КИБЕРЖИНОЯТЛАР ПРОФИЛАКТИКАСИНИНГ ТАШКИЛИЙ-ТЕХНИК ЧОРАЛАРИ: ИЛҒОР ХОРИЖИЙ ТАЖРИБАНИ МИЛЛИЙ ТИЗИМГА ИМПЛЕМЕНТАЦИЯ ҚИЛИШНИНГ ДОЛЗАРБ ЙЎНАЛИШЛАРИ

Марзажонов Шохрухбек Собиржонович
Ўзбекистон Республикаси Криминология тадқиқоти институти мустақил изланувчиси

Аннотация: Тезисда кибержиноятларнинг трансчегаравий ва аноним хусусияти миллий хавфсизлик ҳамда иқтисодий барқарорликка таҳдид сифатида баҳоланади. Профилактиканинг самарадорлиги ташкилий-ҳуқуқий механизмлар (норматив базани такомиллаштириш, давлат-хусусий шериклиги, ахборот алмашинуви, кадрлар салоҳияти) ва техник ечимлар (CERT/CSIRT, криптография, инцидентларга тезкор жавоб, реал вақт мониторинги) уйғунлигига боғлиқ экани асосланади. Илғор тажриба сифатида ЕИ (NIS2, “Secure by Design/Default”), АҚШ (NIST CSF, “Zero Trust”, “Assume Breach”), Хитой (MLPS 2.0) каби ёндашувлар қиёсий таҳлил қилинади. Ўзбекистоннинг GCI 2024 контекстида миллий тизимни кучайтириш учун мажбурий инцидент хабарномаси, секторал CSIRTлар, кибер-аудитни институционаллаштириш ва рақамли маҳсулотлар хавфсизлигига доир стандартларни ҳуқуқий мустаҳкамлаш бўйича таклифлар илгари сурилади.

Калит сўзлар: кибержиноятлар профилактикаси; ташкилий-техник чоралар; CERT/CSIRT; кибер-инцидент; ITU GCI; давлат-хусусий шериклиги; NIS2; NIST CSF; Zero Trust; имплементация.

Аннотация: В тезисе киберпреступность рассматривается как трансграничная и анонимная угроза национальной безопасности и экономической устойчивости. Обосновывается, что результативная профилактика требует сочетания организационно-правовых механизмов (совершенствование нормативной базы, государственно-частное партнёрство, обмен информацией, развитие кадрового потенциала) и технических инструментов (CERT/CSIRT, криптография, оперативное реагирование на инциденты, мониторинг в реальном времени). В качестве лучших практик анализируются подходы ЕС (NIS2, Secure by Design/Default), США (NIST CSF, Zero Trust, Assume Breach) и Китая (MLPS 2.0). В контексте показателей Узбекистана в GCI 2024 предлагаются направления усиления национальной системы: введение обязательного уведомления об инцидентах, создание отраслевых CSIRT, институционализация кибераудита и правовое закрепление стандартов безопасности цифровых продуктов.

Ключевые слова: профилактика киберпреступлений; организационно-технические меры; CERT/CSIRT; киберинциденты; ITU GCI; ГЧП; NIS2; NIST CSF; Zero Trust; имплементация.

Abstract: The thesis frames cybercrime as a cross-border and anonymous threat to national security and economic resilience. It argues that effective prevention depends on the alignment of organizational-legal mechanisms (regulatory improvement, public–private partnership, information sharing, and capacity building) with technical capabilities (CERT/CSIRT, cryptographic protection, rapid incident response, and real-time monitoring). The paper highlights comparative best practices from the EU (NIS2; Secure by Design/Default), the United States (NIST CSF; Zero Trust; Assume Breach), and China (MLPS 2.0). With reference to Uzbekistan's GCI 2024 context, it proposes priority measures for strengthening the national system, including mandatory incident notification, sectoral CSIRTs, institutionalized cyber-audit, and legally enforceable security standards for digital products.

