Conference on Social Sciences and Humanities Research (CSSHR)
volume. 3 № 4
CSSHR
EYIB EDUCATIONAL YIELD INSIGHTS & BREAKTHROUGHS
ISSN: 3060-4648

БАНК-МОЛИЯ ВА ТЕЛЕКОММУНИКАЦИЯ СОҲАЛАРИДА КИБЕРЖИНОЯТЛАР ПРОФИЛАКТИКАСИНИ ТАКОМИЛЛАШТИРИШ: ҲУҚУҚИЙ-ТАҲЛИЛИЙ ВА ТЕХНОЛОГИК ЁНДАШУВЛАР УЙҒУНЛИГИ

Марзажонов Шохрухбек Собиржонович,

Ўзбекистон Республикаси Криминология тадқиқоти институти мустақил изланувчиси

Аннотация: Ушбу тезисда Янги Ўзбекистон шароитида банк-молия ва телекоммуникация тармоқларида кибержиноятлар профилактикасини таъминлашга қаратилган ҳуқуқий механизмлар ва амалий тартиб-таомиллар таҳлил қилинади. Мавжуд норматив тартибга солишдаги зиддиятлар ҳамда “регулятор бўшлиқлар” аниқланиб, профилактиканинг фақат техник ҳимоя билан чекланмаслиги, балки ҳуқуқий жавобгарлик, ташкилотларнинг профилактик масъулияти, рақамли ҳуқуқий онг ва кибермаданиятни қамраб олган интеграл тизим сифатида қурилиши асосланади. Шунингдек, телеком операторлари кесимида антифрод ечимларни марказлаштириш, киберрискларни суғурталаш механизмларини жорий этиш ва трансчегаравий рақамли далиллар алмашинувини такомиллаштириш бўйича таклифлар баён этилади.

Калит сўзлар: кибержиноят; профилактика; антифрод; регулятор бўшлиқ; юридик шахс масъулияти; кибермаданият; киберриск суғуртаси; рақамли далил.

Аннотация: В тезисе рассматриваются актуальные вопросы профилактики киберпреступности в банково-финансовом и телекоммуникационном секторах в условиях «Нового Узбекистана». Анализируются действующие правовые механизмы и практики правоприменения, выявляются противоречия регулирования и ключевые «регуляторные пробелы». Обосновывается необходимость понимания профилактики как интегральной системы, включающей не только техническую защиту, но и меры юридической ответственности, усиление профилактической ответственности организаций, формирование цифрового правосознания и киберкультуры. Дополнительно предлагаются направления централизации телеком-антифрод-решений, развития страхования киберрисков и совершенствования трансграничного обмена цифровыми доказательствами.

Ключевые слова: киберпреступность; профилактика; антифрод; регуляторные пробелы; ответственность юридических лиц; киберкультура; страхование киберрисков; цифровые доказательства.

Abstract: This thesis highlights key challenges in preventing cybercrime in the banking/financial and telecommunications sectors within the “New Uzbekistan” context. It examines existing legal mechanisms and enforcement practices, identifying regulatory inconsistencies and major “regulatory gaps.” The paper argues that prevention should be

treated as an integrated framework extending beyond technical protection to include legal liability, strengthened organizational preventive duties, and the promotion of digital legal awareness and cyber culture. It further outlines policy options for centralizing telecom anti-fraud solutions, advancing cyber-risk insurance instruments, and improving cross-border transfer and admissibility of digital evidence.

Keywords: cybercrime; prevention; anti-fraud; regulatory gaps; corporate liability; cyber culture; cyber-risk insurance; digital evidence.

Ҳеч кимга сир эмаски, сўнгги йилларда янги Ўзбекистонда интернет фойдаланувчилари сони 31 миллиондан ошган бир шароитда, кибержиноятлар сонининг 68 бараварга ошганлиги кузатилди[1]. 2025 йилнинг ўзида 46 мингдан ортиқ кибержиноят ҳолатлари қайд этилиб, улар натижасида кўрилган молиявий зарар 1,2 триллион сўмдан ортиб кетган[2]. Ушбу жиноятларнинг аксарияти, яъни 98 фоизи айнан банк карталари билан боғлиқ фирибгарлик ва ўғирликлар ҳиссасига тўғри келади[3]. Банк-молия ва телекоммуникация соҳалари кибержиноятчилар учун асосий нишон бўлиб қолмоқда, чунки бу ерда энг катта молиявий ресурслар ва шахсий маълумотлар жамланган.

