



National and foreign experience in preventing crimes committed using information technologies

Anvar CHORIEV¹

Tashkent State University of Law

ARTICLE INFO

Article history:

Received December 2024

Received in revised form

15 December 2024

Accepted 20 January 2025

Available online

15 February 2025

Keywords:

cybercrime,
digital security,
information technology,
financial fraud,
personal data,
cybersecurity,
crypto assets,
international experience,
legal regulation.

ABSTRACT

This article examines crimes committed using digital technologies and explores national and international experiences in their prevention. It analyzes different types of cybercrimes, their risks at global and local levels, and legislative measures taken by various countries. Special attention is given to effective methods of combating cybercrime and proposals for enhancing preventive measures in the future.

2181-1415/© 2025 in Science LLC.

DOI: <https://doi.org/10.47689/2181-1415-vol6-iss1/S-pp319-325>

This is an open access article under the Attribution 4.0 International (CC BY 4.0) license (<https://creativecommons.org/licenses/by/4.0/deed.ru>)

Ахборот технологияларидан фойдаланган ҳолда содир этиладиган жиноятларнинг олдини олишдаги миллий ва хорижий тажриба

АННОТАЦИЯ

Калит сўзлар:

кибержиноятлар,
рақамли хавфсизлик,
ахборот технологиялари,
молиявий фирибгарлик,
шахсий маълумотлар,
киберхавфсизлик,
криптоактивлар,
халқаро тажриба,
ҳуқуқий тартибга солиш.

Мазкур мақолада рақамли технологиялардан фойдаланган ҳолда содир этиладиган жиноятлар ва уларнинг олдини олишга оид миллий ҳамда хорижий тажрибалар таҳлил қилинади. Кибержиноятларнинг турлари, уларнинг глобал ва маҳаллий миқёсдаги хавф-хатарлари, шунингдек, халқаро ва миллий қонунчилик тажрибалари ёритилган. Шунингдек, мақолада кибержиноятларга қарши курашишнинг самарали усуллари ҳамда келгусида амалга оширилиши лозим бўлган чора-тадбирлар таклиф этилади.

¹ Independent Researcher, Tashkent State University of Law.

Национальный и зарубежный опыт в предотвращении преступлений, совершаемых с использованием информационных технологий

АННОТАЦИЯ

Ключевые слова:

киберпреступления, цифровая безопасность, информационные технологии, финансовое мошенничество, персональные данные, кибербезопасность, криптоактивы, международный опыт, правовое регулирование.

В данной статье рассматриваются преступления, совершаемые с использованием цифровых технологий, а также национальный и международный опыт их предотвращения. Анализируются виды киберпреступлений, их риски на глобальном и локальном уровнях, а также законодательные меры различных стран. Особое внимание уделяется эффективным методам борьбы с киберпреступностью и предложениям по совершенствованию превентивных мер в будущем.

Ҳозирги вақтда ахборот (ёки рақамли) технологиялар жамият ҳаётининг ҳар бир соҳасига жадаллик билан кириб келмоқда, мавжуд ижтимоий муносабатларни ўзгартириб, янгидан-янги ижтимоий муносабатлар юзага келмоқда. Бу эса ўз навбатида турли ҳуқуқбузарликлар, жумладан жиноятларнинг янги турларини, уларни содир этишнинг янги шаклларини келтириб чиқармоқда.

Одатда рақамли технологиялардан фойдаланиб содир этиладиган жиноятлар кибержиноятлар ёки кибермаконда содир этиладиган жиноятлар деб юритилади.

Кибермаконда содир этилаётган жиноятларнинг ижтимоий хавфлилик даражаси аввало ушбу турдаги жиноятларни кескин кўпайиб бораётганлиги ҳамда жабрланувчилари сони ва зарар кўлами катталиги, ер юзининг исталган ҳудудида туриб, мол-мулкни талон-торож қилиш имкониятининг мавжудлиги ҳамда уларни аниқлаш ва фош этишнинг мураккаблиги билан изоҳланмоқда.