Keywords: cybercrime prevention; organizational and technical measures; CERT/CSIRT; cyber incident; ITU GCI; public–private partnership; NIS2; NIST CSF; Zero Trust; implementation.

Сўнгги йилларда дунё миқёсида *"кибер-тенгсизлик" (cyber inequity)* муаммоси ҳам юзага келмоқда. Кичик ва ўрта бизнес корхоналари йирик корпорацияларга нисбатан киберҳужумларга кўпроқ заиф бўлиб қолмоқда. Тадқиқотларга кўра, киберҳужумларнинг 50 фоиздан ортиғи айнан кичик ва ўрта бизнес субъектларига қаратилган бўлиб, уларнинг аксарияти бундай таҳдидларга қарши туриш учун етарли ресурсларга эга эмас[1]. Бу эса давлат томонидан ташкилий-техник кўмак механизмларини ишлаб чиқиш заруратини янада оширади.

Dapo Akande, Antonio Coco ва *Talita Dias* кибермаконни алоҳида ҳуқуқий вакуум деб эмас, балки мавжуд халқаро ҳуқуқ нормалари амал қиладиган муҳит сифатида талқин қиладилар[2]. Уларнинг қарашича, кибер-операциялар орқали бошқа давлатнинг ички ишларига аралашиш тақиқланган ва бу борада ривожланган давлатларнинг прецедентларини ўрганиш миллий норма ижодкорлигида хатоликлардан қочишга ёрдам беради.

Kubo Mačák, Laurent Gisel ва *Tilman Rodenhäuser* бўлса, соғлиқни сақлаш соҳасини киберҳужумлардан ҳимоя қилишнинг ҳуқуқий жиҳатларини тадқиқ этганлар[3]. Улар кибержиноятларнинг профилактикасида критик инфратузилмани алоҳида ҳимоя қилиш бўйича халқаро консенсус зарурлигини илгари сурадилар.

Michael N. Schmitt эса, кибер-суверенитет ва сайлов жараёнларига кибер-аралашув масалаларида етакчи эксперт ҳисобланади. Унинг *"Таллин қўлланмаси"* (Tallinn Manual) лойиҳасидаги иштироки кибержиноятчиликка қарши курашнинг халқаро стандартларини белгилашда пойдевор бўлиб хизмат

[1] Global Cybersecurity Outlook 2024 // https://www3.weforum.org/docs/WEF_Global_-Cybersecurity_Outlook_2024.pdf

[2] *Dapo Akande, Antonio Coco, Talita Dias* "The Oxford Process on International Law Protections in Cyberspace" // Part I - International Law Protections of the Healthcare Sector,
– P. 13. /https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf
Kubo Mačák, Laurent Gisel, Tilman Rodenhäuser "The Oxford Process on International Law Protections in Cyberspace" // Part II - International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research, – P. 128. /https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf

қилди[4]. *Michael N. Schmitt* қарашларига кўра, давлатлар кибержиноятларга қарши жавоб чораларини (countermeasures) кўришда халқаро ҳуқуқ доирасида ҳаракат қилишлари ва бу борада АҚШ ва ЕИ каби давлатларнинг амалиётини ўрганишлари муҳимдир.

Шунингдек, *Kate Jones* рақамли муҳитда инсон ҳуқуқларини ҳимоя қилиш, хусусан, онлайн манипуляция ва дезинформацияга қарши курашнинг ҳуқуқий асосларини ёритиб берган[5]. У кибержиноятлар профилактикасини нафақат техник чеклов, балки фикр эркинлигини таъминловчи ташкилий тизим сифатида кўради. *Scott J. Shackelford, Scott Russell* ва *Andreas Kuehn* кибер-тинчлик *(cyber peace)* концепциясини ривожлантириб, хусусий сектор ва давлат ўртасидаги ҳамкорликнинг ташкилий моделларини таҳлил қилганлар[6]. Уларнинг фикрича, ривожланган давлатлардаги *“давлат-хусусий шериклиги”* механизми кибержиноятчиликнинг олдини олишда энг самарали воситадир. Колимбиялик олим *Juan David Gutiérrez Rodriguez* ва Сенегаллик олим *Jean Aloise Ndiaye* эса сунъий интеллект тизимларининг кибержиноятчиликдаги роли ва уларни ҳуқуқий жиҳатдан жиловлаш масалаларини тадқиқ этганлар[7]. Уларнинг илмий қарашлари кибержиноятлар профилактикасида алгоритмик шаффофликни таъминлашга қаратилган.

