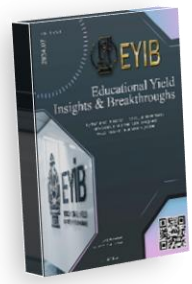
EYIB
EDUCATIONAL YIELD INSIGHTS & BREAKTHROUGHS
TA'LIMGA OID TUSHUNCHALAR VA YUTUQLAR
ISSN:3060-4648
Vol.4 №3
https://eyib.uz



КИБЕРМАКОНДА СОДИР ЭТИЛАДИГАН МУЛКИЙ ЖИНОЯТЛАРНИНГ КРИМИНОЛОГИК ТАВСИФИ: КИБЕРЎҒРИЛИК ВА КИБЕРФИРИБГАРЛИК МИСОЛИДА

Марзажонов Шохрухбек Собиржонович

Ўзбекистон Республикаси Криминология тадқиқоти институти мустақил зланувчиси

Annotatsiya

Мақолада кибермаконда содир этиладиган мулкий жиноятлар, хусусан киберўғрилик ва киберфирибгарликнинг криминологик хусусиятлари тизимли таҳлил қилинади. Кибержиноятчиликка нисбатан дуалистик ёндашув доирасида ахборот технологиялари “восита” сифатида қўлланилганда анъанавий мулкий жиноятлар конструкцияси рақамли муҳитга мослашаётгани асосланади. Тадқиқотда жиноят предметининг рақамли активлар ва электрон пул маблағлари томон трансформацияланиши, жиноят содир этишнинг масофавийлиги ва анонимлиги, фош этиш мураккаблиги ҳамда латентлик даражасининг юқорилиги каби омиллар ёритилади. Шунингдек, киберўғриликда ноқонуний кириш (hacking) элементлари, киберфирибгарликда эса ижтимоий муҳандислик (social engineering) усулларининг устуворлиги криминологик мезонлар асосида фарқланади. Мақола хулосалари профилактика механизмларини такомиллаштириш ва ҳуқуқий таърифларни замонавий рақамли муносабатларга мослаштириш заруратини кўрсатади.

Kalit so‘zlar: кибермакон; мулкий жиноятлар; киберўғрилик; киберфирибгарлик; рақамли активлар; электрон пул маблағлари; ноқонуний кириш (hacking); ижтимоий муҳандислик; виктимологик омиллар; латентлик; профилактика

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ИМУЩЕСТВЕННЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В КИБЕРПРОСТРАНСТВЕ: НА ПРИМЕРЕ КИБЕРКРАЖИ И КИБЕРМОШЕННИЧЕСТВА

Аннотация: В статье проводится системный анализ имущественных преступлений, совершаемых в киберпространстве, прежде всего киберкраж и кибермошенничества, с позиций современной криминологии. В рамках дуалистического подхода показано, что при использовании информационных технологий как «средства» традиционные конструкции имущественных преступлений адаптируются к цифровой среде. Обосновывается трансформация предмета посягательства в сторону цифровых активов и электронных денежных

средств, а также раскрываются особенности дистанционности и анонимности совершения деяний, сложности их раскрытия и высокой латентности. Отмечается, что для киберкраж характерны элементы несанкционированного доступа (hacking), тогда как для кибермошенничества — преобладание методов социальной инженерии (social engineering). Сделанные выводы подчеркивают необходимость совершенствования профилактических механизмов и адаптации правовых дефиниций к современным цифровым отношениям.

Ключевые слова: киберпространство; имущественные преступления; киберкража; кибермошенничество; цифровые активы; электронные денежные средства; несанкционированный доступ (hacking); социальная инженерия; виктимологические факторы; латентность; профилактика

CRIMINOLOGICAL CHARACTERISTICS OF PROPERTY CRIMES COMMITTED IN CYBERSPACE: THE CASE OF CYBER THEFT AND CYBER FRAUD

Abstract: This article provides a systematic criminological analysis of property crimes committed in cyberspace, with particular emphasis on cyber theft and cyber fraud. Using a dualistic approach to cybercrime, it argues that when information technologies function as a “means” of offending, traditional property-crime constructs are increasingly adapted to the digital environment. The study highlights the shift of the crime object toward digital assets and electronic funds, and discusses key features such as remoteness and anonymity, investigative complexity, and a high level of latency (the “dark figure” of cybercrime). It further differentiates cyber theft—often linked to unauthorized access (hacking)—from cyber fraud, where social engineering techniques tend to dominate. The conclusions support the need to strengthen preventive mechanisms and to align legal definitions with rapidly evolving digital relations.

Keywords: cyberspace; property crimes; cyber theft; cyber fraud; digital assets; electronic funds; unauthorized access (hacking); social engineering; victimological factors; latency (dark figure); prevention

Замонавий криминология фанида кибержиноятчилик тушунчаси дуалистик ёндашув асосида таҳлил қилинади. *Биринчидан,* бу компьютер маълумотлари ва тизимларининг хавфсизлигига қарши қаратилган жиноятлар бўлса, *иккинчидан,* ахборот технологиялари ва тармоқларидан восита сифатида фойдаланиб содир этиладиган *“анъанавий”* жиноятлардир.

Мулкий жиноятлар контекстида *кибер-ўғрилик* ва *кибер-фирибгарлик* марказий ўринни эгаллайди. Ўзбекистон ва Россия Федерацияси қонунчилиги таҳлили шуни кўрсатадики, бу қилмишлар ахборот-коммуникация технологиялари ёрдамида ўзганинг мулкини ёки мулкий ҳуқуқини талон-торож қилишни ифодалайди. Технотрон жамиятда мулк объекти жисмоний шаклдан рақамли активлар ва электрон пул маблағлари шаклига трансформация бўлди. Бу эса жиноятнинг предмети сифатида нафақат моддий бойликларни, балки

иқтисодий қийматга эга бўлган компьютер маълумотларини ҳам эътироф этишни талаб қилмоқда[1].

Ҳеч кимга сир эмаски, сўнгги йилларда янги Ўзбекистонда кибержиноятчиликнинг ўсиш суръатлари геометрик прогрессия характерига эга бўлмоқда. Хусусан, Ички ишлар вазирлигининг тизимли таҳлилларига кўра, сўнгги беш йиллик давр ичида мазкур турдаги жиноятлар сони 68 бараварга ортган.