Кейинги пайтда жиноятчи шахслар аҳолининг банк ҳисобидаги пулларини талон-торож қилишда янги усуллардан фойдаланаётганликлари, хусусан, дастурий аппарат қурилмалари ёрдамида қонунга хилоф тарзда банк картаси ёки бошқа тўлов карталарини нусхасини яшаш ёки сохталаштириш орқали ўзганинг банк ҳисобидаги ёхуд электрон тўлов ҳамёнларидаги пулларини талон-торож қилиш ҳолатлари кузатилмоқда.

Маълумотларга кўра, бугунги кунда дунё бўйича кибержиноятлардан келадиган зарар 6,6 триллион АҚШ доллари миқдорида баҳоланмоқда.

2025 йилда ушбу жиноятлардан кўриладиган зарар миқдори 10,5 триллион АҚШ долларини ташкил қилиши мумкинлиги прогноз қилинмоқда.

Дунё бўйича кибермаконда содир этилаётган жиноятларнинг турли соҳалар бўйича ажратиб кўрсатганда қуйидагилар маълум бўлган:

- Молия соҳасида 33%;
- Соғлиқни сақлаш соҳасида 24%;
- Давлат секторида 22%;
- Чакана савдо соҳасида 17%;
- Энергетика соҳасида 4%.

Мамлакатимизда ҳам кибержиноятлар йилдан-йилга ошиб кетаётганлигини таъкидлаб ўтиш жоиз. Бундай жиноятлар кўпроқ қуйидаги йўналишларда содир этилмоқда:

1) Ўзгалар мулкани қўлга киритиш билан боғлиқ жиноятлар.

Тошкент шаҳар ИИББ берган маълумотларга кўра, рақамли технологиялардан фойдаланиб содир этилган жиноятлар 2020 йилда 106 тани ташкил қилган бўлса, ушбу кўрсаткич 2021 йилда 2281 тани, 2022 йилда 4332 тани ташкил қилган. 2022 йилда рақамли технологиялардан фойдаланиб содир этилган жиноятлардан 2747 тасини киберўғрилик, 625 тасини кибертовламачилик, 884 тасини наркотиклар савдоси билан боғлиқ жиноятлар ташкил қилган.

2) Шахсга доир маълумотлар тўғрисидаги қонунчиликни бузиш.

Таҳлилларга кўра, охириги 3 йилда шахсга доир маълумотлар тўғрисидаги қонунчиликни бузиш жинояти 38 фоизга, ноқонуний эгалланган шахсга доир маълумотлар орқали - ҳақорат қилиш ва туҳмат қилиш жиноятлари 50 фоизга, шахсга доир маълумотларни ошкор қилиш билан қўрқитиб - аёлни жинсий алоқа қилишга мажбур этиш жиноятлари 4 бараварга, товламачилик жиноятлари 18 бараварга ошганлигини, мазкур қилмишлар натижасида ўз жонига қасд қилиш ҳолатлари кескин кўпайганлигини кўрсатмоқда. Халқаро миқёсда “сексуал товламачилик” деган атама кўпроқ қўлланилмоқда.

3) Наркотиклар савдоси.

Сўнгги вақтларда наркотиклар савдоси бутун дунёда бўлгани каби, мамлакатимизда ҳам кибермаконга ўтмоқда. Аниқланган маълумотларга кўра, 2023 йилда мамлакатимизда интернетда психотроп моддалар савдосига ихтисослашган 52 та ахборот ресурси аниқланган, улардан 14 таси веб-сайтларни, 38 таси эса Telegram мессенжерини ташкил этган. Telegram-каналлар орқали 120 мингга яқин фойдаланувчи қамраб олинган.

Сўнгги уч йил (2021-2023 йиллар) мобайнида мазкур йўналишда

25 мингга яқин жиноят иши қўзғатилиб, 17 мингдан ортиқ шахс жиний жавобгарликка тортилган. Шундан 5 мингга яқини (30 фоиз) 30 ёшгача бўлган шахсларни ташкил этган.

