РАҚАМЛИ ЖИНОЯТЧИЛИКНИНГ ЗАМОНАВИЙ КЎРИНИШЛАРИ ВА УЛАРНИНГ ХУСУСИЯТЛАРИ

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.18515943

ARTICLE INFO

Qabul qilindi: 01- fevral 2026 yil
Ma'qullandi: 04- fevral 2026 yil
Nashr qilindi: 07- fevral 2026 yil

KEY WORDS

кибержиноят, киберҳуқуқбузарлик, ахборот хавфсизлиги, киберхавфсизлик, фишинг, фирибгарлик, зарарли дастурлар (малваре), кибертерроризм, трансмиллий жиноятлар, ахборот технологиялари.

ABSTRACT

Мазкур мақолада рақамли технологиялар орқали содир этилаётган жиноятларнинг жаҳон ҳамжамияти учун долзарб ва мураккаб муаммо сифатида шаклланаётгани, кибержиноятлар трансмиллий хусусият касб этиб, давлат институтлари, халқаро ташкилотлар, тижорат ва молия секторлари ҳамда фуқароларга жиддий хавф туғдириши атрофлича таҳлил қилинган. Киберҳуқуқбузарликларнинг турлари, замонавий йўналишлари ва уларнинг тез ўсиш динамикасига халқаро манбалар, қонунчилик ҳамда илғор таҳлиллар асосида баҳо берилган. Шунингдек, фишинг, фирибгарлик, зарарли дастурлар, deepfake ва кибертерроризм каби таҳдидлар, уларга қарши курашнинг ҳуқуқий, техник ва ташкилий йўналишлари, рақамли хавфсизликни таъминлашда жамият ва давлат органларининг ўзаро ҳамкорлиги, ахолининг саводхонлиги ва миллий қонунчиликдаги янгиликлар ёритилган. Мақолада рақамли хавфсизлик соҳасидаги долзарб тенденциялар ва муаммолар таҳлил қилиниб, уларга қарши самарали ёндашувлар таклиф этилган

Рақамли технологиялар воситасида содир этилаётган жиноятлар бугунги кунда жаҳон ҳамжамиятининг энг долзарб ва мураккаб муаммоларидан бирига айланган. Глобаллашув шароитида кибержиноятлар кун сайин ортиб бормоқда. Афсуски, рақамли технологиялар воситасида содир этилаётган жиноятлар рақамли муҳитнинг барқарорлигига узлуксиз зарба бермоқда. Бу соҳадаги киберҳуқуқбузарликлар давлат институтлари, халқаро ташкилотлар, тижорат субъектлари, банк-молия тузилмалари ҳамда жамият аъзолари ўртасидаги алоқаларга салбий таъсир кўрсатмоқда.

Бугунги кунда киберҳужумлар давлат бошқарувининг ахборот инфратузилмаси ва имкониятларига, халқаро ҳамда миллий корхоналарнинг маълумотлар омборларига,

банк секторининг рақамли технологияларига, шунингдек, фуқароларнинг турмуш тарзи ва саломатлигига, фуқароларнинг ҳуқуқ ва эркинликларига хавф солмоқда.

Бундан ташқари, киберҳужумлар трансмиллий хусусиятга эга бўлиб, бир давлат ҳудудидан бошқа мамлакатга нисбатан содир этилиши мумкин ва ҳуқуқбузарликлар иқтисодий жиҳатдан тез фойда келтириши ва амалга ошириш осон ва тезлиги уларга ўз вақтида қарши курашни талаб этади. Натижада, жиноят-ҳуқуқий соҳада рақамли жиноятчиликни тартибга солувчи меъёрий-ҳуқуқий нормаларни такомиллаштириш, кибержиноятларни содир этган шахсларни муносиб жазолаш зарурати кундалик ҳаётда яққол намоён бўлмоқда.