Президент *Ш. Мирзиёев* томонидан 2022-2026 йилларга мўлжалланган тараққиёт стратегиясининг *“Фуқароларнинг ахборот олиш ва тарқатиш эркинлиги борасидаги ҳуқуқларини янада мустаҳкамлаш”* деб номланган 89-мақсаднинг 327-бандида ахборот технологиялари ҳужумларидан ҳимояланиш ва киберхавфсизликни таъминлаш тизимини яратиш бўйича аниқ вазифалар қўйилган[4]. Бу борада нафақат техник ҳимоя воситаларини кучайтириш, балки ҳуқуқий базани такомиллаштириш ва аҳолининг кибермаданиятини ошириш ҳам муҳим аҳамият касб этади. Давлат раҳбарининг таъкидлашича, кибержиноятчиликка қарши курашишда давлат органлари, банк тизими ва фуқаролик жамияти институтларининг жипслашиши талаб этилади.

Шу ўринда, бугунги кунда янги Ўзбекистонда рақамли трансформация жараёнларининг жадаллашиши ижтимоий-иқтисодий соҳаларда ижобий ўзгаришлар билан бирга, кибермакондаги таҳдидларнинг ҳам экспоненциал равишда ўсишига олиб келмоқда. Маҳаллий олимлар ва экспертларнинг фикрича, ушбу муаммони ҳал этиш комплекс илмий ёндашув ва кўп босқичли профилактика тизимини талаб этади.

Маҳаллий ҳуқуқшунос олимлар кибержиноятчиликни ижтимоий ва техник омилларнинг мураккаб ўзаро таъсири сифатида баҳоламоқдалар. *Ф.Э. Жураевнинг* тадқиқотларига кўра, *“кибержиноят”* тушунчаси анъанавий *“компьютер жинояти”* тушунчасидан кенгроқ бўлиб, у ахборот маконида содир этиладиган ҳар қандай жиноий қилмишлар мажмуини қамраб олади. Ушбу жиноятларнинг асосий белгилари сифатида *трансчегаравийлик, юқори даражадаги*

[1] *Мирзиёев Ш.М.* Ҳамма ислоҳотларни, ҳамма ҳаракатларни жамият билан бирга қиламиз // www.president.uz/uz/lists/view/4942
[2] Кибержиноятлар сони 68 баробарга кўпайган // https://kknews.uz/uz/270441.html
[3] Инсон ҳуқуқлари бўйича Ўзбекистон Республикаси Миллий маркази расмий веб-сайти //
[4] https://lex.uz/docs/5841063

латентлик (90% гача) ва *жиноят субъектининг интеллектуал салоҳияти* юқорилиги кўрсатилади[5].

Шунингдек, *А.А. Таштемиров* кибержиноятчиликнинг тарихий шаклланиш босқичларини таҳлил қилар экан, унинг генезисини 1960 йиллардаги илк ҳакерлик ҳаракатлари ва 1980 йиллардаги "компьютер вируслари" эпидемияси билан боғлайди. Олимнинг фикрича, кибержиноятчилик шахсларнинг соддалиги ва ҳуқуқий билими етишмаслигидан фойдаланишнинг замонавий кўриниши бўлиб, бугунги кунда ижтимоий тармоқ мессенжерлари орқали ўзгалар мулкини талон-торож қилиш энг кўп тарқалаётган шакл ҳисобланади[6]. *Д.Б. Сафарова*[7] эса кибермакондаги жиноятларнинг келиб чиқишини ижтимоий-иқтисодий омиллар билан боғлайди. Унинг таҳлилига кўра, иқтисодий инқироз, ишсизлик даражасининг ошиши ва зарур товарлар нархининг кўтарилиши шахсларнинг кибержиноятчиликка қўл уришига замин яратмоқда. Шу билан бирга, виктимологик омиллар ҳам муҳим аҳамиятга эгадир. Унинг таҳлилларига шуни кўрсатадики, кўп ҳолатларда жабрланувчиларнинг ўзи шахсий маълумотларини ошкор қилиш ёки зарарли ҳаволаларга кириш орқали жиноятга шароит яратиб бермоқдалар.