Энг ёмони бундай жиноят содир этганлар орасида ёшларнинг кўпайиб кетаётганлиги ачинарли ҳол. Таҳлилларга кўра, наркожиноят содир этган ёшларнинг сони йилдан йилга ўсиб бормоқда. Хусусан, 2021 йилда бундай жиноятлар содир қилганларнинг 23 фоизини ёшлар ташкил қилган бўлса,

2022 йилда 24,6 фоизга, 2023 йилда эса 31,2 фоизга етган.

4) Мобил қурилманинг IMEI-кодларини ўзгартириш, клонлаштириш билан боғлиқ ҳуқуқбузарликлар.

Кейинги пайтда айрим шахслар томонидан ноқонуний олиб кирилган, шунингдек, йўқотилган ёки ноқонуний эгалланганлиги сабабли алоқа тармоғидан фойдаланиши тўсиб қўйилган бир неча минглаб мобил қурилмаларнинг IMEI-кодларини ҳуқуқбузарлар томонидан ҳақ эвазига **клонлаш** орқали рўйхатдан ўтказиб, тармоқдан фойдаланишига эришилмоқда.

Бугунги кунда 80 минг сўмдан 500 минг сўмгача ҳақ эвазига мобил қурилмаларнинг IMEI-кодларини клонлаштириб бераётган “телефон усталари” сони ошиб, аксарияти ошқора тарзда фаолият олиб бормоқда.

IMEI-кодларни клонлаштиришни олди олинмаганлиги мобил телефон ўғирлиги жиноятлари ошишига ва уларнинг аксарияти фош этилмасдан қолишига бевосита сабаб бўлмоқда.

Хусусан, сўнгги уч йилда мобил телефон ўғирлиги жиноятлари 500 %га ошган, биргина 2021 йилда мобил телефон ўғирлиги жиноятлари 4.324 та содир этилиб, умумий ўғирлик жиноятларнинг 26 фоизини ташкил этган.

IMEI-кодларни клонлаштирилганлиги сабабли йўқотилган ёки ноқонуний эгалланган мобил телефонларнинг 60 фоизга яқини аниқланмасдан қолмоқда.

5) “Дипфейк”дан фойдаланиб, фирибгарлик содир этиш.

Сунъий интеллектдан фойдаланиб жиноят содир қилиш ҳолатлари кўпаймоқда. Жумладан таниқли шахсларнинг тасвирларидан фойдаланиб, уларнинг номидан маълум бир хизматларни реклама қилиш, турли ресурсларга шахсий маълумотларни, телефон, банк карталари маълумотларини киритишга тарғиб қилиш орқали, фирибгарлик содир этиш ҳолатлари кўпайиб бормоқда.

б) Крипто-активлар соҳасидаги ҳуқуқбузарликлар.

Ахборот-коммуникация технологиялари билан боғлиқ жиноятларнинг сўнгги йилларда кенг тарқалаётган турларидан бири бу крипто-активлар айланмаси билан боғлиқ жиноятлар ҳисобланади.

Крипто-активлар соҳасидаги ҳуқуқбузарликларга крипто-активлар ва блокчейн технологиялардан фойдаланиб содир этилган турли ҳуқуқбузарликлар киради. Сўнгги йилларда криптоактивлардан молиявий операцияларни амалга ошириш учун кенг қўлланилаётганлиги бундай фаолият билан боғлиқ ҳуқуқбузарликларнинг ҳам кўпайишига олиб келмоқда.

Халқаро тажрибадан келиб чиққан ҳолда, крипто-активлар айланмаси билан боғлиқ қуйидаги ҳуқуқбузарликларни ажратиш кўрсатиш мумкин:

- жинорий фаолиятдан олинган даромадларни легаллаштириш. Крипто-активлар коррупция, гиёвандлик воситалари ёки психотроп моддалар билан қонунга хилоф равишда муомала қилишдан иборат жиноятлар, контрабанда жиноятлари орқали олинган даромадларни легаллаштириш махсус миксер (mixers) ёки транзакцияларни анонимлаштириш хизматлари орқали яширилади ҳамда қонунийлаштирилади;