Нигериялик олим *Jake Okechukwu Effoduh* бўлса, кибермакондаги дискриминация ва технологияларнинг инсон ҳуқуқларига таъсирини ўрганиб, ривожланаётган давлатлар учун технологияларни импорт қилишда хавфсизлик стандартларини қатъий белгилаш лозимлигини таъкидлайди[8]. Шунингдек, *Przemysław Roguski* ва *Lori F. Damrosch* киберҳужумларга қарши жамоавий жавоб чораларини қўллашнинг ҳуқуқий асосларини таҳлил қилиб, халқаро ҳамкорликнинг ташкилий механизми сифатида *“колектив хавфсизлик”* тушунчасини кибермаконга мослаштиришни таклиф этадилар[9]. Италиянинг Милан университети профессори *Giovanna Adinolfi* ўз асарида халқаро иқтисодий ҳуқуқ ва киберхавфсизлик ўртасидаги боғлиқликни ўрганиб, профилактика чораларини иқтисодий санкциялар ва савдо чекловлари билан қандай мувофиқлаштириш мумкинлигини кўрсатиб берган[10]. *Barrie Sander*

---

[4] *Michael N. Schmitt.* Background Paper: Foreign Cyber Interference in Elections: // Part III - International Law Protections Against Foreign Electoral Interference Through Digital Means – P. 211. /https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf

[5] *Kate Jones.* Background Paper: Protecting Political Discourse from Online Manipulation: the International Human Rights Law Framework // Part III - International Law Protections Against Foreign Electoral Interference Through Digital Means – P. 233. /https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf

[6] *Scott J. Shackelford, J.D., Scott Russell, J.D., & Andreas Kuehn* Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors – P. 32. // https://chicagounbound.uchicago.edu

[7] *Juan David Gutiérrez Rodriguez & Jean Aloise Ndiaye.* UNESCO Network of Experts on AI and the Rule of Law // https://www.unesco.org/en/artificial-intelligence/rule-law/network-experts

[8] *Jake Okechukwu Effoduh.* UNESCO Network of Experts on AI and the Rule of Law // https://www.unesco.org/en/artificial-intelligence/rule-law/network-experts

[9] *Przemysław Roguski & Lori F.* Damrosch Dapo Akande, Antonio Coco, Talita Dias “The Oxford Process on International Law Protections in Cyberspace” // Part VII - Countermeasures in Cyberspace – *pp*. 507, 521. /https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf

[10] *Giovanna Adinolfi.* States’ Measures to Counter Cyberattacks from the Perspective of International Economic Law. - p. 19 / https://eucd.s3.eu-central-1.amazonaws.com

кибермаконда инсон ҳуқуқларини бошқариш тизимини тадқиқ этади ва рақамли суверенитетни ҳимоя қилишда индивидуал эркинликларни чеклаб қўймаслик муҳимлигини алоҳида таъкидлайди[11].

Вера Русинова [12] ва ҳалқаро ҳуқуқшунос олим, профессор *Duncan Hollis*[13] илмий ёндашувича кибер-операцияларни *"куч ишлатиш билан таҳдид қилиш" (threat of force)* контекстида ўрганиб, БМТ Низомининг кибермакондаги талқини бўйича илмий мулоҳазалар юритганлар. Уларнинг фикрича, кибержиноятлар профилактикасининг ташкилий чоралари давлатлараро можароларнинг олдини олишга хизмат қилиши керак. Бундан ташқари, Европа Иттифоқининг рақамли сиёсат ва киберхавфсизлик йўналишларида фаол иштирок этувчи сиёсий арбоблардан бири бўлган Финландиялик сиёсатчи *Henna Virkkunen* эса ўзининг *"Europe's New Cyber Rules Target China — and US"* номли асарида Европа Иттифоқининг технологик суверенитети ва хавфсизлиги бўйича стратегик қарашларни илгари суриб, Хитой ва АҚШ технологияларига қарамликни камайтиришнинг ташкилий йўлларини кўрсатиб ўтган[14].