Шу ўринда, Ички ишлар вазири *А.А. Тошпўлатов* ҳам кибержиноятчилик нафақат янги Ўзбекистонда балки жаҳон ҳамжамияти миқёсида ҳам кескин ўсиб бораётганлигини тасдиқлайди. Хусусан, у сўнгги беш йилда ахборот технологиялари ёрдамида содир этилган жиноятлар 68 бараварга ошгани, *2024* йил якунларига кўра, кибержиноятларнинг умумий жиноятчиликдаги улуши *44,4* фоизни ташкил этгани, уларнинг асосий қисми (98%) банк карталаридан маблағларни ноқонуний ўзлаштириш билан боғлиқ эканлигига алоҳида урғу беради.

Мазкур маҳаллий олимлар ва соҳа экспертларининг кибержиноятчиликнинг олдини олишни қуйидаги учта стратегик йўналиш доирасида амалга оширишни илгари сураётганликларини кўришимиз мумкин. Буларга:

- *Техник-технологик профилактика*.
- *Ҳуқуқий-институционал профилактика*.
- *Маърифий-тарбиявий профилактика*.

Хорижий илмий адабиётларда эса кибержиноятчилик ва унинг профилактикаси борасида бир қатор фундаментал назариялар ҳам мавжуд бўлиб, улар мазкур параграфнинг илмий мазмунини бойитишга хизмат қилади. Хусусан, *К.Н. Евдокимовнинг* ўзининг докторлик диссертациясида *"Технотрон жиноятчилик"* (Technotron crime) концепциясини илгари суради[8]. Унинг фикрича, биз тўртинчи илмий-техник инқилоб даврида яшамоқдамиз, бу даврда анъанавий компьютер жиноятлари назорат қилиб бўлмайдиган технотрон жиноятчиликка трансформация

[5] *Джураев Ф.Э.* "Кибержиноятлар тушунчаси, белгилари ва шахсий изкуварлик маҳорати орқали уларни олдини олиш ва фош этилишининг аҳамияти ҳақида айрим мулоҳазалар" // Central Asian Research Journal For Interdisciplinary Studies (CARJIS) ISSN (online): 2181-2454

[6] *Тоштемиров А.А.* "Кибержиноятчилик ва уни ўзига хос шаклланиш даврлари" // "Замонавий дунёда ижтимоий фанлар: назарий ва амалий изланишлар" номли илмий, масофавий, онлайн конференция

[7] *Сафарова, Д. Б.* Кибермакондаги жиноятларнинг ижтимоий-иқтисодий ва виктимологик омиллари таҳлили. *"Юридик фанлар ахборотномаси – Вестник юридических наук – Review of Law Sciences"* журнали // 42–46-бетлари

[8] *Евдокимов К.Н.* «Противодействие компьютерной преступности: теория, законодательство, практик» // Москва – 2021, – С. 430.

бўлмоқда. *К.Н.Евдокимов* ушбу ҳодисани қуйидаги омиллар билан детерминация қилади:

•*Ўз-ўзини белгилаш (Самодетерминация):* Кибержиноятчилик юқори технологиялар ва олдин содир этилган жиноятлар асосида янги, мураккаб жиноят турларини ўзидан-ўзи ишлаб чиқариш қобилиятига эга.[9]

•*Зарарли дастурлар эволюцияси:* Вирус ва зарарли кодлар инсон иштирокисиз автоматик равишда кўпайиш ва қарор қабул қилиш хусусиятини касб этмоқда.

