КИБЕРЖИНОЯТ НИМА ВА УНИ АНЪАНАВИЙ ЖИНОЯТЛАРДАН ФАРҚЛОВЧИ АСОСИЙ ХУСУСИЯТЛАР

Аширбоев Ахроржон Тиркаш ўғли
Ўзбекистон Республикаси Ички
ишлар вазирлиги Академияси
Киберҳуқуқ кафедраси катта ўқитувчиси
E-mail: ashirboyevaxrorjon@gmail.com
https://doi.org/10.5281/zenodo.17617591

ARTICLE INFO

Qabul qilindi: 10-noyabr 2025 yil
Ma'qullandi: 12-noyabr 2025 yil
Nashr qilindi: 15-noyabr 2025 yil

KEYWORDS

кибержиноят, киберҳавфсизлик, жиноят қонунчилиги, рақамли ҳуқуқлар, трансчегаравий жиноят, анонимлик, компютер тизимлари, ахборот технологиялари.

ABSTRACT

Ушбу мақолада замонавий ахборот жамиятида кибержиноятларнинг долзарблиги, уларнинг умумий тушунчаси ва анъанавий жиноятлардан фарқловчи хусусиятлари таҳлил қилинган. Мақолада Ўзбекистон Республикасида амалга оширилаётган суд-ҳуқуқ ислоҳотлари ва кибержиноятчиликка қарши курашнинг ҳуқуқий асослари кўриб чиқилган. Кибержиноятларнинг икки асосий категорияси ҳамда Жиноят кодексида белгиланган турлари тавсифланган. Мақолада киберҳавфсизликни таъминлаш ва фуқароларнинг рақамли ҳуқуқларини ҳимоя қилиш давлат сиёсатининг устувор йўналиши сифатида таъкидланган

Ҳозирги замонда ахборот-коммуникация технологияларининг жадал суръатлар билан ривожланиши кибержиноятларни глобал даражадаги муаммога айлантирди. Рақамли технологиялар инсоният ҳаётининг барча соҳаларини қамраб олган шароитда, киберҳужумлар, маълумотлар ўғирланиши, молиявий алдов ва ахборот тизимларига ноқонуний кириш каби жиноятлар тобора кенг кўлам олмоқда. Дунё бўйича йиллик миллиардлаб доллар зарар келтираётган бу жиноятлар нафақат алоҳида шахсларга, балки йирик корхоналар, давлат муассасалари ва ҳатто бутун мамлакатларнинг миллий хавфсизлигига жиддий таҳдид солмоқда. Шу сабабли, кибержиноятчиликка қарши курашиш бутун жаҳон ҳамжамияти учун долзарб вазифага айланган бўлиб, ҳар бир давлатдан самарали қонунчилик базасини яратиш ва халқаро ҳамкорликни кучайтиришни тақозо этмоқда.

Республикада 2023 йилда содир этилган жами жиноятларнинг 7,2%, 2024 йилда 45% кибержиноятлар ташкил етган бўлса, жорий йилнинг 8 ойида жами содир етилган жиноятларнинг 45% кибержиноятлар ташкил етганлигини, шундан, 97% ёки 37 207 тасини электрон тўлов тизимлари орқали банк карталаридаги пулларни ўғирлаш ва фирибгарлик йўли билан қўлга киритиш жиноятлари, 316 тасини крипто-активлар билан боғлиқ ва 23 тасини ахборот технологиялари соҳасидаги жиноятлар ташкил этганлигини кузатишимиз мумкин[1].

Бундай кескин ўсишнинг асосий сабаби банк карталари, интернет-банкинг ва мобил алоқа орқали амалга оширилаётган киберфирибгарлик ҳамда киберўғирлик ҳолатларининг тобора кенг тарқалиб кетишидадир. Айниқса, пандемиядан кейинги даврда аҳолининг рақамли хизматлардан фойдаланиши жадал суръатлар билан ошганлиги, лекин киберхавфсизлик саводхонлиги шу даражада ривожланмаганлиги муаммони янада чуқурлаштирди. Мазкур статистик маълумотлар киберхавфсизлик масаласи нафақат техник ва ҳуқуқий, балки кенг қамровли ижтимоий-иқтисодий муаммога айланганлигидан, шунингдек, бу соҳада комплекс профилактика чораларини кўриш зарурлигидан далолат беради.