Шунингдек, Маврикий Республикасининг Ахборот технологиялари, коммуникация ва инновациялар вазири *Deepak Balgobin* фикрича "сўнгги беш йил мобайнида вазирлик томонидан, CERT-MU *(Computer Emergency Response Team – Mauritius)* кўмагида амалга оширилган муҳим ташаббуслар ҳақида ҳам маълумот берди. Жумладан, қуйидаги ташаббус ва норматив-ҳуқуқий ҳужжатлар жорий амалиётга жорий этилган. Буларга:

Maucors — кибержиноятлар ҳақида онлайн хабар бериш тизими;

Cybersecurity and Cybercrime Act 2021 — "Киберхавфсизлик ва кибержиноятчилик тўғрисида"ги қонун;

Maushield — киберҳужумлар бўйича ахборот алмашиш миллий тизими;

National Cybersecurity Strategy 2023–2026 — Миллий киберхавфсизлик стратегияси;

MauHNET — Маврикий Honeynet лойиҳаси (киберҳужумларни мониторинг қилиш ва таҳлил этишга қаратилган инфратузилма).

Шунингдек, у Маврикий Республикасини Маврикий Африка қитъасида ва Жанубий ярим шарда SIM3 сертификатини олган биринчи давлат ҳисобланади, бу эса миллий CERT тизимининг халқаро стандартларга мувофиқлигини тасдиқлайди дейди.

1. Ташкилий-ҳуқуқий асослар ва "Due Diligence" принципи;

2. Критик инфратузилма ва тармоқлараро ҳамкорлик;

[11] *Barrie Sander*. Human Rights and Cybersecurity Governance, - *pp*. 31-33 // international-law-and-cybersecurity-governance.pdf

[12] *Вера Русинова*. Application of Sovereignty to Information and Communications Technologies - *pp*. 31-33 // international-law-and-cybersecurity-governance.pdf

[13] *Duncan Hollis.* The Oxford Process on International Law Protections in Cyberspace. – *P.* 146. /https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf

[14] *Henna Virkkunen* "Europe's New Cyber Rules Target China — and US" // https://cepa.org/article/europes-new-cyber-rules-target-china-and-us

3. Технологик суверенитет ва стандартлаштириш;

4. Инсон ҳуқуқлари ва рақамли этика мутаносиблиги;

Шу ўринда, хорижий давлатлар тажрибасини илмий таҳлил қилишдан аввал халқаро ҳуқуқшунос ва хорижий олимларнинг илмий-назарий қарашларини ёритишнинг аҳамияти нимада, деган мантиқий савол юзага келади. Ушбу саволга жавоб сифатида таъкидлаш жоизки, ҳар қандай давлат амалиёти муайян назарий концепциялар ва ҳуқуқий доктриналар замирида шаклланади. Шу боис амалиётни унинг илмий пойдеворидан ажратиб ўрганиш тадқиқотнинг концептуал асосланганлигини сусайтириши мумкин.