Хусусан, 2024 йилда қайд этилган ҳуқуқбузарликлар динамикаси 2023 йилга нисбатан 910 фоизлик (9,1 баравар) ўсишни кўрсатган бўлиб, бу рақамли макондаги криминоген вазиятнинг кескинлашганидан далолат беради. Шунингдек, кибержиноятчилик натижасида фуқаролар ва иқтисодий субъектларга етказилаётган моддий зарар кўлами стратегик хавф даражасига етди. Жумладан, 2021–2024 йиллар мобайнида фуқароларнинг кибержиноятчилар томонидан ўзлаштирилган жами маблағлари миқдори *1,9 триллион* сўмдан ортиқни ташкил этди[2]. Ҳудудий таҳлил қилинганда биргина 2025 йилнинг ҳисобот даврида кибержиноятлар сони *16 мингтадан* ошди. Ушбу ҳуқуқбузарликлар натижасида етказилган моддий зарар миқдори қарийб *2 триллион сўмга* яқинлашди[3]. Мазкур кўрсаткичлардан билиш мумкинки, бугунги кунда рақамли жиноятларнинг латентлик (яширинлик) даражаси юқорилигича қолмоқда. 2025 йилги тадқиқотлар шуни кўрсатадики, Тошкент шаҳрида қайд этилган кибержиноятларнинг *фош этилиш кўрсаткичи 8 фоиздан паст* натижани қайд этган[4].

Кузатувлар шуни кўрсатадики, кибержиноятларнинг салмоқли қисми мулкий манфаатга қаратилган ўғрилик ва фирибгарликка хос усуллар *(ахборот ресурсларига ноқонуний кириш, тўлов реквизитларини қўлга киритиш, шахсий маълумотлардан фойдаланиб алдов йўли билан пул маблағларини ўзлаштириш ва бошқалар)* орқали амалга оширилмоқда. Мазкур ҳолат кибермаконда мулкий жиноятларнинг *трансформацияланиши* — яъни анъанавий ўғрилик ва фирибгарлик конструкциясининг рақамли муҳитга мослашиши, жиноят содир этишнинг *“масофавийлиги”,* анонимлиги ва тезкорлиги билан тавсифланиши — ҳақидаги илмий-назарий хулосаларни долзарб қилади. Шу боис, кибермаконда ўғрилик ва фирибгарлик билан боғлиқ мулкий жиноятларнинг криминологик тавсифи *(субъект таркиби, мотивация, виктимологик омиллар, содир этиш усуллари, латентлик даражаси ҳамда профилактика механизмлари)* маҳаллий ва хорижий олимларнинг доктринал қарашлари асосида қай даражада ўрганилгани, мавжуд ёндашувлар ўртасида қандай умумийлик ва фарқлар мавжуд экани, шунингдек миллий амалиёт учун қайси назарий моделлар энг мақбул экани масаласи илмий тадқиқотнинг мустақил объекти сифатида қўйилиши мақсадга мувофиқдир.

---

[1] *Евдокимов К.Н.* «Противодействие компьютерной преступности: теория, законодательство, практика» г. Москва, г. 2021., – С. 301.

[2] Ущерб от киберпреступлений в 2021−2024 годах в Узбекистане превысил 1,9 трлн сумов // https://www.gazeta.uz/

[3] https://x.com/Sherzod_Asadov

[4] president.uz

Хусусан, Ўзбекистон Республикасида кибермаконда содир этилаётган жиноятларнинг, хусусан мулкий хусусиятга эга бўлган киберўғрилик ва киберфирибгарликларнинг криминологик тавсифини тадқиқ этиш юридик фанлар доктори, профессор *С.С. Гулямов* томонидан тизимли равишда ўрганилган. Олимнинг таъкидлашича, кибермакон тушунчаси ва ундаги ҳуқуқбузарликларнинг динамикаси анъанавий жиноятлардан ўзининг трансчегаравийлиги ва виртуаллиги билан фарқ қилади[5]. Шу билан бирга, кибержиноятларнинг детерминацияси ва жиноятчи шахсининг деформацияси масалалари тадқиқотчи *А.О. Халмуратов* ишларида ўз ифодасини топган. У кибержиноятларнинг генезисини таҳлил қилар экан, ахборот технологиялари воситасида содир этиладиган жиноятларнинг криминологик тавсифида виктимологик омиллар ва технологик бўшлиқларнинг ўрни юқори эканлигини қайд этади[6]. Бундан ташқари, кибермакондаги мулкий жиноятларни содир этиш усуллари ва уларнинг олдини олишнинг ташкилий-ҳуқуқий механизмларини такомиллаштириш бўйича *И. Абдихакимов* томонидан ҳам илмий изланишлар олиб борилган. Муаллиф рақамли муҳитда шахсий маълумотларнинг ҳимояланиш даражаси киберфирибгарликнинг олдини олишда асосий тўсиқ бўлишини асослаб беради[7].

Шунингдек, кибержиноятчиликнинг жиноий-ҳуқуқий ва криминологик жиҳатларини тадқиқ этиш масалалари замонавий юридик фаннинг энг долзарб йўналишларидан бири ҳисобланади. Мазкур муаммонинг назарий-услубий асосларини шакллантиришда бир қатор етакчи ҳорижий олимларнинг тадқиқотлари муҳим пойдевор бўлиб хизмат қилган. Хусусан, *Ю.М. Батурин* ва *А.М. Жодзишский* ўзларининг илк изланишларида компьютер маълумотлари соҳасидаги жиноятларнинг ижтимоий хавфлилик даражасини илмий асослаб берган бўлсалар[8], *И.Р. Бегишев*[9], *М.А. Ефремова*[10] ва *У.В. Зинина*[11] каби олимлар ахборот хавфсизлигига қарши қаратилган жиноятларнинг объектив ва субъектив белгиларини замонавий жиноят қонунчилиги нуқтаи назаридан тадқиқ этганлар. *Т.М. Лопатина* томонидан эса компьютер жиноятчилигига қарши курашнинг жиноий-ҳуқуқий ва криминологик асослари яхлит тизим сифатида ўрганилган[12]. Шунингдек, кибержиноятчиликнинг криминологик тавсифи ва унинг генезисига оид ёндашувлар муҳим назарий аҳамият касб этади. Бу борада *В.Б. Веховнинг*