•*Жиноятчи шахсининг ўзгариши:* Технотрон жиноятчи — бу юқори интеллектуал салоҳиятга эга, АТ соҳасида махсус билимларга эга бўлган, кўпинча банк ёки телекоммуникация соҳасида фаолият юритувчи мутахассисдир.

Шунингдек, *К.Н.Евдокимов* профилактика чораси сифатида юридик шахсларнинг жиноий жавобгарлигини жорий этиш ва кибермаконда ижтимоий назоратни кучайтиришни таклиф этади.

Г.Ф. Шипулин ўз тадқиқотларида компьютер тармоқларидан фойдаланган ҳолда содир этиладиган жиноятларнинг криминологик хусусиятларига эътибор қаратади[9]. Унинг назариясига кўра, профилактика чоралари жиноят қуролига қараб дифференциация қилиниши керак:

•*жиноят қуролининг ўзига хослиги:* Бу ерда жиноят қуроли нафақат компьютер қурилмаси, балки зарарли дастурий таъминот ёки олдиндан бузиб кирилган ботнет-тармоқлардир.[9]

•*тармоқ трафигини ҳуқуқий тоифалаш: Г.Ф. Шипулин* тармоқ трафигини ахборотнинг алоҳида тури сифатида баҳолашни ва унинг хавфсизлигини таъминлаш бўйича махсус нормаларни ишлаб чиқишни таклиф этади.

Г.Ф. Шипулиннинг концепцияси банк-молия соҳасидаги тармоқ хавфсизлигини таъминлашда рақамли далилларни йиғиш ва идентификация қилиш усулларини такомиллаштиришга хизмат қилади.

Шунингдек, профессор *В.Б. Вехов*[10] фикрича, кибержиноятчиликка қарши курашда ҳуқуқий ва техник чораларнинг синтезини биринчи ўринга қўяди. Унинг фикрича, профилактика фақат жазо чоралари билан эмас, балки рақамли изларни *(digital traces)* автоматик қайд этиш тизимларини такомиллаштириш орқали самарали бўлади. *С.В. Максимов*[11] бўлса, кибержиноятларнинг иқтисодий омилларига эътибор қаратади. Унинг фикрича, кибержиноятларнинг олдини олиш учун давлатнинг ахборот хавфсизлиги тизими ва иқтисодий қонунчилиги ўртасида мустаҳкам ҳуқуқий боғлиқлик бўлиши керак. Шунингдек, *П.Н. Панченко* ва *Ю.Г. Гамаюнова*[12] каби олимлар ўзларининг *“Компьютер жиноятчилигининг криминологик мониторинги”* номли асарида профилактиканинг асоси сифатида “доимий криминологик мониторинг” тизимини таклиф этишади. Уларнинг фикрича, жиноят содир бўлишини кутмасдан, тармоқдаги аномал фаолликларни таҳлил қилиш орқали потенциал хавфларни аниқлаш лозим.

---

[9] *Шипулин Г.Ф.* Криминологическая характеристика и предупреждение преступлений, совершаемых с использованием компьютерных сетей: Дис. ... канд. юрид. наук: 12.00.08. – М., 2003. – 186 с.

[10] *Вехов В.Б.* Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки: Монография. – Волгоград: ВА МВД России, 2002. – С. 112-115.

[11] *Максимов С.В.* Эффективность уголовно-правовых мер борьбы с преступлениями в сфере компьютерной информации. – М.: Юрист, 2011. – С. 42-47.

[12] *Панченко П.Н., Гамаюнова Ю.Г.*. Криминологические проблемы обеспечения безопасности в сфере компьютерной информации / Новгород, 2005. – С. 74-78.

Буюк Британиялик олим *Дэвид Уолл*[13] эса кибержиноятларни тўртта асосий тоифага *(кибер-қароқчилик, кибер-фирибгарлик, кибер-тажовуз ва кибер-порнография)* ажратиб, уларнинг профилактикасини *“жамоатчилик назорати”* ва *“интернет-провайдерлар масъулияти”* орқали амалга оширишни таклиф қилади. У анъанавий полиция назорати кибермаконда чекланганини, шу боис *“тармоқ ички тартибини”* ривожлантириш лозимлигини таъкидлайди. *Б. Лоудер*[14] бўлса ёшларнинг кибержиноятлар қурбонига айланиши ёки ўзлари жиноят содир этишининг олдини олишда *“рақамли таълим” (digital literacy)* моделини илгари суради. У профилактикани мактаб ёшиданоқ кибер-этикани шакллантиришдан бошлаш зарурлигини илмий асослаб беради.