Эндиликда, кибержиноятларга қарши кураш ва профилактика самарадорлигини баҳолашда Халқаро электр алоқа иттифоқи (ITU) томонидан 2025 йил 17 мартдаги эълон қилинадиган *Глобал киберхавфсизлик индекси* (GCI) асосий кўрсаткич ҳисобланади. 2024 йилги GCI ҳисоботида мамлакатларни гуруҳлашнинг янги тизими жорий этилди[15]. Мазкур натижаларга кўра, киберхавфсизликнинг *ҳуқуқий асослар, техник чоралар, ташкилий салоҳият, кадрлар тайёрлаш, ҳамкорлик механизмлари ва халқаро интеграция даражаси* бўйича энг юқори кўрсаткичларга эга бўлган давлатлар қаторига қуйидагилар киритилди. Буларга:

Рейтинг / Ўрин	**Давлат**	**GCI 2024 Скор** (100 баллик тизимда)	**Асосий кучли томонлари**
1	**Дания**	100	Халқаро ҳамкорлик ва ташкилий бошқарув
1	**Финляндия**	100	Техник чоралар ва кадрлар салоҳияти
1	**Саудия Арабистони**	100	Ташкилий стратегия ва ҳуқуқий база
1	**Жанубий Корея**	100	Технологик инновациялар ва кибер-барқарорлик
1	**Бирлашган Араб Амирликлари**	100	Рақамли инфратузилма хавфсизлиги ва инвестиция
1	**Буюк Британия**	100	Миллий киберхавфсизлик

[15] https://codesealer.com/blog/itu-global-cybersecurity-index-2024-a-changing-cybersecuri-ty-landscape

			маркази (NCSC) фаолияти
1	**Италия**	100	Норматив тартибга солиш ва давлат назорати
1	**Маврикий**	100	Африка минтақасидаги кибер-хаб роли
1	**Туркия**	100	Техник ҳимоя ва миллий CSIRT тизими
1	**Миср**	100	Минтақавий ҳамкорлик ва ҳуқуқий нормалар

Ушбу давлатларнинг тажрибаси шуни кўрсатадики, киберхавфсизликнинг юқори даражасига фақатгина техник воситалар билан эмас, балки тизимли ташкилий чоралар орқали эришилади. *Масалан,* **Даниянинг** юқори кўрсаткичи унинг ***халқаро ва ички ҳамкорлик*** (cooperation) механизмларининг ниҳоятда кучлилиги билан изоҳланади. **Германия** ва **Швейцария** каби иқтисодий бақувват давлатларнинг рейтингда бир оз пастлагани айнан ҳамкорлик ва мувофиқлаштириш ишларидаги камчиликлар билан боғлиқ деб топилган[16].

АҚШ кибержиноятлар профилактикасида *“хавфларни бошқариш” (risk management)* ва *“интеграциялашган назорат”* тамойилига таянади.

АҚШда кибержиноятлар профилактикасининг ташкилий чоралари: Миллий стандартлар ва технологиялар институти (NIST) томонидан ишлаб чиқилган *“Cybersecurity Framework”* (CSF) нафақат АҚШда, балки бутун дунёда стандарт сифатида қабул қилинган. У бешта асосий функцияни ўз ичига олади: *а) идентификация; б) ҳимоя қилиш; в) аниқлаш; г) жавоб бериш; д) тиклаш.* АҚШда киберхавфсизлик нафақат IT мутахассисларнинг, балки ташкилот раҳбариятининг *(Executive level)* масъулияти сифатида белгиланган.

Хитой давлати кибермаконда *“кибер-суверенитет”* концепциясини илгари суради ва кибержиноятлар профилактикасини давлат назорати билан чамбарчас боғлайди.

Россия Федерациясида эса кибермаконни миллий хавфсизликнинг ажралмас қисми деб ҳисоблайди ва асосий эътиборни давлатнинг рақамли мустақиллигини таъминлашга қаратади. Хусусан, *ташкилий чоралар бўйича фаолиятига:*

- ***Марказлашган бошқарув;***
- ***Меъёрий-ҳуқуқий база;***
- ***Жиноий-ҳуқуқий профилактика.***

[16] https://codesealer.com/blog/itu-global-cybersecurity-index-2024-a-changing-cybersecuri-ty-landscape

Техник чоралар бўйича фаолиятига:

- ***техник воситаларни жорий этиш (ТСПУ);***
- ***импорт ўрнини босиш;***
- ***миллий DNS тизими;***

Европа Иттифоқи (ЕИ). Жумладан:

- ***ташкилий чоралар бўйича фаолияти;***
- ***техник чоралар бўйича фаолияти;***

Шунингдек, GCI натижаларига кўра, Ўзбекистон киберхавфсизлик соҳасида *"Advancing"* (фаол ривожланаётган) давлатлар қаторига киритилиб, 89,2 балл билан *Tier 2* гуруҳида эътироф этилди[17].