---

[5] *Гулямов С.С.* Киберҳуқуқ (Cyber Law). Дарслик. – Тошкент: ТДЮУ нашриёти, 2023. – Б. 112-115.
[6] *Khalmuratov A.* Genesis of Cybercrime and its Concept Peculiarities // International Journal of Law and Criminology. – 2024. – Vol. 4. – No. 01. – P. 34-39.
[7] *Абдихакимов И.* Рақамли маконда шахсий маълумотлар дахлсизлигини таъминлашнинг ҳуқуқий муаммолари // Юридик фанлар ахборотномаси. – 2023. – №4.
– Б. 45-50.
[8] *Батурин Ю.М., Жодзишский А.М.* Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 1991. – 160 с.
[9] *Бегишев И.Р.* Уголовная ответственность за изготовление, хранение, перевозку или сбыт специальных технических средств, предназначенных для негласного получения информации. – Казань, 2010. – С. 45–52.
[10] *Ефремова М.А.* Уголовно-правовая охрана информационной безопасности. Монография. – М.: Юрлитинформ, 2017. – С. 88–104.
[11] *Зинина У.В.* Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. Дисс. … канд. юрид. наук. – М., 2007. – С. 112–120.
[12] *Лопатина Т.М.* Криминологические и уголовно-правовые основы противодействия компьютерной преступности. Дисс. … докт. юрид. наук. – М., 2006. – С. 145–160.

компьютер воситаларидан фойдаланиб содир этиладиган жиноятларни тергов қилиш методикасига оид ишлари пойдевор бўлиб хизмат қилган[13]. Глобал тармоқлардаги жиноятчиликнинг олдини олишнинг ташкилий-ҳуқуқий жиҳатлари *А.Л. Осипенко* тадқиқотларида ўз ифодасини топган бўлса, *Р.И. Дремлюга*[14] ва *Т.Л. Тропина*[15] Интернет-жиноятчиликнинг криминологик детерминантлари ва ривожланиш тенденцияларини очиб берганлар[16]. Шунингдек, *И.Г. Чекунов* компьютер маълумотлари соҳасидаги жиноятларга қарши криминологик кураш чораларини такомиллаштириш концепциясини илгари сурган[17].

Бундан ташқари, қиёсий-ҳуқуқий ва халқаро ҳамкорлик йўналишида *А.Г. Волеводзнинг* ишлари алоҳида ажралиб туради. У кибержиноятларга қарши курашда халқаро ҳуқуқий ёрдам кўрсатиш ва трансмиллий кибержиноятчиликка қарши курашнинг ҳуқуқий механизмларини ишлаб чиққан[18]. Бу йўналишдаги изланишлар *В.В. Хилюта*[19] ва *В.А. Голубев*[20] каби олимларнинг ахборот хавфсизлигини таъминлаш борасидаги хорижий тажрибани таҳлил қилишга қаратилган тадқиқотлари билан тўлдирилади. *К.Н. Евдокимов* эса замонавий компьютер жиноятчилигига қарши курашишга doir (унинг технотрон жиноятчиликка айланиб бораётгани шароитида) назарий, қонун ижодкорлиги ва амалий мазмундаги қоидалар, таклифлар ва тавсияларнинг комплекс тизими ишлаб чиқилган [21].

Юқорида тилга олинган олимларнинг илмий изланишларини умумлаштирган ҳолда таъкидлаш жоизки, замонавий юридик фанда кибержиноятчиликка нисбатан *комплекс* ва *тизимли ёндашув* шаклланган. Тадқиқотларнинг эволюцияси шуни кўрсатмоқдаки, кибермакондаги ҳуқуқбузарликлар фақат техник хусусиятга эга бўлмай, балки чуқур ижтимоий-психологик ва криминологик илдизларга эгадир. Шу ўринда, кибермаконда содир этиладиган мулкий жиноятлар, хусусан, *киберўғрилик* ва *киберфирибгарликнинг* криминологик табиатини тушуниш учун аввало ушбу соҳадаги мавжуд илмий мактаблар ва концептуал қарашларни тизимлаштириш лозим.

---

[13] *Вехов В.Б.* Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники. – М.: ЦИиНМО КП МВД России, 2000. – С. 12–18.
[14] *Осипенко А.Л.* Борьба с преступностью в глобальных компьютерных сетях: Международный опыт. – М.: Юрлитинформ, 2004. – С. 210–225.
[15] *Дремлюга Р.И.* Интернет-преступность: монография. – Владивосток: Изд-во Дальневост. ун-та, 2008. – С. 134–150.
[16] *Тропина Т.Л.* Киберпреступность: понятие, состояние, тенденции развития. Дисс. … канд. юрид. наук. – Владивосток, 2005. – С. 67–82.
[17] *Чекунов И.Г.* Криминологическое противодействие преступлениям в сфере компьютерной информации. Дисс. … канд. юрид. наук. – М., 2010. – С. 95–110.
[18] *Волеводз А.Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2002. – С. 340–355.
[19] *Хилюта В.В.* Преступления против информационной безопасности: проблемы квалификации. – Гродно: ГрГУ, 2005. – С. 44–58.
[20] *Голубев В.А.* Расследование компьютерных преступлений. – Запорожье: ПГУ, 2002. – С. 118–130.
[21] *Евдокимов К. Н.* «Противодействие компьютерной преступности: теория, законодательство, практика» М.: 2021. - С. 15.

Жумладан, *С.С. Гулямов*[22] томонидан илгари сурилган кибермаконнинг *“виртуаллиги”* ва *А.О. Халмуратов*[23] қайд этган *“технологик бўшлиқлар”* мулкий жиноятларнинг янги генезисини белгилаб беради. Хусусан, киберўғрилик *(cyber-theft)* ва киберфирибгарлик *(cyber-fraud)* содир этилганда, жиноятчи ва жабрланувчи ўртасидаги жисмоний масофанинг мавжуд эмаслиги *(“anonimity impact”),* жиноятни фош этишнинг қийинлиги ва зарар кўлами бир лаҳзада глобал даражага етиши мумкин.

Криминологик тадқиқотлар шуни кўрсатадики, кибермакондаги мулкий жиноятларнинг тавсифида қуйидаги учта асосий детерминант мавжуддир. Буларга:

❖ ***технологик детерминантлик.*** Бунда *И. Абдихакимов*[24] ва *К.Н. Евдокимов*[25] таъкидлаганидек, тизимдаги заифликлар ва шахсий маълумотларнинг ҳимояланмаганлиги жиноятчи учун *“рақамли калит”* вазифасини ўтайди. Бугунги кунда ўғрилик компьютер тизимига рухсатсиз кириш (hacking) орқали амалга оширилса, фирибгарлик кўпроқ *“ижтимоий муҳандислик”* (social engineering) усуллари билан боғланмоқда.