Ҳозирги замон кенг кўламли модернизация жараёнларининг жорий босқичида жаҳон мамлакатлари томонидан рақамли жиноятчиликка қарши умумий кураш олиб бориш, давлатлараро норматив ҳужжатларни такомиллаштириш ҳамда уларни мувофиқлаштириш, халқаро миқёсда стандартлаштирилган рақамли тадқиқот юритиш, маълумотлар алмашинувини интеграциялашган тарзда йўлга қўйиш, кибермуҳит хавфсизлигини таъминлашда ўзаро маълумот алмашиш, мутахассисларнинг касбий малакасини ривожлантириш, халқаро майдонларда тажриба алмашинувни йўлга қўйишни талаб қилмоқда. Мамлакатимизда “Кибержиноят” деб аталувчи рақамли жиноятчилик турларига қарши амалдаги қонунчиликни тизимлаштириш, ташкилий-амалий тадбирларни биргаликда амалга ошириш бўйича муҳим қадамлар қўйилмоқда. Жорий этилаётган ислоҳотлар доирасида, трансмиллий рақамли жиноятчиликни жиноят-ҳуқуқий меъёрий жиҳатдан тартибга солувчи қонунчилик базасини уйғунлаштириш ҳамда стандартлаштириш йўли билан мазкур жиноятларга қарши курашни мустаҳкамлаш, шунингдек кибермуҳит барқарорлигини халқаро ҳамкорлик алоқаларини мустаҳкамлаш орқали таъминлаш мумкин.

Ҳар бир давлатнинг барқарор тараққиёти ҳамда ривожланишини инсон омили, шунингдек, интернет ва компьютерларсиз тасаввур қилиш қийин. Рақамли технологиялар, электрон хизматлар ҳар бир хонадонга кириб улгурди. Инсонлар кундан-кун ахборот-коммуникация технологияларига тобора қарам бўлиб бораётганлиги, ахборотларни ҳимоялаш ва улардан фойдаланиш қоидаларига риоя этилишини таъминлаш муҳим аҳамият касб этмоқда. Яъни, жамиятни ахборотлаштиришнинг муҳим шарти, бу киберхавфсизликни таъминлашдан иборат.

Шунингдек, рақамли технологиялар ҳозирги ёш авлод ҳаётини кўп жиҳатдан ўзгартириб, уларни интернет ва ижтимоий тармоқлар асирига айлантирилмоқда.

БМТ Халқаро телекоммуникация иттифоқи (ITU) 2024 йил ҳисоботига кўра, дунёда интернетдан фойдаланувчи ёшлар сони барча ёш тоифалари орасида энг баланд кўрсаткичга эга бўлган гуруҳ — 15-24 ёшлардир.

2024 йилда мазкур ёш гуруҳининг 70% дан ортиғи интернетдан фойдалангани қайд этилган[1].

Бу рақам катта ёшлилар (24 ёшдан юқорилар) билан солиштирилганда анча юқори.

Юртимизда энг аввало ёш авлодда кибержиноятлардан ҳимояланиш иммунитетини шакллантириш, кибержиноятлар турларидан огоҳлантириш ҳамда бу каби жиноятлар оламига қадам қўйишларига йўл қўймаслик биринчи галдаги вазифалардан бири ҳисобланади.

Шу билан бирга, замонавий ахборот тизимларини яратилиши билан бир қаторда, турли вирусли дастурларнинг тарқалиши, ҳимоя паролларни бузиш, қонунга зид бўлган ахборотларни тарқатиш, хакерлик ҳужумлари, корхона, муассаса ва ташкилотларнинг расмий веб-сайтларига ноқонуний кириш, муаллифлик ҳуқуқини бузилиши, фирибгарлик ва банк карталарини ноқонуний эгаллаш ҳамда пул маблағларини талон-торож қилиш каби ахборот технологияларидан фойдаланиб содир этилаётган жиноятлар кун сайин ортиб бормоқда.

Хусусан, Cybersecurity Ventures ва Statista маълумотларига кўра, киберҳужумлар ва киберфирибгарлик ҳолатлари ҳар йили ўртача 15–20% га кўпайган[2].