- фирибгарлик. Ушбу соҳани ҳуқуқий тартибга солиш етарли даражада эмаслиги ҳамда крипто-активлар махфийлиги даражаси юқори бўлганлиги учун крипто-активлар билан боғлиқ битимларни амалга оширишда фирибгарлик қурбони бўлиш эҳтимоли юқори. Жумладан, крипто-активларни сотиб олиш ёки сотишда фирибгарликка асосланган платформалар ёки ICO (Initial Coin Offering)[1] дан фойдаланишда алданиб қолиш эҳтимоли юқори;

- киберҳужумлар ва тармоқни бузиш. Крипто-активлар биржалари, крипто ҳамёнлар ва шунга ўхшаш тизимлар кўпинча киберҳужумлар объектига айланади;

- терроризмни молиялаштириш. Крипто-активлар махфийлиги даражаси юқори бўлганлиги учун ундан терроризм ва ноқонуний қуроли гуруҳларни молиялаштиришда фойдаланилиши эҳтимоли юқори;

- муаллифлик ҳуқуқларини бузиш. Блокчейн технологияларидан фойдаланадиган онлайн платформаларда ноқонуний контентлар, дастурий маҳсулотлар, мусиқалар, фильмлар ва бошқа рақамли активлар нусхаларидан ноқонуний фойдаланиш эҳтимоли юқори.

Ахборот технологиялар соҳасидаги ҳуқуқбузарликларга қарши курашиш бўйича хориж тажрибаси.

Юқорида таъкидлаб ўтганимиздек, раамли технологиялар соҳасида ҳуқуқбузарликлар туфайли етказилаётган зарарлар триллионлаб АҚШ долларини ташкил этмоқда ва бунга қарши курашиш ҳам такомиллаштирилиб борилмоқда.

Халқаро парламентлараро иттифоқнинг 2024 йил 23-27-март кунлари ўтказилган 148-Ассамлеясида “Автомном қурол тизимлари ҳамда сунъий интеллектнинг ижтимоий ва гуманитар таъсирини кўриб чиқиш тўғрисида”ги резолюцияни қабул қилди. Хабарингиз бор 2024 йилда 80 дан ортиқ давлатларда парламент ва президентлик сайловлари ўтказилади, шунинг учун ушбу йилни супер сайловлар йили ҳам дейишади. Айнан сайлов жараёнларида “дипфейк”лардан фойдаланиш ортиб бораётганлиги, сайлов ташвиқотини олиб боришда кенг қўлланилиши мумкинлигини, унинг олдини олиш чораларини кўриш зарурлиги таъкидланган.

2024 йил март ойида Европарламент томонидан “Сунъий интеллект тўғрисида”ги қонун қабул қилинди. Қонун сунъий интеллектдан фойдаланишда шаффофлик ва аниқлик бўлиши, унинг устидан назорат механизмлари ҳақида умумий қоидаларни ўз ичига олган.

Хорижий давлатларда киберхавфсизликни таъминлаш бўйича қонунчилик асослари яратилган ва у такоимиллаштириб борилмоқда. Жумладан, АҚШда 2002 йилда “Ахборот хавфсизлигини бошқариш тўғрисида” қонун қабул қилинган бўлиб, ушбу қонун ахборотга рухсатсиз киришлардан ҳимоя қилиш, ундан фойдаланиш, эълон қилиш, тарқатиш, ўзгартириш ёки йўқ қилиш, ахборот тизимларини ҳимоя қилиш, шахсий ва мулкый ахборотларнинг махфийлигини таъминлаш масалаларини тартибга солади.

Шу билан биргаликда, 2015 йилда “Ахборот алмашиш ва киберхавфсизлик тўғрисида” қонун (CISA) қабул қилинган бўлиб, у АҚШ ҳукуматидаги йирик технологик компаниялар (APPLE, GOOGLE ва ...) билан интернет трафик ва бошқа ахборотлар алмашиш имконини беради.