❖ ***виктимологик детерминантлик.*** Бунда *Р.И. Дремлюга*[26] ва *Т.Л. Тропина*[27] асарларида кўрсатилганидек, фойдаланувчиларнинг рақамли саводхонлиги пастлиги ва "виртуал ишончувчанлиги" киберфирибгарликнинг асосий драйвери ҳисобланади. Жабрланувчининг жиноятга ўз ҳаракатлари билан *(масалан, фишинг ҳаволасига кириш ёки кодни тақдим этиш)* замин яратиши кибермакондаги виктимологик деформациянинг энг юқори нуқтасидир.

❖ ***трансчегаравийлик*** *(International scope).* Бунда *А.Г. Волеводз*[28] концепциясига таянган ҳолда айтиш мумкинки, мулкий кибержиноятлар кўпинча бир давлат ҳудудида режалаштирилиб, иккинчи давлатдаги сервер орқали амалга оширилади ва учинчи давлат фуқаросининг маблағларини ўзлаштиришга қаратилади.

Юқоридаги таҳлиллардан келиб чиқиб таъкидлаш жоизки, кибермаконда содир этилаётган мулкий жиноятларнинг криминологик тавсифида *киберўғрилик* ва *киберфирибгарлик* ўртасидаги фарқли жиҳатларни аниқлаш муҳим илмий аҳамиятга эга. Жумладан, киберўғриликда жиноят содир этиш усули асосан компьютер тизимига рухсатсиз кириш (hacking) орқали мулкни яширин талон-торож қилишни ифодаласа, киберфирибгарлик кўпроқ *“ижтимоий муҳандислик”* (social engineering) усуллари билан боғланмоқда.

---

[22] *Гулямов С.С.* Киберҳуқуқ (Cyber Law). Дарслик. – Тошкент: ТДЮУ нашриёти, 2023. – 464 б.

[23] *Khalmuratov A.* Genesis of Cybercrime and its Concept Peculiarities // International Journal of Law and Criminology. – 2024. – Vol. 4. – No. 01. – P. 34-39.

[24] *Абдихакимов И.* Рақамли маконда шахсий маълумотлар дахлсизлигини таъминлашнинг ҳуқуқий муаммолари // Юридик фанлар ахборотномаси. – 2023. – №4.
– Б. 45-50.

[25] *Евдокимов К.Н.* Противодействие компьютерной преступности: теория, законодательство, практика: Монография. – Иркутск: ИЮИ (ф) УП РФ, 2021. – 180 с.

[26] *Дремлюга Р.И.* Интернет-преступность: монография. – Владивосток: Изд-во Дальневост. ун-та, 2008. – 240 с.

[27] *Тропина Т.Л.* Киберпреступность: понятие, состояние, тенденции развития: Дисс. … канд. юрид. наук. – Владивосток, 2005. – 234 с.

[28] *Волеводз А.Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2002. – 496 с.

Мазкур жиноятларнинг динамикаси ва уларнинг детерминацияси масалалари тадқиқотчи *А.О. Халмуратов* ишларида ўз ифодасини топган бўлиб, муаллиф кибержиноятларнинг генезисида технологик бўшлиқлар ва виктимологик омилларнинг ўрни юқори эканлигини алоҳида қайд этади. Хусусан, жабрланувчининг жиноят содир этилишига ўз ҳаракатлари билан *(масалан, фишинг ҳаволасига кириш ёки махфий кодни тақдим этиш)* замин яратиши кибермакондаги виктимологик деформациянинг энг юқори нуқтаси сифатида баҳоланади. *Р.И. Дремлюга* ва *Т.Л. Тропина* асарларида таъкидланганидек, фойдаланувчиларнинг рақамли саводхонлиги пастлиги ва *“виртуал ишончувчанлиги”* киберфирибгарликнинг асосий драйвери (турткиси) бўлиб хизмат қилмоқда.

Кибержиноятларнинг латентлик даражасининг юқорилиги ҳам долзарб муаммо бўлиб қолмоқда. Жумладан, 2025 йилги тадқиқотлар Тошкент шаҳрида қайд этилган кибержиноятларнинг фош этилиш кўрсаткичи 8 фоиздан паст натижани ташкил этганини кўрсатади. Бу ҳолат *И. Абдихакимов* томонидан асослаб берилганидек, рақамли муҳитда шахсий маълумотларнинг ҳимояланиш даражаси пастлиги ва жиноят содир этишнинг *“масофавийлиги”* ҳамда анонимлиги билан изоҳланади.

Шу билан бирга, *А.Г. Волеводз* концепциясига кўра, мулкий кибержиноятларнинг трансчегаравий характери уларга қарши курашишда халқаро ҳамкорликни тақозо этади. Бунда жиноят бир давлат ҳудудида режалаштирилиб, бошқа давлатдаги сервер орқали амалга оширилиши ва учинчи давлат фуқаросининг маблағларини ўзлаштиришга қаратилиши мумкин. *К.Н. Евдокимов* таъкидлаганидек, замонавий компьютер жиноятчилиги технотрон жиноятчиликка айланиб бораётган шароитда, унга қарши курашишнинг назарий, қонун ижодкорлиги ва амалий мазмундаги комплекс тизимини ишлаб чиқиш лозимдир.

Юқорида қайд этилган олимларнинг илмий-назарий ёндашувларини таҳлил қилиш билан бир қаторда, мазкур параграфнинг илмий салоҳияти ва амалий аҳамиятини ошириш мақсадида ривожланган давлатлар тажрибасини қиёсий-илмий асосда ўрганиш мақсадга мувофиқ. Хорижий амалиёт таҳлили шуни кўрсатадики, кибержиноятчиликка қарши кураш самарадорлиги фақат жиноий-ҳуқуқий жазо чоралари билан эмас, балки тизимли профилактика, технологик чеклов ва ҳимоя механизмлари, шунингдек халқаро ҳамкорликни институционал жиҳатдан мустаҳкамлаш билан белгиланади. Шу нуқтаи назардан *Сингапур, Буюк Британия, Эстония* ҳамда *АҚШнинг* илғор тажрибалари алоҳида илмий қизиқиш уйғотади.