Америкалик профессор *С. Бреннер*[15] кибержиноятчиликнинг трансчегаравий табиати анъанавий ҳудудий профилактика усулларини самарасиз қилиб қўйишини таъкидлайди. Унинг қарашича, профилактиканинг асосий бўғини — давлат ва хусусий сектор *(IT-компаниялар)* ўртасидаги мажбурий ҳамкорликдир. Германиялик машҳур ҳуқуқшунос, *Макс Планк* институти профессори *У. Зибер*[16] кибержиноятчиликка қарши курашда *“ахборот хавфсизлигининг халқаро ҳуқуқий стандарти”*ни ишлаб чиқиш тарафдори. У профилактикани жиноят кодексларини уйғунлаштириш ва халқаро тезкор ахборот алмашинуви орқали амалга оширишни назарий жиҳатдан асослаб берган. Нидерландиялик криминолог *Ян ван Дейк*[17] *“вазиятли жиноятчиликнинг олдини олиш”* (Situational Crime Prevention) назариясини кибермаконга татбиқ этган. Унинг фикрича, жиноятчига жазо билан қўрқитишдан кўра, тизимдаги техник заифликларни ёпиш *(масалан, икки босқичли идентификация)* энг самарали профилактика ҳисобланади.

Дарҳақиқат, бугунги кунда банк-молия ва телекоммуникация тизимлари кибержиноятчиликнинг асосий нишонига айланиши, ушбу соҳада профилактика чораларини нафақат техник, балки чуқур илмий-назарий асосда қайта кўриб чиқишни тақозо этмоқда. Маҳаллий ва хорижий олимларнинг тадқиқотларини ўрганиш асосида, ушбу йўналишдаги профилактиканинг илмий мазмунини қуйидаги *учта фундаментал ёндашув* орқали ёритиш мумкин:

1. Технотрон детерминация ва тизимли мониторинг стратегия ёндашуви.

2. Виктимологик барқарорлик ва “Рақамли маданият” парадигма ёндашуви.

3. Институционал ҳамкорлик ва трансчегаравий назорат ёндашуви.

Юқоридаги олимларнинг қарашларини синтез қилган ҳолда, банк-молия ва телекоммуникация соҳасидаги кибержиноятлар профилактикасини такомиллаштириш бўйича қуйидаги *муаллифлик позитсияларини* илгари сурамиз. Буларга:

Биринчидан, ***интеллектуал профилактика концепцияси.*** Бунга кўра, *П.Н. Панченконинг* “криминологик мониторинг” ғоясини банк соҳасига татбиқ этиб,

[13] *Wall D.S.* Cybercrime: The Transformation of Crime in the Information Age. – Cambridge: Polity Press, 2007. – P. 154-159.

[14] *Loader B.D.* The Governance of Cyberspace: Politics, Technology and Global Restructuring. – London: Routledge, 1997. – P. 88.

[15] *Brenner S.W.* Cybercrime: Criminal Threats from Cyberspace. – Santa Barbara: Praeger, 2010. – P. 210-214.

[16] *Sieber U.* The International Emergence of Cybercrime // Review of European, Comparative & International Environmental Law. – 2011. – Vol. 20. – P. 45-51.

[17] Van Dijk J.J.M. The World of Crime: Breaking the Silence on Problems of Security, Justice and the Victims. – Los Angeles: SAGE, 2008. – P. 128.

жиноят содир бўлишини кутмасдан, тармоқдаги аномал фаолликларни *(масалан, бир вақтнинг ўзида турли нуқталардан картага кириш)* автоматик блоклашнинг ҳуқуқий асосларини яратиш.