Замонавий ахборот жамиятининг ривожланиши билан кибержиноятлар янги турдаги таҳдидга айланди. Давлатнинг кибержиноятчиликка қарши кураш сиёсатини амалга оширишда жиноят қонунчилиги муҳим аҳамиятга эга, чунки у кибержиноятчиликка қарши курашнинг асосий ҳуқуқий асосларидан биридир.

Шунингдек, кибержиноятчиликка қарши курашда шахс ахборот технологиялари соҳасида содир этган ижтимоий хавфли қилмиши учун жиноий жавобгарликка тортилади ҳамда унга нисбатан мос жазо тайинланади. Кибержиноятларнинг трансчегаравий характери, анонимлик имкони ва технологик мураккаблиги уларни анъанавий жиноятлардан ажратиб турувчи хусусиятлар ҳисобланади.

Республикамизда рақамли технологияларнинг жадал ривожланиши ва интернет фойдаланувчилари сонининг ортиши натижасида киберхавфсизликни таъминлаш давлат сиёсатининг муҳим йўналишларидан бирига айланди. Бу жараёнда фуқароларнинг рақамли ҳуқуқларини ҳимоя қилиш ҳамда кибержиноятларнинг олдини олиш устувор вазифалар қаторига киритилган.

Шу ўринда кибержиноятнинг умумий тушунчасига тўхталиб ўтиш мақсадга мувофиқдир. Замонавий ахборот технологияларининг ривожланиши билан бирга жиноятчилик соҳасида ҳам янги турдаги хавфли қилмишлар юзага келди. Кибержиноят деганда ахборот-коммуникация технологиялари, компьютер тизимлари, интернет тармоқлари ва рақамли қурилмалардан восита сифатида фойдаланиш ёки уларни бевосита нишонга олиш орқали амалга ошириладиган ноқонуний ҳаракатлар тушунилади.

Ўзбекистон Республикаси Жиноят кодексининг тегишли моддаларида кибержиноятларнинг асосий турлари белгиланган. Жиноят Кодексининг XX[1] бобида ахборот технологиялари орқали содир этиладиган жиноятлар аниқ белгиланган. Булар 278[1]-модда “Ахборотлаштириш қоидаларини бузиш”, 278[2]-модда “Компьютер ахборотидан қонунга хилоф равишда (рухсатсиз) фойдаланиш”, 278[3]-модда “Компьютер тизимидан, шунингдек телекоммуникация тармоқларидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус воситаларни ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш”, 278[4]-модда “Компьютер ахборотини модификациялаштириш”, 278[5]-модда “Компьютер саботажи”, 278[6]-модда “Зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш”, 278[7]-модда “Телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш”, 278[8]-модда “Крипто-активлар айланмаси соҳасидаги қонунчиликни бузиш” ва 278[9]-модда “Майнинг фаолиятини қонунга хилоф равишда амалга ошириш” киради[2]. Ушбу

қилмишлар виртуал муҳитда содир этилади ва технологик тараққиёт билан доимий равишда янги кўринишларга эга бўлиб боради.

Таъкидлаш жоизки, юқорида рўйхати келтирилган жиноятлар кибермаконда содир этилаётган жиноятларнинг деярли 10%ни ташкил етаётган бўлса, қолган қисмини, яъни 90%ни, электрон тўлов тизимлари орқали банк карталаридаги пулларни ўғирлаш ва фирибгарлик йўли билан қўлга киритиш жиноятлари ташкил етаётганлигини кўришимиз мумкин.

Савол туғилади нима сабабдан айнан мазкур жиноятларнинг салмоғи ортиб бормоқда?

Электрон тўлов тизимлари орқали банк карталаридаги пулларни ўғирлаш ва фирибгарлик йўли билан қўлга киритиш жиноятларининг салмоғи ортиб боришининг бир қатор объектив ва субъектив сабаблари мавжуд.

Биринчидан, пандемия даврида ва ундан кейинги даврда аҳолининг рақамли молиявий хизматлардан фойдаланиши жадал суръатлар билан ошди. Статистик маълумотларга кўра, Ўзбекистонда интернет-банкинг ва мобил иловалар орқали амалга ошириладиган молиявий операциялар ҳажми сўнгги беш йилда ўн баробардан ортиқ ўсди. Бунда аҳолининг катта қисми анъанавий банк хизматларидан рақамли технологияларга ўтди, аммо киберхавфсизлик саводхонлиги шу даражада ривожланмади.