Сингапур давлати киберхавфсизлик бўйича дунёда етакчи ўринлардан бирини эгаллайди. Мазкур мамлакатнинг 1993 йилда қабул қилинган ва мунтазам такомиллаштирилаётган *“Компьютердан ноқонуний фойдаланиш тўғрисида”*ги Қонуни *(Computer Misuse Act - CMA)* кибержиноятларга қарши курашнинг асосий ҳуқуқий базаси ҳисобланади[29].

[29] Computer Misuse Act 1993 - Singapore Statutes Online, accessed February 1, 2026, https://sso.agc.gov.sg/Act/CMA1993

Сингапур тажрибасининг энг муҳим жиҳати шундаки, мазкур давлатда *“пул ташувчилар”* (money mules) деб аталувчи, жиноий маблағларни нақдлаштиришда иштирок этувчи шахсларга нисбатан жавобгарликнинг қатъий белгиланганидадир. 2023 йилда Сингапур парламенти CMA ва Жиноят кодексига янги ўзгартиришлар киритди[30]. Ушбу ўзгартиришларга кўра, агар шахс ўз банк картаси ёки рақамли идентификация маълумотларини (Singpass) бошқаларга берса ва бу маълумотлар жиноят содир этишда ишлатилса, шахснинг ўзи ҳам *“эҳтиётсизлик”* ёки *“бепарволик”* учун жавобгарликка тортилади[31].

Шунингдек, ***Сингапурда*** CMAнинг 4-моддасига биноан, компьютер тизимига мулкка қарши жиноят, фирибгарлик ёки ноҳалоллик содир этиш мақсадида киришнинг ўзи алоҳида жиноят ҳисобланиб, 10 йилгача қамоқ жазоси билан жазоланади[32]. Бу жиноятнинг “тайёргарлик” босқичидаёқ қатъий жазо белгиланишини ифодалайди. Шунингдек, Сингапур пул-кредит бошқармаси (MAS) банклар билан ҳамкорликда анти-мальваре тизимларини ишлаб чиққан бўлиб, улар агар фойдаланувчи телефонида шубҳали (sideloaded) иловалар аниқланса, банк иловасига киришни чеклаб қўяди[33].

Буюк Британия давлатида эса кибержиноятчиликка қарши курашда 1990 йилги *“Компьютердан ноқонуний фойдаланиш тўғрисида”*ги Қонун ва 2006 йилги *“Фирибгарлик тўғрисида”*ги Қонун асосий роль ўйнайди[34]. Бироқ, сўнгги йиллардаги энг муҳим янгилик – 2025 йил 2 декабрда кучга кирган *“Мулк (Рақамли активлар ва бошқалар) тўғрисида”*ги Қонун *(Property (Digital Assets etc) Act 2025)* бўлди[35].

Ушбу қонун крипто-токенлар, NFT ва бошқа рақамли активларни мулкнинг *“учинчи тоифаси” (third category of personal property)* сифатида расман тан олди[36]. Илгари инглиз ҳуқуқида мулк фақат икки турга бўлинарди: *эгаликдаги ашёлар (кўчмас мулк, автомобиль)* ва *даъво ҳуқуқлари (акциялар, қарзлар)*. Рақамли активлар бу икки турга ҳам тўлиқ тушмасди, бу эса улар ўғирланганда ҳуқуқий ҳимояни қийинлаштирарди[37]. Янги қонуннинг аҳамияти қуйидагича:

---

[30] CDSA and CMA Bill Amendments - Singapore Police Force, accessed February 1, 2026, https://www.police.gov.sg/Knowledge-Hub/Legislation/CDSA-and-CMA-Bill-Amendments

[31] Commencement of Amendments to the Computer Misuse Act and Corruption, Drug Trafficking, and Other Serious Offences (Confiscation of Benefits) Act - Ministry of Home Affairs, accessed February 1, 2026, https://www.mha.gov.sg/mediaroom/media-detail/commencement-of-amendments-to-the-computer-misuse-act-and-corruption-drug-trafficking-and-other-serious-offences-confiscation-of-benefits-act/

[32] Computer Misuse Act 1993 - Singapore Statutes Online, accessed February 1, 2026, https://sso.agc.gov.sg/Act/CMA1993?ViewType=Pdf&_=20260107214642

[33] Estonia SG Report, accessed February 1, 2026, https://www.vm.ee/sites/default/-files/documents/2025-03/Singapore%20Strategy_Cybersecurity.pdf

[34] Computer Misuse Act | The Crown Prosecution Service, accessed February 1, 2026, https://www.cps.gov.uk/prosecution-guidance/computer-misuse-act

[35] The Property *(Digital Assets etc)* Act 2025 comes into force - Hogan Lovells, accessed February 1, 2026, https://www.hoganlovells.com/en/publications/the-property-digital-assets-etc-act-2025-comes-into-force

[36] Property (Digital Assets Etc.) Bill: factsheet - GOV.UK, accessed February 1, 2026, https://www.gov.uk/government/publications/property-digital-assets-etc-bill/property-digital-assets-etc-bill-factsheet

[37] Redefining ownership: How the Property (Digital Assets etc) Bill will protect digital assets - Legal Advice Centre - Queen Mary University of London, accessed February 1, 2026, https://www.qmul.ac.uk/lac/our-legal-blog/blogs/redefining-ownership-how-the-property-digital-assets-etc-bill-will-protect-digital-assets.html

1. Рақамли активларни ўғирлаганлик учун анъанавий мулкий жиноятлар бўйича жавобгарликка тортиш асослари мустаҳкамланди[38].

2. Жабрланувчилар ўзларининг ўғирланган крипто-активларини мулк сифатида қайтариб олиш (proprietary restitution) ҳуқуқига эга бўлдилар[39].

3. Судлар ўғирланган маблағларни музлатиш бўйича "мулкка оид инъюнкциялар" (proprietary injunctions) чиқариш имкониятига эга бўлдилар[40].

Буюк Британия тажрибаси шуни кўрсатадики, рақамли муҳитда мулк тушунчасини кенгайтирмасдан туриб, киберўғриликка самарали қарши курашиб бўлмайди.

Эстония давлати ҳам дунёдаги энг рақамлашган давлатлардан бири сифатида киберхавфсизликни миллий устувор йўналиш деб белгилаган. *Эстония* Жиноят кодексининг 213-моддаси (Computer-related fraud) компьютер маълумотларига ноқонуний аралашиш орқали мулкий зарар етказишни алоҳида жиноий таркиб сифатида тавсифлайди[41].