Kaspersky Lab ҳисоботларида қайд этилишича, 2022–2025 йиллар орасида аниқланган глобал киберҳужумлар сони йил сайин ўсиб, айрим йилларда 30–40% гача ўсиш кузатилган[3].

INTERPOL маълумотига кўра, 2024–2025 йилларда кибержиноятлар – айниқса, фирибгарлик ва фишинг — дунё бўйича энг тез ўсувчи жиноят турларидан бирига айланган[4].

Шундан, фирибгарлик, ўғрилик, тақиқланган материалларни тарқатиш, тинчлик, хавфсизлик ва давлатга қарши жиноятлар (кибертерроризм), товламачилик, туҳмат ва ҳақорат, таваккалчиликка асосланган ўйинларни интернет орқали ўтказилиш ҳамда молиявий пирамида шаклидаги пул маблағларини ва бошқа мол-мулкни жалб этишга доир ноқонуний фаолият турлари олдинги йилларга нисбатан кўпайган.

Жаҳон иқтисодий форуми (World Economic Forum) ва Cybersecurity Ventures'нинг маълумотларига кўра, 2023 йилда кибержиноятлардан дунё миқёсида келадиган зарар $8 трлн (8 trillion) долларни ташкил этган. Cybersecurity Ventures таҳминига кўра, 2026 йилга бориб бу кўрсаткич $10.5 трлн (10 trillion) долларга етиши мумкинлигини такидлаган[5].

Ўзбекистон Республикасининг "Киберхавфсизлик тўғрисида"ги 2022 йил 15 апрелдаги Қонуни билан "Кибержиноятчилик" тушунчасига таъриф берилган бўлиб, унга кўра, "Ахборотни эгаллаш, уни ўзгартириш, йўқ қилиш ёки ахборот тизимлари ва ресурсларини ишдан чиқариш мақсадида кибермаконда дастурий таъминот ва техник воситалардан фойдаланилган ҳолда амалга ошириладиган жиноятлар йиғиндиси – кибержиноятчилик" деб белгиланган[6].

Ўзбекистон Республикаси Жиноят кодексида кўзда тутилган ахборот технологиялари соҳасига оид жиноят турлари белгилаб берилган. Жумладан:

1. Ўзини ўзи ўлдириш даражасига етказиш (ЖК 103-м 2-қ "г" банд);
2. Ўзини ўзи ўлдиришга ундаш (ЖК 103^1-м 2-қ "в" банд);
3. Порнографик маҳсулотни тайёрлаш, олиб кириш, тарқатиш, реклама қилиш, намойиш этиш (ЖК 130-м);
4. Тазйиқни, зўравонликни ёки шафқатсизликни тарғиб қилувчи маҳсулотни тайёрлаш, олиб кириш, тарқатиш, реклама қилиш, намойиш этиш (ЖК 130^1-м);
5. Туҳмат (ЖК 139-м 2-қ);
6. Ҳақорат қилиш (ЖК 140-м 2-қ);
7. Шахсга доир маълумотлар тўғрисидаги қонунчиликни бузиш (ЖК 141^2-м);

8. Шахснинг шаънини ва қадр-қимматини камситувчи ҳамда инсон ҳаётининг сир тутиладиган томонларини акс эттирувчи маълумотларни ошкор қилиш (ЖК 141^3-м);

9. Ўзбекистон Республикаси Президентига тажовуз қилиш (ЖК 158-м 3-қ);

10. Товламачилик (Ахборот технологиялари воситасида содир этилган бўлса) (ЖК 165-м);

11. Ўзлаштириш ёки растрата йўли билан талон-торож қилиш (ЖК 167-м 3-қ "г" банд);

12. Фирибгарлик (ЖК 168-м 3-қ "г" банд);

13. Ўғрилик (ЖК 169-м 3-қ "б" банд);

14. Пул маблағларини ва (ёки) бошқа мол-мулкни жалб этишга доир ноқонуний фаолият (ЖК 188^1-м 2-қ "г" банд);

15. Оммавий тартибсизликлар (244-м 2-қ "б" банд);