Хитойда 2016 йил 7 ноябрда “Киберхавфсизлик тўғрисида”ги қонун қабул қилинган бўлиб, у миллий хавфсизлик билан боғлиқ бўлган ахборотларни йиғиш, сақлаш ва ундан фойдаланишга оид муносабатларни тартибга солади.

Қонун ахборот тўплаш, сақлаш, қайта ишлаш ва узатиш билан боғлиқ фаолият шуғулланадиган, компьютерлар ва тегишли техникага эга барча операторлар ва тизимларга нисбатан қўлланилади. Қонун ахборот тизимлари операторларини тегишли сертификациядан ўтиши зарурлигини ҳамда миллий хавфсизлик ёхуд жамоат манфаатларига дахл қилувчи иқтисодий, технологик ёки илмий маълумотларни экспорт қилишни ва маълумотларни Хитойдан ташқарида сақлашни таъқиқлайди.

Қонунга мувофиқ, ХХР мансабдор шахслари Хитойнинг муҳим ахборот инфраструктураларига хакерлик ҳужумлари уюштириш, киришга уриниш, арилишида гумон қилинган хорижий муассасалар активларига банд солиш ҳуқуқини беради.

Хорижий экспертлар томонидан 2020 йил 1 июндан кучга Хитойнинг “Киберхавфсизлик чоралари” ўзининг энг майда жиҳатларига ишлаб чиқилганлиги таъкидланади.

Сингапур киберхавфсизлик бўйича етакчи давлатлардан ҳисобланади.

Сингапурда киберхавфсизлик чоралари “Киберхавфсизлик тўғрисида”ги, “Шахсий маълумотлар муҳофазаси тўғрисида”ги, “Кибержиноятлар ва бошқа кибертаҳдидларга қарши курашиш тўғрисида”ги, “Киберхавфсизлик ва компьютерлардан ноқонуний фойдаланиш тўғрисида”ги қонунлар билан тартибга солинади.

Грузияда киберхавфсизлик масаласи “Ахборот хавфсизлиги тўғрисида”ги қонун билан тартибга солинади.

Мудофаа вазирлиги ҳузурида Киберхавфсизлик бюроси, ҳарбий объектлар ва мудофаа соҳасидаги, Адлия вазирлиги ҳузуридаги Ахборот алмашиш бўйича агентлик давлат секторидаги киберхавфсизлик масалалари билан шуғулланади ва ахборот хавфсизлиги тўғрисидаги қонун ижроси бўйича назоратни олиб боради. Шунингдек, ички ишлар вазирлиги ҳузурида Кибержиноятлар бўлими ташкил этилган.

Қўшни давлат **Қозоғистонда** ҳам кибержиноятчилик масаласига жиддий эътибор қаратилмоқда. Чунки, охириги 7 йилда Қозоғистонда кибержиноятлар сони 10 баробардан кўпроққа ошган. Кибержиноятлар умумий жиноятларнинг 18%ни, фирибгарлик билан боғлиқ жиноятларнинг 43%ни ташкил этмоқда.

Кибержиноятчиликка қарши курашишнинг ҳуқуқий асосини “Ахборотлаштириш тўғрисида”ги қонун ташкил қилади. Ушбу қонунга мувофиқ, ахборот хавфсизлиги бўйича масъул орган Рақамли ривожланиш, инновациялар ва аэрокосмик саноат вазирлиги ҳисобланади. Шунингдек, Қозоғистонда ахборот хавфсизлиги бўйича оператив марказ, ахборот хавфсизлиги ҳодисалари бўйича хизмат, ахборот хавфсизлигини мувофиқлаштириш миллий маркази, ахборот тизимлари хавфсизлиги маркази, давлат техник хизмати, ахборот хавфсизлиги бўйича миллий институт каби тизимлар фаолият юритади.

Юқорида кўрсатиб ўтилган барча давлатларда, рақамли технологиялардан фойдаланиб содир этилган молиявий жиноятлар, шахсга доир маълумотларни ошкор қилганлик бўйича жиноий, маъмурий ва фуқаролик жавобгарлиги мавжуд.

Мамлакатимизда ҳам рақамли технологиялардан фойдаланиб содир этиладиган ҳуқуқбузарликларга қарши курашишнинг ҳуқуқий асослари яратилган.