Иккинчидан, жиноятчилар учун электрон тўлов тизимлари нисбатан осон ва хавфсиз нишонга айланган. Анъанавий ўғирлик ва талон-торож жиноятларидан фарқли равишда, киберфирибгарлик масофадан, анонимлик шароитида ва жисмоний хавф-хатарсиз амалга оширилади. Жиноятчилар сохта веб-сайтлар, фишинг хабарлари ва ижтимоий муҳандислик усулларидан фойдаланиб, қурбонларнинг банк карталари маълумотлари, SMS-кодлар ва паролларини осонгина қўлга киритмоқдалар.

Учинчидан, банк сирини ташкил етувчи маълумотларнинг қурбонлар томонидан ўзлари томонидан очиб берилиши муаммони янада оғирлаштирмоқда. Фирибгарлар психологик таъсир усулларини қўллаб, ўзларини банк ходимлари, ҳуқуқ-тартибот органлари вакиллари ёки яқин қариндошлар деб таништириб, қурбонларни вақтинча ишончга киритадилар. Хавотир, қўрқув ва шошилинчлик ҳолатида одамлар танқидий тафаккур қилиш қобилиятини йўқотиб, махфий маълумотларни берадилар.

Тўртинчидан, молиявий муассасаларнинг киберҳимоя тизимлари ҳали етарли даражада такомиллашмаган. Гарчи банклар замонавий шифрлаш технологиялари ва икки факторли аутентификацияни жорий етган бўлсалар-да, жиноятчилар доимо янги заифликларни топиб, ҳужум усулларини такомиллаштириб бормоқдалар. Айниқса, булутли технологиялар, криптовалюталар ва халқаро тўлов тизимлари орқали пул маблағларини тезкор кўчириш имкониятлари жиноятчиларга қулай шароитлар яратмоқда.

Бешинчидан, трансчегаравий характер ва юрисдикция муаммолари бу турдаги жиноятларнинг очилиш даражасини пасайтирмоқда. Кўпинча жиноятчилар бошқа давлатлар ҳудудида жойлашган бўлиб, уларни қўлга олиш ва жавобгарликка тортиш халқаро ҳуқуқий ҳамкорлик ва экстрадиция жараёнларининг мураккаблиги туфайли қийинлашади. Бу эса жиноятчиларга жазосизлик ҳиссини бериб, уларнинг фаолиятини давом эттиришига туртки бўлмоқда.

Фикримизча кибержиноятларни икки асосий категорияга бўлиш тўғри бўлади. Биринчиси, компютер ва ахборот тизимларининг ўзига қарши йўналтирилган қилмишлар бўлиб, бунда технология асосий нишон ҳисобланади. Иккинчиси, анъанавий жиноятларни содир этишда рақамли воситалардан фойдаланишни ўз ичига олади.

Кибержиноятларнинг анъанавий жиноятлардан фарқловчи хусусиятлари:

Жойлашув ва масофа омилининг йўқлиги. Анъанавий жиноятларда жиноятчи ва жабрланувчи одатда бир жойда бўлиши ёки жисмоний яқинлик мавжуд бўлиши зарур. Масалан, ўғирлик, босқинчилик ёки қасдан жароҳат етказиш содир этилиши учун айбдор воқеа рўй берган жойда бўлиши керак. Кибержиноятларда эса вазият бутунлай бошқачадир – жиноят содир этаётган шахс дунёнинг исталган нуқтасидан ҳаракат қилиши мумкин. Жиноятчи бир қитъада туриб, бутунлай бошқа қитъадаги банк ҳисобларини ўғирлаши ёки корхоналарнинг тизимларини бузиши мумкин. Бундай масофавий амалларни содир этиш имкони жиноятчи шахсларга катта устунлик беради: улар ўз шахсларини яширадилар ва қўлга олиниш эҳтимолини сезиларли даражада камайтирадилар.

Трансчегаравий характер. Анъанавий жиноятлар асосан бир давлат ҳудудида содир этилади ва маҳаллий ҳуқуқ-тартибот органлари томонидан тергов қилинади. Кибержиноятлар эса бир вақтнинг ўзида бир неча мамлакат ҳудудларини қамраб олиши мумкин. Масалан, жиноятчи шахс биринчи давлатда бўлиб, иккинчи давлатдаги серверлардан фойдаланган ҳолда, учинчи давлатдаги жабрланувчиларга зарар етказиши мумкин. Бундай вазият халқаро ҳуқуқий мураккабликлар келтириб чиқаради, чунки ҳар бир мамлакатнинг ўз юрисдикцияси ва қонунчилиги мавжуд.

