси кўрсатадики, киберхавфсизлик соҳасидаги ислоҳотлар кўп харажатли бўлиши мумкин, лекин улар узоқ муддатда иқтисодий ва ижтимоий барқарорликни таъминлайди[28].

Киберхавфсизлик тизимини ривожлантириш учун Ўзбекистон давлат бюджетида махсус маблағлар ажратиш тавсия этилади. Масалан, Сингапурда киберхавфсизликка йиллик бюджетнинг 1% дан ортиқ қисми йўналтирилади, бу технологик инфратузилма ва мутахассислар тайёрлашга сарфланади[29]. Ўзбекистонда Ички ишлар вазирлигининг кибер жиноятларга қарши курашиш бўлими (КЖҚКБ) учун махсус молиялаштириш дастурини жорий қилиш зарур. Бу маблағлар техник таъминот, сунъий интеллект асосидаги тизимлар ва тренинг дастурларига йўналтирилиши мумкин[30]. Бундан ташқари, халқаро донор ташкилотлар, масалан, Жаҳон банки ёки БМТнинг киберхавфсизлик лойиҳалари орқали қўшимча молиявий ёрдам жалб қилиш имконияти мавжуд[31].

Институционал жиҳатлар: Ўзбекистонда киберхавфсизлик соҳасида фаолиятни мувофиқлаштириш учун махсус киберхавфсизлик агентлиги ташкил қилиш тавсия этилади. Бу агентлик Сингапурнинг Cyber Security Agency (CSA) ёки АҚШнинг CISA'га ўхшаш функцияларни бажариши мумкин. Агентлик Ички ишлар вазирлиги, Алоқа ва ахборотлаштириш агентлиги ва хусусий сектор ўртасидаги фаолиятни мувофиқлаштириб, кибер таҳдидларга қарши яхлит ёндашувни таъминлайди[32]. Бундан ташқари, киберхавфсизлик бўйича миллий стратегия доирасида махсус бўлинмаларнинг ваколатлари ва жавобгарлиги аниқ белгиланиши керак[33].

Хорижий тажрибани амалиётга татбиқ этиш ва қўллаш бир қатор муаммоларга дуч келиши мумкин:

– Молиявий чекловлар: Киберхавфсизлик тизимини ривожлантириш учун керак бўлган юқори харажатлар Ўзбекистоннинг бюджет имкониятларига мувофиқ

[25] Uzcard. "Молиявий транзакциялар хавфсизлиги." https://uzcard.uz/, 2024
[26] CSA Singapore. "Cybersecurity Startup Incubator." https://www.csa.gov.sg/, 2024.
[27] Global Cybersecurity Forum. "Best Practices in Cybercrime Prevention." 2024.
[28] Global Cybersecurity Forum. "Best Practices in Cybercrime Prevention." 2024.
[29] CSA Singapore. "Cybersecurity Budget Allocation." https://www.csa.gov.sg/, 2024.
[30] Ўзбекистон Ички ишлар вазирлиги. "Кибер жиноятларга қарши курашиш бўйича йўл харитаси." Тошкент, 2024.
[31] World Bank. "Cybersecurity Development Projects." https://www.worldbank.org/, 2023.
[32] CISA. "National Cybersecurity Coordination." https://www.cisa.gov/, 2024.
[33] Lee, K. "National Cybersecurity Strategies." Cybersecurity Journal, 2024.

бўлмаслиги мумкин. Бу муаммони халқаро грантлар ва хусусий сектор инвестициялари орқали ечиш мумкин.

– **Кадрлар етишмаслиги**: Киберхавфсизлик соҳасида малакали мутахассисларнинг камлиги хорижий технологияларни жорий қилишда тўсиқ бўлиши мумкин. Бу муаммони ечиш учун қисқа муддатли тренинг дастурлари ва узоқ муддатли таълим реформалари зарур.