16. Жамоат ҳавфсизлиги ва жамоат тартибига таҳдид соладиган материалларни тайёрлаш, сақлаш, тарқатиш ёки намойиш этиш (ЖК 244^1-м 3-қ "г" банд);

17. Карантинли ва инсон учун хавфли бўлган бошқа юқумли касалликлар тарқалиши ҳақида ҳақиқатга тўғри келмайдиган маълумотларни тарқатиш (ЖК 244^5-м);

18. Ёлғон ахборот тарқатиш (ЖК 244^6-м);

19. Гиёҳвандлик воситалари, уларнинг аналоглари ёки психотроп моддалар ҳисобланмайдиган кучли таъсир қилувчи моддаларни тарғиб қилувчи маҳсулотни тайёрлаш, тарқатиш, реклама қилиш, намойиш этиш ёки бундай моддаларни ёхуд заҳарли моддаларни қонунга хилоф равишда муомалага киритиш (ЖК 251^1-м);

20. Гиёвандлик воситалари, уларнинг аналоглари ёки психотроп моддаларни ўтказиш мақсадини кўзлаб қонунга хилоф равишда тайёрлаш, олиш, сақлаш ва бошқа ҳаракатлар қилиш, шунингдек уларни қонунга хилоф равишда ўтказиш (ЖК 273-м 3-қ "д" банд);

21. Гиёҳвандлик воситаларини, уларнинг аналогларини ёки психотроп моддаларни тарғиб қилувчи маҳсулотни тайёрлаш, тарқатиш, реклама қилиш, намойиш этиш ёки бундай моддаларни истеъмол қилишга жалб этиш (ЖК 274-м);

22. Қимор ва таваккалчиликка асосланган бошқа ўйинларни ташкил этиш ҳамда ўтказиш (ЖК 278-м 3-қ);

23. Ахборотлаштириш қоидаларини бузиш (ЖК 278^1-м);

24. Компьютер ахборотидан қонунга хилоф равишда (рухсатсиз) фойдаланиш (ЖК 278^2-м);

25. Компьютер тизимидан, шунингдек телекоммуникация тармоқларидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус воситаларни ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш (ЖК 278^3-м);

26. Компьютер ахборотини модификациялаштириш (ЖК 278^4-м);

27. Компьютер саботажи (ЖК 278^5-м);

28. Зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш (ЖК 278^6-м);

29. Телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш (ЖК 278^7-м);

30. Крипто-активлар айланмаси соҳасидаги қонунчиликни бузиш (ЖК 278^8-м);

31. Майнинг фаолиятини қонунга хилоф равишда амалга ошириш (ЖК 278^9-м) каби жиноятлардан иборат.

Замонавий ахборот-коммуникация технологияларининг жадал ривожланиши билан бирга жиноятчиликнинг янги ва хавфли турлари пайдо бўлмоқда. Шуни алоҳида таъкидлаш лозимки, юқорида келтирилган рўйхат доимий хусусиятга эга эмас, чунки ҳозирги кунда рақамли технологиялар воситасида содир этиладиган жиноятлар қаторига янги турдаги жиноий ҳаракатларни ҳам киритиш зарурати туғилмоқда. Яни:

1. Жосуслик (ЖК 160-м);

2. Давлат сирларини ошкор қилиш (ЖК 162-м);

3. Валюта қимматликларини қонунга хилоф равишда олиш ёки ўтказиш (ЖК 177-м);

4. Савдо ёки хизмат кўрсатиш қоидаларини бузиш (ЖК 189-м);

5. Қонунга хилоф равишда ахборот тўплаш, уни ошкор қилиш ёки ундан фойдаланиш (ЖК 191-м);

6. Рақобатчини обрўсизлантириш (ЖК 192-м);

7. Атроф табиий муҳитнинг ифлосланганлиги тўғрисидаги маълумотларни қасддан яшириш ёки бузиб кўрсатиш (ЖК 194-м);

8. Давлат рамзларига ҳурматсизлик қилиш (ЖК 215-м);