Анонимлик ва яширинлик имкони. Анъанавий жиноятларда айбдорни аниқлаш учун кўп сонли физик далилларга таянилади: бармоқ излари, ДНК намуналари, гувоҳлар кўрсатувлари, видео кузатув материаллари ва бошқалар. Кибержиноятларда эса жиноятчи махфий тармоқлар, сохта профиллар, прокси серверлар ва шифрлаш технологияларидан фойдаланиб ўз шахсини сир сақлаши мумкин. Улар ҳақиқий IP манзилларини беркитиш, сохта электрон почта ва виртуал аккаунтлар яратиш, “Bitcoin” каби криптовалюталардан фойдаланиш орқали ўз изларини йўқотишга интиладилар.

Тезкорлик ва кўп қурбонлик. Анъанавий жиноятларда одатда бир вақтда чекланган сондаги қурбонлар бўлади. Масалан, ўғри бир уйга кириб бир оилага зарар етказади ёки фрибгар бир неча кишини алдайди. Кибержиноятларда жиноятчи бир неча сония ичида минглаб, ҳатто миллионлаб одамга зарар етказиши мумкин. Масалан, компютер вируси тарқалгандан сўнг бир неча соат ичида дунё бўйлаб миллионлаб компютерни зарарлаши мумкин.

Далилларни йўқ қилиш осонлиги. Анъанавий жиноятларда далилларни тўлиқ йўқ қилиш қийин, чунки жисмоний излар кўп вақт давомида сақланиб қолади. Кибержиноятларда жиноятчи рақамли далилларни тезда ва тўлиқ йўқ қилиши мумкин. Бир марта “delete” тугмасини босиш орқали катта ҳажмдаги ахборотни йўқ қилиш мумкин.

Технологик мураккаблик. Анъанавий жиноятларни тушуниш ва тергов қилиш учун одатий ҳуқуқий билимлар етарли бўлади. Кибержиноятларни тергов қилиш юқори технологик билимларни талаб қилади. Тергов органлари

ходимлари компьютер тармоқлари, дастурлаш, шифрлаш, операцион тизимлар ва бошқа кўп соҳалар бўйича махсус билимларга эга бўлиши керак.

Замонавий характер. Анъанавий жиноятлар одатда муайян вақт давомида содир этилади ва аниқ бошланиш ҳамда тугаш нуқталарига эга. Кибержиноятлар узоқ вақт давомида давом этиши мумкин. Масалан, хакер компанияга кириб, ойлар давомида махфий маълумотларни ўғирлаб туриши мумкин.

Катта молиявий оқибатлар. Анъанавий жиноятларнинг молиявий зарари одатда чекланган ва аниқ бўлади. Кибержиноятларнинг иқтисодий оқибатлари эса жуда катта ва кўп қиррали бўлиши мумкин. Бир марталик ҳужум миллиардлаб доллар зарар келтириши мумкин.

Автоматлаштириш имкони. Анъанавий жиноятчилар ўз фаолиятини автоматлаштира олмайдилар ва ҳар бир ҳаракатни қўлда бажариши керак. Кибержиноятчилар эса ўз ҳужумларини тўлиқ автоматлаштириши мумкин. Улар бир марта зарарли дастур ишлаб чиқиб, уни тармоққа жойлаштириши мумкин ва бу дастур автоматик тарзда минглаб қурилмага зиён етказа бошлайди.

Доимий ривожланувчи характер. Анъанавий жиноят усуллари асрлар давомида деярли ўзгармайди. Кибержиноят усуллари эса технология тараққиёти билан доимо янгиланиб ва мураккаблашиб боради. Ҳар куни янги зарарли дастурлар, ҳужум тартиблари ва заифликлар юзага келади.

Кибержиноятчиликка қарши самарали курашиш ва киберхавфсизликни таъминлаш бўйича таклифлар:

Кибержиноятлар учун жиноят кодексида белгиланган жазо санкцияларини қайта кўриб чиқиш ва оғирлаштириш. Кибержиноятлар келтирадиган молиявий зарарнинг жуда юқори миқдорда бўлишини ҳисобга олган ҳолда, жарима миқдорларини ошириш ва озодликдан маҳрум қилиш муддатларини узайтириш мақсадга мувофиқдир.

Ҳуқуқни муҳофаза қилувчи орган ходимларининг киберхавфсизлик бўйича малакасини ошириш тизимини жорий этиш. Тергов органлари, суд ва прокуратура ходимлари учун рақамли далилларни йиғиш, таҳлил қилиш ва судда тақдим этиш бўйича доимий тренинглар ва қайта тайёрлов курсларини ташкил этиш зарур.