– **Қонунчилик тўсиқлари**: Хорижий қонунчилик моделларини, масалан, GDPR'ни Ўзбекистон шароитига мослаштиришда миллий қонунчилик билан зиддиятлар юзага келиши мумкин. Бу муаммони ечиш учун қонунчиликни босқичма-босқич ислоҳ қилиш тавсия этилади[34].

– **Халқаро ҳамкорликдаги чекловлар**: Ўзбекистоннинг киберхавфсизлик соҳасидаги халқаро ташкилотлар билан ҳамкорлиги чекланган. Бу муаммони ечиш учун Интерпол ва Europol билан стратегик шерикликни кучайтириш зарур[35].

Ушбу муаммоларга қарамай, хорижий тажрибанинг Ўзбекистонда қўлланиши кибер жиноятларга қарши курашишнинг самарадорлигини оширишга хизмат қилади. Масалан, Сингапур ва АҚШ тажрибаси кўрсатадики, молиявий ва институционал ислоҳотлар узоқ муддатда ижобий натижалар беради[36].

Хорижий тажрибани Ўзбекистонда қўллаш киберхавфсизлик тизимининг самарадорлигини ошириш, фуқароларнинг хавфсизлигини таъминлаш ва иқтисодий барқарорликни мустаҳкамлашга хизмат қилади. Европа Иттифоқи, АҚШ, Сингапур ва Россия тажрибалари асосида ишлаб чиқилган таклифларни амалга ошириш орқали Ўзбекистонда кибер жиноятларга қарши курашишнинг янги босқичига чиқиш мумкин.

Ўзбекистонда кибер жиноятларга қарши курашишни янада самарали қилиш учун қуйидаги тавсиялар берилади:

– **Қонунчиликни такомиллаштириш**: GDPR'га ўхшаш қонунчилик механизмларини жорий қилиб, шахсий маълумотларни ҳимоя қилиш ва кибер жиноятларга қарши жазо чораларини кучайтириш.

– **Технологик инфратузилмани ривожлантириш**: Сунъий интеллект ва блокчейн технологияларини кибер таҳдидларни аниқлаш ва зарарсизлантиришда қўллаш.

– **Халқаро ҳамкорликни кенгайтириш**: Europol, Интерпол ва CISA каби ташкилотлар билан маълумот алмашинуви ва биргаликдаги операцияларни кучайтириш.

– **Мутахассислар тайёрлаш**: Киберхавфсизлик мутахассисларини тайёрлаш учун таълим дастурларини ривожлантириш ва хорижий тажриба алмашинувини ташкил қилиш .

– **Жамоатчиликни хабардор қилиш**: Ижтимоий тармоқлар ва мактаблар ва университетларда киберхавфсизлик бўйича махсус дарслар ёки семинарлар ташкил қилиш зарур.

– **Хусусий сектор билан ҳамкорлик**: Маҳаллий IT компаниялари ва молиявий платформалар билан биргаликда киберхавфсизлик лойиҳаларини амалга ошириш.

– **Миллий киберхавфсизлик стратегияси**: Давлат, хусусий сектор ва таълим муассасалари ўртасидаги фаолиятни мувофиқлаштирувчи яхлит стратегия ишлаб чиқиш.

Ушбу тавсияларни амалга ошириш Ўзбекистоннинг киберхавфсизлик тизимини глобал стандартларга мослаштиришга ва кибер жиноятларга қарши курашишнинг самарадорлигини оширишга хизмат қилади. Келгусида Ўзбекистон нафақат миллий, балки минтақавий миқёсда киберхавфсизлик соҳасида етакчи давлатга айланиш имкониятига эга.

---

[34] Qodirov, S. "Киберхавфсизлик қонунчилиги." Юридик фанлар журнали, 2024.

[35] Interpol. "Global Cybercrime Programme." https://www.interpol.int/, 2024.

[36] Smith, J. "Global Cybercrime Trends." Journal of Cybersecurity, 2023.