Жумладан, “Ахборотлаштириш тўғрисида”ги, “Ахборот эркинлиги принциплари ва кафолатлари тўғрисида”ги, “Автоматлаштирилган банк тизимида ахборотни муҳофаза қилиш тўғрисида”ги, “Шахсга доир маълумотлар тўғрисида”ги, “Киберхавфсизлик тўғрисида”ги қонунлар мавжуд.

Шунингдек, Жиноят кодексининг Махсус қисми 21-боби (Ахборот технологиялари соҳасидаги жиноятлар ЖК 2781-2789-моддалар)да ҳамда ЖК махсус қисмининг муайян жиноятлар учун жавобгарлик белгиланган моддаларида, Маъмурий жавобгарлик тўғрисидаги кодекснинг 155, 1551-1555-моддаларида жавобгарлик белгиланган.

Ўзбекистон Республикасининг 2024 йил 19 январдаги “Ўзбекистон Республикасининг Жиноят, Жиноят-процессуал кодексларига ҳамда Ўзбекистон Республикасининг Маъмурий жавобгарлик тўғрисидаги кодексига ўзгартириш ва қўшимчалар киритиш ҳақида” ЎРҚ-899-сон Қонуни Жиноят кодексига Кристо-активлар айланмаси соҳасидаги қонунчиликни бузиш, деб номланган 2788-модда, Майнинг фаолиятини қонунга хилоф равишда амалга ошириш, деб номланган 2789-модда киритилди. Шунингдек, Маъмурий жавобгарлик тўғрисидаги кодексга

Крипто-активлар айланмаси соҳасидаги қонунчиликни бузиш, деб номланган 1554-модда ҳамда Майнинг фаолиятини қонунга хилоф равишда амалга ошириш, деб номланган 1555-модда киритилди.

Тан олиш керак, бундай чоралар сабаб билан эмас, балки оқибат билан курашишдир. Рақамли технологиялар соҳасидаги ҳуқуқбузарликлар учун жавобгарлик чоралари кучайтирилиб бораётганлигига қарамасдан, бундай жиноятлар кўпайиб бормоқда. Шу сабабдан, бундай жиноятларни келтириб чиқарувчи сабабларни аниқлаш ва олдини олишга эътибор қаратиш лозим. Бунда қуйидаги чора-тадбирлар таклиф этилади:

1. Молиявий саводхонлик концепциясини қабул қилиш ва аҳолининг молиявий саводхонлигини ошириш.

2. Ўзгалар номига он-лайн кредитлар расмийлаштиришнинг олдини олиш мақсадида шахснинг кредит олиш бўйича ўзига-ўзи таъқиқ қўйишини қонуний асосларини яратиш (“Кредит ахбороти алмашинуви тўғрисида”ги, “Банклар ва банк фаолияти тўғрисида”ги, “Истеъмол кредити тўғрисида”ги қонунларга ўзгартириш киритиш).

3. Телефон орқали содир этиладиган фирибгарлик, ўғрилик жиноятларини олдини олиш учун банк ўзининг мобил иловаси орқали хизмат кўрсатишда жисмоний шахсга амалга ошириладиган банк операцияларни у танлаган ишончли вакил томонидан тасдиқлаш ёки бекор қилиш имкониятини яратишнинг ҳуқуқий асосларини яратиш («Банклар ва банк фаолияти тўғрисида»ги ҳамда «Тўловлар ва тўлов тизимлари тўғрисида»ги қонунларга ўзгартириш ва қўшимчалар киритиш) лозим ҳисобланади.

Фойдаланилган адабиётлар рўйхати:

1. ICO - компаниялар янги крипто-активларни чиқариш учун пул йиғиш платформаси. Бунда инвесторлар ўз-молиявий сармоялари ҳисобига криптоактивлар олишади. Ўз моҳиятига кўра ICOни фонд биржасида акцияларни дастлабки оммавий жойлаштириш (IPO)нинг крипто-актив версияси сифатида тушуниш мумкин.