Кибержиноятларга қарши самарали курашиш учун халқаро ҳуқуқий ҳужжатлар ва стандартларга қўшилиш долзарб зарурият ҳисобланади. Айниқса, кибержиноятчилик бўйича асосий халқаро ҳужжат – Европа Кенгашининг 2001-йилда қабул қилинган “Кибержиноятчиликка қарши конвенцияси” (Будапешт конвенцияси)га ахборот алмашиш ва ҳамкорликни ривожлантириш мақсадга мувофиқдир[3]. Мазкур конвенция кибержиноятларнинг умумий таснифини, уларга қарши курашнинг процессуал механизмларини ва давлатлараро ҳамкорлик тартибини белгилаб беради. Республикамизнинг ушбу конвенцияга қўшилиши ёки унинг асосий тамойилларини миллий қонунчиликка имплементация қилиши орқали халқаро тажрибадан фойдаланиш, қўшни ва минтақавий давлатлар билан уйғун меъёрий-ҳуқуқий база яратиш, шунингдек трансчегаравий кибержиноятларни тергов қилишда халқаро ҳамкорликни кучайтириш имкониятлари яратилади. Бундан ташқари, Интерпол ва бошқа халқаро ташкилотлар томонидан ишлаб чиқилган киберхавфсизлик стандартларини қабул қилиш ҳам муҳим аҳамият касб этади.

Аҳоли ўртасида киберхавфсизлик саводхонлигини ошириш бўйича кенг қамровли маълумот кампанияларини ўтказиш. Телевидение, радио, ижтимоий тармоқлар орқали фуқароларни кибержиноятларнинг турли шакллари, уларнинг олдини олиш чоралари ва хавфсиз интернетдан фойдаланиш қоидалари билан доимий равишда таништириб бориш керак.

Таълим тизимига киберхавфсизлик асосларини мажбурий фан сифатида киритиш. Умумтаълим мактаблари, касб-ҳунар коллежлари ва олий таълим муассасаларида киберхавфсизлик, рақамли саводхонлик ва ахборот технологиялари этикаси бўйича алоҳида фанларни жорий этиш зарур.

Банк ва молия муассасалари учун мажбурий киберхавфсизлик стандартларини жорий этиш. Барча банклар, тўлов тизимлари ва молиявий ташкилотлар учун икки факторли аутентификация, зарарли фаолиятни аниқлаш тизимлари ва мижозларнинг ҳақиқийлигини текшириш механизмларини мажбурий равишда жорий этиш лозим.

Рақамли далилларни қонуний асосда йиғиш ва сақлаш бўйича технологик инфратузилмани яратиш. Махсус криминалистик лабораторияларни ташкил этиш, рақамли далилларни йиғиш ва таҳлил қилиш учун халқаро стандартларга мос дастурий таъминот ва аппаратларни жорий этиш керак.

Мамлакатимизда инсон ҳуқуқ ва эркинликларини ҳимоя қилиш, киберхавфсизликни таъминлаш ва кибержиноятчиликка қарши самарали кураш юритиш давлат сиёсатининг устувор йўналишларидан бири сифатида белгиланган. Бу борадаги ислоҳотлар фуқароларнинг рақамли ҳуқуқларини ҳимоя қилиш ва замонавий таҳдидларга мослашувчан ҳуқуқий база яратишга қаратилган.

Фойдаланилган адабиётлар:

1. Ўзбекистон Республикаси Ички ишлар вазирлиги ҳузуридаги Киберхавфсизлик марказининг статистик маълумотномаси, 2023–2025 йиллар.
2. Ўзбекистон Республикаси Жиноят кодекси. – Т., 2025.
3. Будапешт конвенцияси – Европа Кенгашининг “Кибержиноятчиликка қарши конвенцияси” (Convention on Cybercrime). – coe.int.
4. Ўзбекистон Республикасининг 2022 йил 15 апрелдаги ЎРҚ-721-сон “Киберхавфсизлик тўғрисида”ги Қонуни.
5. Ўзбекистон Республикаси Президентининг 2025 йил 30 апрелдаги ПҚ-153-сон “Ахборот технологиялари ёрдамида содир этилган жиноятларга қарши курашни кучайтириш чора-тадбирлари тўғрисида”ги қарори.
6. Ўзбекистон Республикаси Президентининг 2024 йил 11 сентябрдаги ПФ-246-сон ““Ўзбекистон–2030” стратегиясини амалга ошириш чора-тадбирлари тўғрисида”ги Фармони.