9. Жамоат бирлашмалари ёки диний ташкилотларни қонунга хилоф равишда тузиш (ЖК 216-м);

10. Ғайриқонуний жамоат бирлашмалари ва диний ташкилотлар фаолиятида қатнашишга ундаш (ЖК 216^1-м);

11. Диний ташкилотлар тўғрисидаги қонун ҳужжатларини бузиш (ЖК 216^2-м);

12. Йиғилишлар, митинглар, кўча юришлари ёки намойишлар уюштириш, ўтказиш тартибини бузиш (ЖК 217-м).

13. Ҳужжатлар, штамплар, муҳрлар, бланкалар тайёрлаш, уларни қалбакилаштириш, сотиш ёки улардан фойдаланиш (ЖК 228-м).

14. Диний таълимотдан сабоқ бериш тартибини бузиш (ЖК 229^2-м).

15. Далилларни сохталаштириш (қалбакилаштириш) (ЖК 230^1-м);

16. Тезкор-қидирув фаолияти натижаларини сохталаштириш (қалбакилаштириш) (ЖК 230^2-м);

17. Ёлғон хабар бериш (ЖК 237-м);

18. Суриштирув, дастлабки тергов ёки ёпиқ суд мажлиси маълумотларини ошкор қилиш (ЖК 239-м) ва бошқа шу каби жиноятларни келтириб ўтиш мумкин.

Рақамли технологиялар воситасида содир этиладиган жиноятлар деганда биз компьютер, интернет тармоғи ёки бошқа рақамли қурилмалардан воситачи сифатида фойдаланган ҳолда содир этиладиган ноқонуний ҳаракатларни тушунамиз. Бу жиноятлар икки асосий тоифага бўлинади: биринчиси, компьютер тизимларининг ўзига қарши қаратилган жиноятлар, иккинчиси эса, анъанавий жиноятларнинг рақамли

воситалар ёрдамида содир этилиши. Рақамли технологиялар воситасида содир этилаётган жиноятларнинг ўзига хос хусусияти шундаки, улар географик чегаралар билан чекланмайди, жиноятчи дунёнинг бир чеккасида, жабрланувчи эса бошқа қитъада бўлиши мумкин. Бундан ташқари, интернет жиноятчиларга ўз шахсини яширишга, аноним ҳолда фаолият юритишга кенг имкониятлар беради.

Рақамли технологиялар воситасида содир этиладиган жиноятларнинг энг кенг тарқалган турларидан бири фишинг ва ижтимоий инженерия усулларидир. Фишинг деганда жиноятчиларнинг жабрланувчилардан шахсий маълумотлар, пароллар, банк карталари рақамлари ёки бошқа махфий ахборотни ўғирлаш мақсадида танилган ташкилотлар, банклар ёхуд давлат органлари номидан юқори даражада ишончли кўринишдаги хабарлар юбориб, одамларни шошилинч ҳаракат қилишга ундаши тушунилади. Масалан, жиноятчи банк ходими сифатида чиқиб, қурбоннинг картаси блокланганини маълум қилиб, уни қўрқитиш орқали картанинг махфий маълумотларини беришга мажбур этади. Фишинг турлари орасида электрон почта, SMS (смишинг), овозли қўнғироқлар (вишинг) ҳамда ижтимоий тармоқлар орқали амалга ошириладиган усуллар кенг тарқалган бўлиб, ижтимоий инженерия услубида эса жиноятчилар одамларнинг психологияси, ишончи, қўрқуви ёки бефикрлигидан фойдаланиб, уларни ўзлари истаган ҳаракатларни қилишга ундайдилар.