Кибержиноятлар профилактикаси нуқтаи назаридан ушбу рейтинг натижалари алоҳида аҳамиятга эга. Чунки GCI баҳолаш мезонлари қатор омилларни — ҳуқуқий асослар, техник чоралар, ташкилий салоҳият, кадрлар тайёрлаш, ҳамкорлик механизмлари ва халқаро интеграция даражасини қамраб олади. Демак, Ўзбекистоннинг юқори гуруҳга киритилиши кибержиноятлар профилактикаси тизимида комплекс ёндашув шаклланаётганини кўрсатади.

Шу тариқа, GCI 2024 рейтингида Ўзбекистоннинг *"фаол ривожланаётган"* давлатлар қаторига киритилиши кибержиноятлар профилактикаси тизимида амалга оширилаётган чора-тадбирларнинг ижобий самарасини кўрсатиш билан бирга, ***мазкур соҳадаги ислоҳотларни янада чуқурлаштириш зарурлигини ҳам белгилаб беради***. Бу эса диссертация доирасида ташкилий-техник чораларни такомиллаштириш ва илғор хорижий тажрибани миллий тизимга имплементация қилиш бўйича илмий таклифларни ишлаб чиқишнинг долзарблигини янада асослайди.

Ривожланган давлатларнинг тажрибасини таҳлил қилиш шуни кўрсатадики, кибержиноятлар профилактикасининг муваффақияти қуйидаги *учта омилнинг мутаносиблигига боғлиқ*:

1. *Жавобгарликнинг тақсимланиши*;
2. *Маълумот алмашинувининг тезкорлиги*;
3. *Инсон капиталига инвестиция*.

Юқорида маълум қилганимиздек, янги Ўзбекистон GCI 2024 рейтингида 89,2 балл билан *"Advanced"* (Тиер 2) гуруҳига киргани мамлакатда ҳуқуқий базанинг мустаҳкамлигидан далолат беради[18]. Бироқ, техник ва салоҳиятни ошириш *(Capacity Development)* устунлари бўйича ҳали ўсиш заҳиралари мавжудлигини кўрсатади.

Ўтказилган тадқиқот ва қиёсий таҳлил натижасида миллий қонунчиликда кибержиноятлар профилактикасининг ташкилий-техник чоралари билан боғлиқ қуйидаги ҳуқуқий бўшлиқлар кўзга ташланмоқда. Буларга:

Биринчидан, ***маълумотлар сизиб чиқиши (data breach) учун жавобгарликнинг номутаносиблиги;***

Иккинчидан, ***кибер-инцидентларни бошқаришда "Ягона дарча" механизмининг йўқлиги;***

[17] https://codesealer.com/blog/itu-global-cybersecurity-index-2024-a-changing-cybersecuri-ty-landscape

[18] CIS countries' results in the field of cybersecurity according to the Global Cybersecurity Index 2024 and the role of ITU cyberdrills in improving the readiness of countries to respond to cyberthreats // https://www.itu.int

Учинчидан, ***IT таъминот занжири хавфсизлиги (Supply Chain Security) бўйича нормаларнинг йўқлиги;***

Тўртинчидан, ***секторал CSIRT марказларининг етишмаслиги;***

Бешинчидан, ***кибер-аудит тушунчасининг декларативлиги***.