Эстониянинг 2024–2030 йилларга мўлжалланган Киберхавфсизлик стратегиясида *"Кибер-қалқон"* (Cyber-shield) яратиш асосий мақсад қилиб қўйилган[42]. Бу стратегия аҳолининг рақамли саводхонлигини ошириш, давлат ва хусусий сектор ўртасида тезкор ахборот алмашинувини таъминлашни назарда тутади. Эстония полициясининг маълумотига кўра, 2023 йилда фишинг ва инвестиция фирибгарлиги орқали фуқаролардан 8,3 миллион евродан ортиқ маблағ ўғирланган[43]. Бунга жавобан давлат "Кибер-онгли Эстония" (Cyber-conscious Estonia) лойиҳасини амалга ошириб, ҳар бир фуқарони кибертаҳдидларни аниқлай оладиган даражада тайёрламоқда[44].

АҚШда *"Компьютер фирибгарлиги ва суиистеъмоли тўғрисида"*ги Қонун *(Computer Fraud and Abuse Act - CFAA, 18 U.S.C. § 1030)* кибержиноятчиликка қарши курашнинг асосий воситасидир[45]. CFAA еттита асосий жиноят турини белгилайди, улар орасида компьютер тизимига фирибгарлик мақсадида кириш (1030(a)(4)) алоҳида ўрин тутади[46].

АҚШ тажрибасида киберўғрилик ва киберфирибгарлик учун жазолар жуда оғир бўлиб, улар зарар миқдори ва жиноятнинг мақсадига қараб белгиланади.

---

[38] The Property (Digital Assets etc) Act 2025: Digital Asset Ownership - Mishcon de Reya, accessed February 1, 2026, https://www.mishcon.com/news/the-property-digital-assets-etc-act-2025-digital-asset-ownership

[39] UK Law Recognizes Bitcoin & NFTs as Personal Property - Cryptobooks, accessed February 1, 2026, https://cryptobooks.tax/en/blog/uk-property-act-2025

[40] The Property (Digital Assets etc) Act 2025: Digital Asset Ownership - Mishcon de Reya, accessed February 1, 2026, https://www.mishcon.com/news/the-property-digital-assets-etc-act-2025-digital-asset-ownership

[41] Fraud | Justice Statistics, accessed February 1, 2026, https://statistika.justdigi.ee/en/crime-statistics/varavastased-kuriteod/kelmused

[42] Ensuring the state's cyber security | Ministry of Justice and Digital Affairs, accessed February 1, 2026, https://www.justdigi.ee/en/digital-communications-and-cyber/ensuring-states-cyber-security

[43] Cybersecurity strategy 2024–2030 Cyber-conscious Estonia - ENISA, accessed February 1, 2026, https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_-2024_en.pdf

[44] Ўша манбаа: // https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/-reports/EE_NCSS_2024_en.pdf

[45] Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws - Congress.gov, accessed February 1, 2026, https://www.congress.gov/-crs_external_products/RL/PDF/97-1025/97-1025.17.pdf

[46] Computer Hacking - 18 U.S.C. § 1030 - Cron Israels and Stark, accessed February 1, 2026, https://www.cronisraelsandstark.com/federal-computer-hacking

Агар ўғирланган маълумотлар қиймати $5,000 дан ошса, жиноят оғир жиноят (felony) деб баҳоланади ва 10 йилгача қамоқ жазоси берилиши мумкин[47].

Мазкур давлатларнинг илғор ва ижобий тажрибаларини қиёсий-ҳуқуқий таҳлил қилиш натижалари шуни кўрсатадики, ***Янги Ўзбекистон*** шароитида амалдаги ***Жиноят кодекси***да кибержиноятчиликка доир муайян нормалар мавжуд бўлса-да, уларнинг таркибий қамрови ва қўлланиш имкониятлари ***рақамли муҳитдаги замонавий таҳдидларнинг барча кўринишларини тўлиқ ифодалашга етарли эмас.*** Хусусан, кибермаконда содир этиладиган жиноий хатти-ҳаракатлар динамикасининг юқори суръатда ўзгариши, жиноят усулларининг трансчегаравий ва тармоқлашган хусусият касб этиши, шунингдек рақамли далиллар билан ишлашдаги процессуал-амалий мураккабликлар миллий жиноят-ҳуқуқий тартибга солишни мунтазам равишда янгилаб бориш зарурлигини кўрсатади. Шу асосда ўтказилган илмий таҳлил натижасида амалдаги тартибга солишда ***қуйидаги ҳуқуқий бўшлиқлар*** мавжудлиги аниқланди. Хусусан:

биринчидан, **“Рақамли активлар”** ва **“Виртуал мулк” тушунчасининг йўқлиги!** Мазкур давлатларнинг илғор ва ижобий тажрибаларини қиёсий-ҳуқуқий таҳлил қилиш натижалари шуни кўрсатадики, ***Янги Ўзбекистон*** шароитида амалдаги ***Жиноят кодекси***да кибержиноятчиликка доир муайян нормалар мавжуд бўлса-да, уларнинг таркибий қамрови ва қўлланиш имкониятлари **рақамли муҳитдаги замонавий таҳдидларнинг барча кўринишларини тўлиқ ифодалашга етарли эмас.** Хусусан, кибермаконда содир этиладиган жиноий хатти-ҳаракатлар динамикасининг юқори суръатда ўзгариши, жиноят усулларининг трансчегаравий ва тармоқлашган хусусият касб этиши, шунингдек рақамли далиллар билан ишлашдаги процессуал-амалий мураккабликлар миллий жиноят-ҳуқуқий тартибга солишни мунтазам равишда янгилаб бориш зарурлигини кўрсатади. Шу асосда ўтказилган илмий таҳлил натижасида амалдаги тартибга солишда ***қуйидаги ҳуқуқий бўшлиқлар*** мавжудлиги аниқланди. Буларга *“Рақамли активлар”* ва *“Виртуал мулк”* тушунчасининг йўқлиги. Жиноят кодексининг 168 ва 169-моддаларида мулк деганда анъанавий моддий буюмлар ёки ҳужжатлар тушунилади[48]. Бироқ, крипто-валюталар, NFTлар, тижорат сири бўлган маълумотлар базаси каби рақамли активларнинг ҳуқуқий мақоми аниқ эмас. Бу эса ушбу активлар ўғирланганда, қилмишни *“Мулкни талон-торож қилиш”* сифатида квалификация қилишда мураккабликлар туғдиради. Буюк Британиянинг 2025 йилги тажрибаси шуни кўрсатадики, рақамли активларни мулк сифатида тан олиш уларнинг ҳуқуқий ҳимоясини тубдан яхшилайди[49].