Молиявий кибержиноятлар замонавий рақамли иқтисодиётнинг энг оғир муаммоларидан ҳисобланади. Банк карталарини клонлаш, яъни карта маълумотларини махсус қурилмалар ёрдамида ноқонуний нусхалаш ва кейин бу маълумотлардан фойдаланиб пул ўғирлаш ҳолатлари тез-тез учраб турмоқда. Онлайн фирибгарлик ҳам кенг тарқалган бўлиб, жиноятчилар ёлғон савдо сайтларини яратиб, одамлардан товар учун олдиндан тўловни олиб, кейин маҳсулот юбормайдилар. Идентификацияни ўғирлаш эса жуда хавфли жиноят тури бўлиб, бунда жиноятчи бошқа одамнинг шахсий маълумотларини ўғирлаб, унинг номидан кредит олиш, молиявий операцияларни амалга ошириш ёки бошқа ноқонуний ишларни бажариши мумкин.

Зарарли дастурлар (малваре) – кибержиноятларнинг яна бир хавфли қуроли ҳисобланади. Зарарли дастурлар турлари жуда кўп: вируслар ўзини кўпайтириб, бошқа файлларга ёпишадилар ва тизимни зарарлайдилар; троян отлари фойдали дастурлар қиёфасида кириб, кейин зарарли функцияларни бажарадилар; шпион дастурлар (spyware) фойдаланувчининг барча фаолиятини яширинча кузатиб, маълумотларини йиғадилар; Рансомваре – энг хавфли тур бўлиб, фойдаланувчининг барча файлларини шифрлаб қўяди ва уларни қайтариш учун катта миқдорда пул талаб қилади. Ботнет – зарарланган минглаб компьютерлар тармоғи бўлиб, жиноятчи уларни масофадан бошқариб, турли хил ҳужумлар учун ишлатади. Бу зарарли дастурлар одатда электрон почта қўшимчалари, зарарланган веб-сайтлар, ёлғон дастурларни юклаш орқали тарқалади. Уларнинг зарари жуда катта бўлиб, маълумотларнинг йўқолиши, тизимларнинг ишдан чиқиши, молиявий йўқотишларга олиб келади.

Ахборот тизимларининг хавфсизлигига қаратилган турли хил техник ҳужумлар ҳам рақамли технологиялар воситасида содир этилаётган жиноятларнинг муҳим қисмидир. DDoS (Distributed Denial of Service) ҳужумлари веб-сайтларни ёки онлайн хизматларни жуда кўп миқдордаги сохта сўровлар билан бомбардимон қилиб, уларни ишдан чиқаришга қаратилган ҳаракатлардир. Бу усул кўпинча рақобатчиларга зарар етказиш,

шантаж қилиш ёки сиёсий мақсадларда ишлатилади. Зеро-дей (zero-day) ҳужумлари энг хавфлиларидан бири бўлиб, булар дастурий таъминотнинг ҳали ишлаб чиқарувчи томонидан ҳам билинмаган, тузатилмаган заифликларидан фойдаланадилар. Бундай ҳужумларга қарши ҳимоя қилиш жуда қийин, чунки улар учун ҳали ҳеч қандай хавфсизлик тузатмаси мавжуд эмас.

Замонавий график ва видео-таҳрирлаш дастурлари ёрдамида рақамли ҳужжатларни қалбакилаштириш, электрон имзоларни сохталаштириш ҳозир анча осон бўлиб қолди. Deepfake технологияси эса янада хавфлироқ имкониятлар яратди – сунъий интеллект ёрдамида одамларнинг юзини ва овозини шунчалик ҳақиқийга ўхшаш тарзда қалбакилаштириш мумкинки, уларни фарқлаш жуда қийин. Бу технология сиёсатчиларнинг ёлғон нутқларини яратиш, одамларни шантаж қилиш, қоралаш ёки алдоқчилик учун ишлатилмоқда. Масалан, компания раҳбарининг овози қалбакилаштирилиб, ходимга катта миқдорда пул ўтказиш ҳақида буйруқ берилиши мумкин. Бундай жиноятларни аниқлаш ва исботлаш жуда мураккаб масала бўлиб қолмоқда.