Иккинчидан, ***юридик шахсларнинг профилактик жавобгарлиги.*** Бунда, *К.Н. Евдокимов* таклифига таяниб, мижозлар хавфсизлигини таъминлашда техник заифликка йўл қўйган банк ва телеком ташкилотларининг ҳуқуқий масъулиятини кучайтириш. Бу ўз-ўзидан ташкилотларни замонавий ҳимоя тизимларига инвестиция киритишга ундайди.

Учинчидан, ***синтетик ёндашув.*** Бунда эса *В.Б. Вехов* назариясига кўра, профилактика фақат *"жазо"* эмас, балки *"рақамли изларни"* (digital traces) автоматик қайд этиш тизимини такомиллаштиришдир. Бизнингча, телекоммуникация соҳасида *"антифрод"*[18] тизимларини миллий миқёсда ягона марказга бирлаштириш лозим.

Мазкур илмий таҳлил натижалари шуни англатадики, кибержиноятчилик профилактикаси якка тартибдаги техник чоралар билан чекланмайди, балки ахборот хавфсизлиги воситалари, ҳуқуқий жавобгарлик институтлари ҳамда аҳолининг рақамли ҳуқуқий онги ва хавфсизлик маданиятини уйғунлаштирган комплекс (интеграл) тизим сифатида намоён бўлади.

Шу нуқтаи назардан, Янги Ўзбекистон шароитида банк-молия ва телекоммуникация тармоқларида кибержиноятлар профилактикасини таъминловчи ҳуқуқий механизмларни тизимли-ҳуқуқий таҳлил қилиш, амалдаги норматив тартибга солишнинг самарадорлигини баҳолаш, ҳуқуқни қўллаш амалиётида учраётган зиддият ва камчиликларни аниқлаш, шунингдек, профилактик фаолиятни кучайтиришга қаратилган ҳуқуқий бўшлиқларни *(regulatory gaps)* илмий асосда очиб бериш нуқтаи назаридан мақсадга мувофиқдир.

Ҳеч кимга сир эмаски, бугунги кунда Янги Ўзбекистонда кибержиноятчиликка қарши курашишнинг институционал тизими бир нечта ваколатли органларнинг ўзаро ҳамкорлигига асосланган. Буларга, Давлат хавфсизлик хизмати ҳузуридаги Киберхавфсизлик маркази ушбу тизимни мувофиқлаштирувчи асосий орган сифатида ахборот инфратузилмасининг яхлитлигини таъминлайди[19]. Ички ишлар вазирлигининг Кибержиноятларга қарши курашиш бўлими эса бевосита рақамли далилларни тўплаш ва жиноятларни аниқлаш билан шуғулланади[20].

Бироқ, илмий таҳлил шуни кўрсатадики, ушбу қонунларнинг мазмуни кўпроқ умумий профилактикага қаратилган бўлиб, банк-молия соҳасидаги специфик жараёнларни *(масалан, финтех инновациялари ёки крипто-активлар билан боғлиқ операциялар)* тўлиқ қамраб олмаган.

Шунингдек, кредит бюролари учун 2025 йил 23 сентябрда кучга кирган 3679-сонли Низом[21] алоҳида аҳамиятга эга. Ушбу ҳужжат кредит маълумотлари билан ишловчи ташкилотлар учун киберхавфсизликнинг минимал талабларини белгилайди. Шунингдек, ушбу норматив ҳужжатларнинг қабул қилиниши банк соҳасидаги

[18] *"Антифрод"* (инглизча *anti-fraud* — "фирибгарликка қарши") — бу банк-молия ва телекоммуникация тизимларида шубҳали ҳаракатларни аниқлаш ва уларнинг олдини олишга қаратилган *интеллектуал назорат тизими* ҳисобланади.

[19] *Atkhamjonov Abboskhan "Legal and institutional foundations for combating cybercrime in the context of new uzbekistan"* // https://advancedscienti.com.

[20] Ўша манбаа: // https://advancedscienti.com.