Иккинчидан, **“Пул ташувчилари” (Money Mules) учун махсус жавобгарликнинг йўқлиги!** Бугунги кунда киберфирибгарлик орқали қўлга киритилган пулларни ўз банк картаси орқали ўтказиб берган шахслар кўпинча

[47] Computer Hacking - 18 U.S.C. § 1030 - Cron Israels and Stark, accessed February 1, 2026, https://www.cronisraelsandstark.com/federal-computer-hacking
[48] 22.09.1994. O‘zbekiston Respublikasining Jinoyat kodeksi - LEX.UZ, accessed February 1, 2026, https://lex.uz/docs/-111453#1480131
[49] The Property (Digital Assets etc) Act 2025: Digital Asset Ownership - Mishcon de Reya, accessed February 1, 2026, https://www.mishcon.com/news/the-property-digital-assets-etc-act-2025-digital-asset-ownership

“билмасдан қилдим” деган важ билан жавобгарликдан қутилиб қолмоқдалар[50]. Сингапур давлатининг ижобий тажрибасига назар ташлаксак, мазкур мамлакатда *“эҳтиётсизлик”* ёки *“бепарволик”* (negligence) учун қатъий жавобгарликнинг мавжудлиги мамлакатда киберфирибгарликни олдини олишга хизмат қилмоқда. Бугунги кунда мазкур қоиданинг мамлакатимиз қонунчилигида ўз аксини топмаганлиги жиноий гуруҳларга ўз фаолиятини кенгайтиришга имкон бермоқда[51].

Учинчидан,* Ижтимоий муҳандислик (Social Engineering) усуллари орқали содир этиладиган киберфирибгарликни квалификация қилиш муаммоси!** Амалиёт таҳлили киберфирибгарлик ҳолатларининг салмоқли қисми жабрланувчини ***психологик таъсир* ва *ишонтириш орқали алдашга асосланган ижтимоий муҳандислик технологиялари *(фишинг, телефон орқали сохта қўнғироқлар — “vishing”, SMS/мессенжер хабарлари орқали алдов — “smishing”, қалбаки идентификация ва “spoofing” каби усуллар)* ёрдамида содир этилаётганини кўрсатади. Бунда жиноят содир этишнинг марказий механизми — ахборотни техник воситалар орқали узатишнинг ўзи эмас, балки жабрланувчининг иродасига таъсир қилиш, уни шошилинч қарор қабул қилишга мажбурлаш ва мол-мулкни (пул маблағини) ***ўзи ихтиёрий равишда*** жиноятчига ўтказишига эришишдан иборат.

Айни пайтда, амалдаги қонунчиликда фирибгарликнинг оғирлаштирувчи белгиларидан бири сифатида ***“ахборот тизимидан, шу жумладан ахборот технологияларидан фойдаланиб”*** содир этиш назарда тутилган[52]. Шунингдек, Олий суд Пленуми ўз тушунтиришларида мазкур белги мазмунини кенг талқин қилиб, компьютер техникаси ва алоқа воситалари *(телефон, планшет ва бошқалар)* орқали манипуляция қилиш йўли билан мулкни алдов асосида қўлга киритиш ҳолатларини ҳам қамраб олишини қайд этади[53].

Шу билан бирга, мавжуд норматив конструкция ижтимоий муҳандисликнинг ***психологик-информацион таъсир*** хусусиятини *(қалбаки шахс сифатида чиқиш, ишончни қасддан суиистеъмол қилиш, “скрипт”лар орқали манипуляция, ишонтириш/қўрқитиш сценарийлари)* батафсил акс эттирмайди. Натижада тергов ва суд амалиётида айрим ҳолатларда бундай қилмишларни *“ахборот технологияларидан фойдаланиб”* содир этилган фирибгарлик сифатида бир хил квалификация қилиш, унинг далилланиши *(алданиш механизми, таъсир усули, жабрланувчи қарор қабул қилиш жараёни)* ҳамда турдош таркиблардан *(масалан, электрон тўлов воситаларига тааллуқли қилмишлар)* аниқ чегаралаш масалалари бўйича ягона ёндашув етарли даражада шаклланмаётгани кузатилади.

***Тўртинчидан,* компьютер тизимига рухсатсиз киришнинг тайёргарлик босқичи етарлича криминализация қилинмагани** *(ёки амалиётда заиф қўлланилаётгани)* **муаммоси!** Қиёсий-ҳуқуқий таҳлиллар шуни

[50] CDSA and CMA Bill Amendments - Singapore Police Force, accessed February 1, 2026, https://www.police.gov.sg/Knowledge-Hub/Legislation/CDSA-and-CMA-Bill-Amendments
[51] *Ўша манбаа:* https://www.police.gov.sg/Knowledge-Hub/Legislation/CDSA-and-CMA-Bill-Amendments
[52] https://lex.uz/uz/docs/111453
[53] Ўзбекистон Республикаси Олий суди пленумининг 2023 йил 23 июндаги *“Фирибгарликка оид ишлар бўйича суд амалиёти тўғрисида”*ги 17-сон Қарори // https://lex.uz/ru/docs/6523582

кўрсатадики, айрим ривожланган давлатлар қонунчилигида *(жумладан Сингапур ва АҚШ амалиётида)* компьютер тизимига мулкий жиноят содир этиш мақсадида рухсатсиз кириш ёки киришга уринишнинг ўзи мустақил ижтимоий хавфли қилмиш сифатида баҳоланиб, эрта босқичда жиноий-ҳуқуқий реакция қўллаш имконини беради[54]. Миллий амалиётда эса кўп ҳолларда ҳуқуқий баҳолаш маркази жиноятнинг *“тугалланган”* натижаси — яъни пул маблағларини қўлга киритиш *(талон-торож қилиш)* фактига кўчиб, тайёргарлик ва уриниш босқичларига нисбатан таъсирчан профилактик инструментлар чекланганлигича қолмоқда. Натижада жиноят содир этилишидан олдин тўхтатиш (preventive) потенциали сусайиб, киберҳужумларни барвақт нейтраллаштириш ва зарарнинг олдини олиш имкониятлари камаймоқда.