Кибертерроризм замонавий жаҳоннинг энг хавфли таҳдидларидан бирига айланган. Кибертерроризм деганда сиёсий, мафкуравий ёки диний мақсадларга эришиш учун рақамли инфратузилмага, муҳим давлат тизимларига қаратилган ҳужумлар тушунилади. Террористик гуруҳлар энергетика тармоқларини, транспорт бошқарув тизимларини, ҳарбий объектларни, соғлиқни сақлаш инфратузилмасини ёки молиявий тизимларни бузишга ҳаракат қиладилар. Бундай ҳужумларнинг мақсади нафақат бевосита зарар етказиш, балки аҳоли орасида қўрқув ва вайронагарчилик туйғусини тарқатишдир. Кибертерроризм миллий хавфсизликка жиддий таҳдид туғдиради, чунки замонавий давлатларнинг барча соҳалари рақамли технологияларга боғлиқ ва улардаги узилишлар ҳавфли оқибатларга олиб келиши мумкин. Бундан ташқари, террорчилар пропаганда тарқатиш, янги аъзолар жалб қилиш, молиявий ресурслар йиғиш ва ҳужумларни координация қилиш учун ҳам интернетдан фаол фойдаланмоқдалар.

Рақамли технологиялар воситасида содир этиладиган жиноятлар анъанавий жиноятлардан фарқи қуйидагича: ***биринчидан,*** трансчегаравий хусусият – кибержиноятлар географик чегаралар билан чекланмайди, жиноятчи бир мамлакатда, жабрланувчи бошқа мамлакатда, сервер эса учинчи давлатда жойлашган бўлиши мумкин. Бу халқаро ҳуқуқий ҳамкорликни талаб қилади; ***иккинчидан,*** аноним бўлиш имкони – интернет жиноятчиларга ўз шахсини яширишга кенг имкониятлар беради: VPN хизматлари, TOR тармоғи, прокси серверлар, сохта аккаунтлар ва криптовалюталар орқали жиноятчини аниқлаш жуда қийин; ***учинчидан,*** тез тарқалиш – рақамли жиноятлар бир неча сониялик вақт ичида минглаб, ҳатто миллионлаб қурбонларга зарар етказиши мумкин; ***тўртинчидан,*** далилларнинг йўқолиш хавфи – рақамли далиллар физик далилларга қараганда осонроқ ўчирилиши, ўзгартирилиши ёки йўқ қилиниши мумкин; ***бешинчидан,*** доимий ривожланиши – жиноятчилар янги технологиялардан тезда фойдаланадилар ва ҳужум усулларини доимо такомиллаштирадилар, бу эса ҳуқуқни муҳофаза қилувчи органларни доим янгиликлардан хабардор бўлишга мажбур қилади.

Ҳуқуқий чоралар рақамли технологиялар воситасида содир этиладиган жиноятларга қарши курашишда муҳим ўрин тутади. Давлатлар рақамли технологиялар

воситасида содир этиладиган жиноятларни қонунчиликда аниқ тартибга солишлари, жиноий жазо чораларини белгилашлари зарур. Кибержиноятлар кўпинча трансчегаравий характерга эга бўлиб, Халқаро ҳамкорлик жуда муҳим аҳамиятга эга.

Хулоса қилиб айтганда, рақамли технологиялар воситасида содир этиладиган жиноятлар фақат технологик масала эмас, балки жиноятнинг ижтимоий, иқтисодий, сиёсий ва ҳуқуқий аспектларга эга мураккаб феномендир. Бу жиноятларнинг хусусиятлари – трансчегаравийлик, аноним бўлиш имкони, тез тарқалиш, доимий ривожланиш – уларга қарши курашишни қийинлаштиради ва янгича ёндашувларни талаб қилади. Самарали курашиш учун давлат органлари, хусусий сектор, фуқаролик жамияти ва ҳар бир фуқаронинг бирлашган ҳаракатлари зарур. Техник ҳимоя воситалари, мустаҳкам қонунчилик, халқаро ҳамкорлик, ташкилий чоралар ва, энг муҳими, аҳолининг рақамли саводхонлигини ошириш – буларнинг комплекси кибержиноятларни камайтиришга ва уларнинг зарарини минималлаштиришга ёрдам беради. Кибермаконда хавфсизликни таъминлаш – бу фақат давлат органлари ёки мутахассисларнинг вазифаси эмас, балки жамиятнинг ҳар бир аъзосининг вазифасидир. Ҳар бир интернет фойдаланувчиси киберхавфсизлик қоидаларини билиши, уларга қатъий риоя қилиши, шубҳали ҳаракатларга эҳтиёт бўлиши, ўз маълумотларини ҳимоялаши ва доимий ўрганиб бориши лозим. Фақат онгли, эҳтиёткор ва жавобгарлик туйғуси билан ҳаракат қилган ҳолда жабрланувчиларни кибержиноятлар қурбонига айланишдан ҳимоя қилишимиз мумкин. Рақамли дунё катта имкониятлар беради.