[21] Uzbekistan Approves Minimum Cybersecurity Requirements for Credit Bureaus // https://www.uzdaily.uz/

профилактика ишларини *“реактив” (воқеадан кейинги жавоб)* ҳолатидан *“проактив” (олдиндан бартараф этиш)* ҳолатига ўтказди. Аммо, таҳлиллар шуни кўрсатадики, банк ходимларининг ўз ваколатларини суиистеъмол қилиши ёки хавфсизлик аудитининг етарли эмаслиги ҳали ҳам тизимли муаммо бўлиб қолмоқда.

Телекоммуникация соҳаси кибержиноятлар профилактикасида *“транспорт қатлами”* вазифасини бажаради. Жиноятчилар фойдаланадиган *“SMS-стеалерлар”* (SMS-хабарларни ўғирловчи дастурлар) ва сохта алоқа каналлари айнан телекоммуникация инфратузилмасидаги бўшлиқлардан фойдаланади[22].

Юқоридаги ҳуқуқшунос олимларнинг илмий-назарий қарашлари, шунингдек, кибержиноятларнинг олдини олишга қаратилган миллий қонунчиликнинг тизимли ва қиёсий-ҳуқуқий таҳлили натижаларидан келиб чиқиб, диссертация тадқиқотининг долзарблиги ҳамда илмий янгилигини кучайтириш мақсадида олиб борилган таҳлил асосида қуйидаги норматив-ҳуқуқий бўшлиқлар ва тартибга солишдаги камчиликлар кузатиш мумкин.

Биринчидан, ***“Дропперлар” мақоми ва жавобгарлигининг ноаниқлиги билан боғлиқ ҳуқуқий бўшлиқ.*** Бунга кўра, кибержиноят занжирида ўғирланган маблағларни нақдлаштириш учун ўз банк карталарини ёки электрон ҳамёнларини ижарага берувчи шахслар *(“дропперлар”)* муҳим бўғин ҳисобланади. Президентнинг 2025 йил 30 апрелдаги ПҚ-153-сонли қарорида[23] ушбу шахслар учун маъмурий ва жиноий жавобгарлик белгилаш вазифаси қўйилган бўлса-да, амалдаги Жиноят кодексида *“дропперлик”* алоҳида жиноят таркиби сифатида ҳали тўлиқ классификация қилинмаган. Бу эса тергов жараёнида уларни фақатгина *“жиноят шериги”* сифатида айблаш билан чекланиб қолишга ва кўп ҳолларда жазодан қутулиб қолишларига сабаб бўлмоқда.

Иккинчидан, ***сунъий интеллект ва Deepfake технологияларини тартибга солиш билан боғлиқ ҳуқуқий бўшлиқ.*** Ҳеч кимга сир эмаски, 2024 йил 14 октябрда Ўзбекистон Республикаси Президенти *Ш.М. Мирзиёевнинг* тегишли ПҚ-358-сонли қарори[24] билан 2030 йилгача сунъий интеллект стратегияси тасдиқланган бўлса-да, ушбу технологиялар ёрдамида содир этиладиган жиноятларнинг *(масалан, овоз ёки видео тасвирни қалбакилаштириш орқали фирибгарлик)* ҳуқуқий квалификацияси мавжуд эмас. Сунъий интеллект ёрдамида яратилган далилларнинг суддаги мақоми ва уларни аниқлашнинг мажбурий экспертиза тартиби қонунчиликда ўз аксини топмаган.

Учинчидан, ***банк ва молия ташкилотларининг фуқаролик-ҳуқуқий масъулияти билан боғлиқ ҳуқуқий бўшлиқ.*** Амалдаги қонунчиликда кибержиноят натижасида зарар кўрган мижознинг маблағларини қайтариш бўйича банкларнинг жавобгарлиги аниқ белгиланмаган. Агар мижоз ижтимоий инженерия қурбони бўлса, банк одатда масъулиятни ўз зиммасидан соқит қилади. Аммо хорижий тажриба ва ПҚ-153-сонли қарорнинг мазмуни шуни кўрсатадики, агар банк хавфсизлик ва