Юқорида илгари сурилган илмий муаммоларни бартараф этиш ва хорижий тажрибани миллий қонунчиликка самарали имплементация қилиш мақсадида қуйидаги илмий асослантирилган таклифлар илгари сурилади. Буларга:

Биринчидан, кибержиноятлар профилактикасининг техник чоралари самарадорлигини ошириш мақсадида, ахборот тизимлари ва дастурий маҳсулотларни ишлаб чиқувчи субъектларнинг масъулиятини кучайтириш лозим. Шу каби салбий ҳолатларни олдини олиш мақсадида ***"Киберхавфсизлик тўғрисида"***ги Ўзбекистон Республикаси Қонунига қуйидаги мазмундаги ***19^1-модда*** киритиш таклиф этилади:

"19^1-модда. Технология ва дастурий маҳсулот етказиб берувчиларнинг жавобгарлиги".

Иккинчидан, кибержиноятлар профилактикасининг самарадорлиги кўп жиҳатдан давлатнинг реал вақт режимида таҳдидлардан хабардорлигига боғлиқ. Шу каби салбий ҳолатларни олдини олиш мақсадида ***"Киберхавфсизлик тўғрисида"***ги Ўзбекистон Республикаси Қонунига қуйидаги мазмундаги ***24^1-модда*** киритиш таклиф этилади.

*"****24^1-модда. Кибер-инцидентлар тўғрисида мажбурий хабардор қилиш****";*

Учинчидан, кибержиноятлар профилактикасининг иқтисодий механизмларини такомиллаштириш мақсадида, МЖтКнинг амалдаги *"Шахсга доир маълумотлар тўғрисидаги қонунчиликни бузиш"* деб номланган ***46^2-моддасини қуйидани мазмундаги учинчи*** қисм билан тўлдириш таклифи илгари сурилади.

"46^2-модда. Шахсга доир маълумотлар тўғрисидаги қонунчиликни бузиш"*;*

Тўртинчидан, бугунги кунда кибержиноятларнинг 80 фоиздан ортиғи фойдаланувчиларнинг оддий техник хатолари ёки эҳтиётсизлиги оқибатида содир бўлишини инобатга олиб, мамлакат миқёсида мажбурий кибер-гигиена қоидаларини ўзида мужассам этган Ўзбекистон Республикаси Вазирлар Маҳкамасининг ***"Кибер-гигиенанинг миллий стандартларини тасдиқлаш ва амалиётга жорий этиш чора-тадбирлари тўғрисида"***ги Қарорини қабул қилиш таклиф этилади;

Бешинчидан, кибержиноятларнинг глобал ва трансчегаравий характерини инобатга олган ҳолда, уларга қарши курашишда давлат ва хусусий секторнинг имкониятларини бирлаштирувчи ягона "Миллий кибер-кооперация платформаси" *(National Cyber Cooperation Platform – NCCP)* ахборот муҳитини яратиш зарур.

Хулоса ўрнида шуни таъкидлаш жоизки, кибержиноятлар профилактикасининг ташкилий-техник чораларини такомиллаштириш ва илғор хорижий тажрибани имплементация қилиш янги Ўзбекистон учун стратегик аҳамиятга эгадир. Таҳлиллар шуни кўрсатадики, дунёнинг етакчи давлатлари

(АҚШ, Хитой, Россия, ЕИ) кибержиноятчиликка қарши курашда нафақат техник тўсиқларни кучайтирмоқда, балки масъулият ва жавобгарликнинг янги ташкилий моделларини яратмоқда. Янги Ўзбекистоннинг ушбу соҳадаги ютуқларини мустаҳкамлаш учун қонунчиликдаги мавжуд бўшлиқларни тўлдириш, хусусан, компанияларнинг масъулиятини ошириш, мажбурий хабар бериш тизимини жорий этиш ва секторал ҳамкорликни йўлга қўйиш зарур. Илмий асосланган таклифларнинг амалиётга татбиқ этилиши мамлакатнинг рақамли барқарорлигини таъминлашга ва фуқароларнинг кибермакондаги хавфсизлигини кафолатлашга хизмат қилади. *Киберхавфсизлик* — бу доимий жараён бўлиб, у халқаро тажрибани мунтазам ўрганишни ва миллий қонунчиликни янги таҳдидларга мослаштиришни талаб этади.