Юқоридаги илмий таҳлиллар ва ривожланган давлатларнинг ижобий тажрибасидан келиб чиқиб, Ўзбекистон Республикаси Жиноят кодексига қуйидаги ўзгартиш ва қўшимчаларни киритиш таклиф этилади:

***Биринчидан,* “Рақамли актив” тушунчасини Жиноят кодексига киритиш!** Бунда Буюк Британиянинг 2025 йилги *“Мулк (Рақамли активлар ва бошқалар) тўғрисида”*ги Қонуни тажрибасига таянган ҳолда янги Ўзбекистон Жиноят кодексининг Саккизинчи бўлими *(“Атамаларнинг ҳуқуқий маъноси”)* қуйидаги мазмун билан тўлдирилиши лозим:

***“Рақамли активлар** — рақамли ёки электрон шаклда мавжуд бўлган, эгалик қилиш ва назорат қилиш имконияти мавжуд бўлган, иқтисодий қийматга эга бўлган маълумотлар, крипто-активлар, электрон пул маблағлари ва бошқа номоддий бойликлар”.*

Ушбу тушунчанинг киритилиши *киберўғрилик* ва *киберфирибгарлик* объектларини кенгайтиришга, жабрланувчиларнинг рақамли активларини мулк сифатида ҳимоя қилишга имкон беради.

***Иккинчидан,* пул ташувчилари учун жавобгарлик белгиловчи янги 243[1]-моддани Жиноят кодексига киритиш!** Бунда Сингапурнинг 2023 йилги CDSA ва CMA ўзгартиришлари асосида Жиноят кодексига қуйидаги мазмундаги моддани киритиш таклиф этилади:

“243[1]-модда. Жиноий фаолиятдан олинган даромадларни легаллаштиришга эҳтиётсизлик ёки бепарволик натижасида кўмаклашиш.

Шахснинг ўз тўлов воситалари, банк карталари ёки электрон ҳамёнлари устидан назоратни бошқа шахсларга бериши ёхуд улар орқали маблағларни ўтказиши, агар бу маблағларнинг жиноий фаолиятдан олинганлиги тўғрисидаги шубҳали белгиларга (red flags) эътибор бермаслик ёки эҳтиётсизлик натижасида содир этилган бўлса, —

базавий ҳисоблаш миқдорининг юз бараваридан уч юз бараваригача миқдорда жарима ёки уч йилгача озодликни чеклаш ёхуд уч йилгача озодликдан маҳрум қилиш билан жазоланади”.

[54] Computer Misuse Act 1993 - Singapore Statutes Online, accessed February 1, 2026, https://sso.agc.gov.sg/Act/CMA1993?ViewType=Pdf&_=20260107214642

Бу норма *“пул ташувчилари”* занжирини узишга хизмат қилади ва фуқароларни ўз банк маълумотларига масъулият билан ёндашишга мажбур қилади.

Учинчидан, **Жиноят кодексининг 168-моддасига** *(Фирибгарлик)* **қўшимча киритиш!**

Киберфирибгарликнинг ўзига хос хусусиятини инобатга олиб, *168-модданинг учинчи қисми “г” бандини* қуйидаги таҳрирда баён этиш:

“г) ахборот технологияларидан фойдаланиб, шу жумладан компьютер тизимига ноқонуний кириш ёки ижтимоий муҳандислик усулларини қўллаган ҳолда содир этилган бўлса”

Ижтимоий муҳандисликнинг *(алдовнинг рақамли ва психологик комбинацияси)* алоҳида кўрсатилиши тергов органларига қилмишни тўғри квалификация қилиш ва жазонинг муқаррарлигини таъминлаш имконини беради.

Тўртинчидан, **Жиноят кодексининг 169-моддасига** ***(Ўғрилик)*** **ўзгартиш киритиш!** Ўзбекистон Республикаси ЖКнинг **169-модда учинчи қисмининг “б” бандини** рақамли активларни ўз ичига оладиган қилиб кенгайтириш:

“б) компьютер тизимига, ахборот ресурсларига ёки рақамли активлар сақланадиган омборларга рухсатсиз кириб содир этилган бўлса;”

Бу Сингапур давлатининг CMA 4-моддаси ва АҚШнинг CFAA 1030(a)(4) нормаларига мос келади ва рақамли муҳитда ўғрилик учун жазони оғирлаштирувчи омил сифатида мустаҳкамлайди.

Хулоса ўрнида шуни таъкидлаш жоизки, кибермакондаги мулкий жиноятларнинг криминологик тавсифи уларнинг нафақат миқдор жиҳатидан ўсишини, балки сифат жиҳатидан мураккаблашиб бораётганини кўрсатмоқда. Ўзбекистонда кибержиноятлар сонининг 68 баравар ортгани ва зарар кўламининг триллионлаб сўмга етгани қонунчиликни зудлик билан ислоҳ қилишни тақозо этади.

Ривожланган давлатлар, хусусан *Сингапур, Буюк Британия* ва бошқа ривожланган давлатларнинг ижобий тажрибаси шуни тасдиқлайдики, кибержиноятчиликка қарши курашда иккита асосий йўналиш бўлиши лозим:

1. ***Ҳуқуқий инструментларнинг мослашувчанлиги:*** Рақамли активларни мулк сифатида тан олиш ва жиноятнинг барча иштирокчиларини (жумладан "бепарво" пул муллаларини) жавобгарликка тортиш.
2. ***Технологик ва ижтимоий профилактика:*** Банк тизимларини ҳимоялаш ва аҳолининг рақамли гигиенасини ошириш (Эстония модели).

Таклиф этилаётган қонунчилик ўзгартиришлари миллий жиноят ҳуқуқини халқаро стандартларга яқинлаштиради, кибержиноятчиликнинг иқтисодий базасини заифлаштиради ва фуқароларнинг рақамли макондаги ҳуқуқларини ишончли ҳимоя қилишга хизмат қилади. Бу эса, ўз навбатида, мамлакатда рақамли иқтисодиётнинг барқарор ўсиши ва фуқароларнинг давлат ахборот тизимларига бўлган ишончини мустаҳкамлашнинг асосий омили бўлади.