[22] Fighting Credit Fraud in Uzbekistan: An Uphill Battle Against Social Engineering // https://www.group-ib.com/
[23] Мирзиёев Ш.М. “Ахборот технологиялари ёрдамида содир этиладиган жиноятларга қарши курашиш фаолиятини янада кучайтиришга қаратилган чора-тадбирлар тўғрисида”ги ПҚ-153-сон Қарор // lex.uz/docs/7511145
[24] *Мирзиёев Ш.М.* “Сунъий интеллект технологияларини 2030 йилга қадар ривожлантириш стратегиясини тасдиқлаш тўғрисида”ги ПҚ 358-сон Қарори // lex.uz/docs/7158604

кибермаданиятни ошириш бўйича етарли чора кўрмаган бўлса, зарарнинг бир қисми банк томонидан қопланиши кераклиги бўйича механизмлар жорий этилиши зарур[25].

Тўртинчидан, ***халқаро юрисдикция ва далиллар трансфери билан боғлиқ ҳуқуқий бўшлиқ.*** Дарҳақиқат, Ўзбекистон Будапешт конвенциясида кузатувчи мақомига эга бўлиб, ҳали унга тўлиқ аъзо бўлмаган. Бу ҳолат хорижий давлатларда жойлашган серверлардан рақамли далилларни олиш жараёнини бюрократик тўсиқларга дучор қилмоқда. Кибержиноятларнинг чегара билмаслиги миллий қонунчиликнинг халқаро стандартларга тезроқ интеграциялашувини тақозо этади[26].

Биринчидан, виктимологик профилактикани институционаллаштириш! Бунга кўра, Ўзбекистон Республикасининг ***"Банклар ва банк фаолияти тўғрисида"***ги Қонуннинг *"Банк бошқаруви"* деб номланган 35-моддасининг иккинчи қисмига қуйидаги мазмундаги *еттинчи* хатбошини қўшиш таклиф этилади:

"...мижозларнинг киберсаводхонлигини ошириш, уларда фишинг, ижтимоий муҳандислик ва бошқа турдаги кибертаҳдидлардан ҳимояланиш кўникмаларини шакллантириш бўйича тизимли ва бепул тарғибот-ташвиқот ишларини амалга ошириш ҳамда ушбу жараённинг мониторингини таъминлаш;"

Иккинчидан, ҳуқуқий тартибга солишда технологик нейтраллик принципини имплементация қилиш! Ўзбекистон Республикасининг "***Киберхавфсизлик тўғрисида"***ги Қонуни 16-моддасининг *иккинчи* қисми *(Киберхавфсизлик субъектларининг мажбуриятлари)* қуйидаги мазмундаги хатбоши билан тўлдириш таклиф этилади:

"...фойдаланиладиган технологиялар ва рақамли идентификация воситаларининг туридан қатъи назар, уларнинг функционал вазифаларига мувофиқ киберхавфсизлик талаблари ва профилактик чораларнинг узлуксиз ижросини таъминлаш;"

Учинчидан, кибер-рискларни бошқаришнинг иқтисодий-ҳуқуқий механизмини такомиллаштириш! Ўзбекистон Республикасининг "Тўловлар ва тўлов тизимлари тўғрисида"ги Қонуннинг 54-моддаси қуйидаги мазмундаги *иккинчи қисм* билан тўлдириш таклиф этилади:

"Тўлов тизими операторлари ва тўлов ташкилотлари кибертаҳдидлар натижасида мижозларга етказилиши мумкин бўлган зарарларни қоплаш мақсадида ўз фуқаролик жавобгарлигини мажбурий суғурта қилиши шарт. Суғурта қилиш тартиби ва суғурта қопламасининг минимал миқдори Ўзбекистон Республикаси Марказий банки томонидан белгиланади."

Ушбу таклифлар диссертациянинг илмий долзарблигини ошириб, Янги Ўзбекистоннинг рақамли иқтисодиёти учун мустаҳкам ҳуқуқий қалқон яратишга хизмат қилади.

[25] https://cis-legislation.com/document.fwx?rgn=166955
[26] *Enver Buçaj & Arsim Thaqi* "Global Regulation of Cybercrime through International Law and Cyberconventions" // /Downloads/pdf.pdf