Технология ривожланиши билан рақамли технологиялар воситасида содир этиладиган жиноятлар ҳам янада мураккаблашиб бормоқда. Квант ҳисоблаш технологияларининг пайдо бўлиши ҳозирги шифрлаш усулларининг бузилишига олиб келиши мумкин, бу тубдан янгича хавфсизлик ёндашувларини талаб қилади. 5G тармоқларининг кенг тарқалиши қурилмалар сонини кескин оширади, бу ҳужум юзасини кенгайтиради. Сунъий интеллект ва машина ўрганиши ҳам ҳимоя, ҳам ҳужум учун қўлланилади – AI ҳужумлар янада нозик ва аниқ бўлиб, уларни аниқлаш қийинлашади. Биометрик маълумотларнинг ўғирланиши ва қалбакилаштирилиши хавфи ортмоқда – бармоқ изи, юз, кўз қорачиғи сканерларини алдаш усуллари такомиллашмоқда. Автоном транспорт воситаларига ҳужумлар хакерларга учраган автомобиллар жисмоний хавф туғдириши мумкин. Тиббиёт соҳасида киберхавфсизлик – тиббий қурилмалар, касалхона тизимлари, беморлар маълумотлари янги ҳужум нишонларига айланмоқда. Метаверс ва виртуал реаллик дунёсида ҳам янги тур жиноятлар пайдо бўлмоқда. Шунинг учун киберхавфсизлик соҳаси доимо ривожланиб, янги таҳдидларга тез мослашишни, инновацион ҳимоя технологияларини жорий қилишни талаб қилади

Фойдаланилган адабиётлар рўйхати:

1. ITU, Facts and Figures 2025: https://www.itu.int/itu-d/reports/statistics/2025/11/30/ff22-young-people-use-internet-more-than-the-rest-of-the-population.
2. Cybersecurity Ventures: Cybercrime Damages Report.
3. Statista: Internet Crime Complaints.
4. Kaspersky: Cyber-Attacks Increased by 38% in 2025.

5. Cybersecurity Ventures: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, Nilson Report: https://nilsonreport.com/, Statista: Global card fraud losses: https://www.statista.com/statistics/1033173/global-payment-card-fraud-losses.
6. Ўзбекистон Республикасининг “Киберхавфсизлик тўғрисида”ги
2022 йил 15 апрелдаги Қонуни.
7. Ўзбекистон Республикасининг Жиноят кодекси // URL: http://www.lex.uz.
8. Жиноят ҳуқуқи. Умумий қисм: Дарслик (Тўлдирилган ва қайта ишланган иккинчи нашри) / Р. Кабулов, А. А. Отажонов ва бошқ. – Т.: Ўзбекистон Республикаси ИИВ Академияси, 2021. – 446 б.
9. Жиноят ҳуқуқи. Махсус қисм: Дарслик / Р. Кабулов, А.Отажонов ва бошқ. – Т.: Ўзбекистон Республикаси ИИВ Академияси, 2021. – 1004 б.
10. Жиноятларни квалификатсия қилиш: ИИВ олий таълим муассасалари учун дарслик. – Т.: Ўзбекистон Республикаси ИИВ Академияси, 2016. – 323 б